Deployment and Customization

iPlanet Delegated Administrator

Version 4.5

Revised April, 2001

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

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

Contents

Part 1

Introduction & Deployment Planning

Chapter 1, “Introduction”

Chapter 2, “Deployment Planning”

Chapter 1

Introduction

This chapter provides a quick overview of Delegated Administrator features and and briefly describes how it works. The chapter includes the following sections:

- Overview of Delegated Administrator
- Delegating Administration
- Architecture
- Customization
- What’s New in This Release
- What’s New in This Manual

Overview of Delegated Administrator

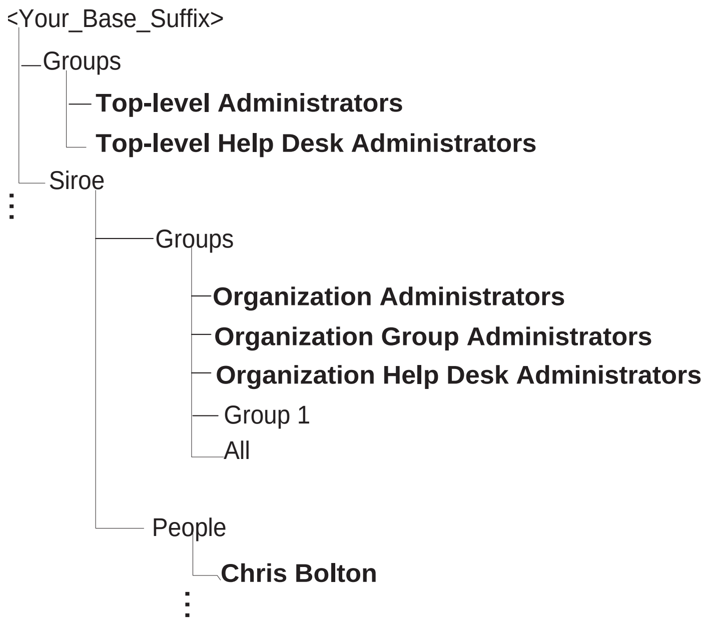
iPlanet Delegated Administrator is a web-based directory application designed for Internet Service Providers (ISPs), enterprise extranets, and large corporate intranets. Using Delegated Administrator, you can automatically create a directory structure that supports six pre-configured administrator types.

Delegated Administrator helps you manage your directory data efficiently. It distributes the workload among a group of administrators rather than focusing it on a select few. It also puts user management in the hands of those who are directly impacted by changes to the directory database. The results are faster turnaround times and reduced administration costs.

Delegating Administration

When you install Delegated Administrator, it automatically creates all user entries and appropriate Access Control Instructions (ACIs) required to support six types of administrators (see Figure 1-1). At the highest level, Top-level Administrators have unrestricted access to data for all users in the entire enterprise. A Top-level Administrator can create new organizations, and then delegate user data management to other administrators at levels further down in the user tree. This makes it possible for Organization Administrators, Help Desk Administrators, Group Administrators, and even end users to make some changes in the directory. An administrator's role determines the scope of changes he or she can make.

Figure 1-1 The default administrator types for Delegated Administrator,


<Your_Base_Suffix>
Groups
Top-level Administrators
Top-level Help Desk Administrators
Siroe
Groups
Organization Administrators
Organization Group Administrators
Organization Help Desk Administrators
Group 1
All
People
Chris Bolton

Architecture

Delegated Administrator uses HTTP or HTTPS and LDAP or LDAPS protocols. It works in conjunction with iPlanet Directory Server 4.12 and a web server such as iPlanet Web Server 4.1 (see Figure 1-2). Directory Server stores user information and makes it accessible to other applications and servers. Delegated Administrator uses a servlet engine and Java servlet APIs to pass user data between Directory Server and Web Server. Web Server serves up HTML forms that administrators can use to create or modify user entries in the directory (see Figure 1-3).

Figure 1-2 Delegated Administrator Architecture

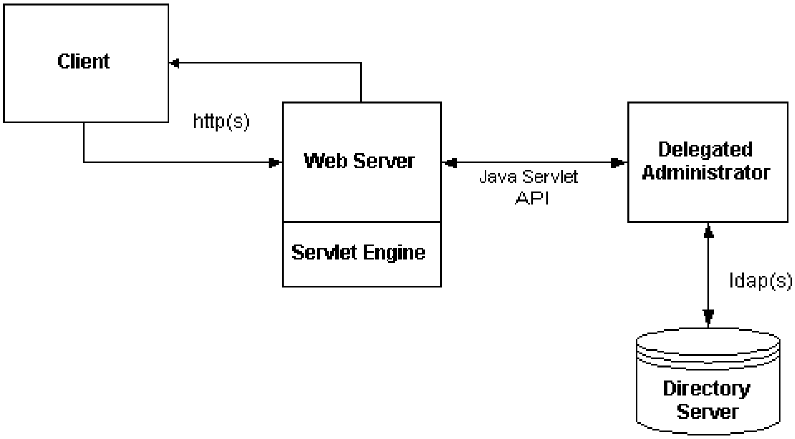
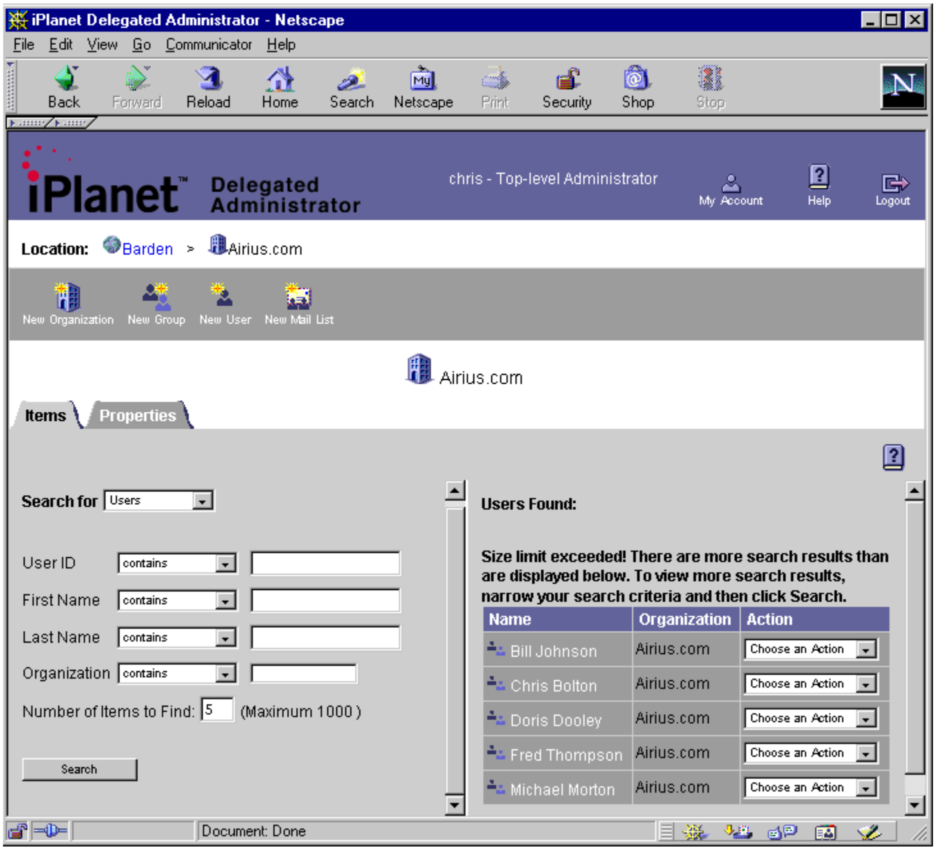


Figure 1-3 Customizable HTML forms comprise the Delegated Administrator UI.



Location: Barden > Airius.com

Airius.com

Search for: Users

User ID	contains	
First Name	contains	
Last Name	contains	
Organization	contains	

Number of Items to Find: 5 (Maximum 1000)

Users Found:

Size limit exceeded! There are more search results than are displayed below. To view more search results, narrow your search criteria and then click Search.

Name	Organization	Action
Bill Johnson	Airius.com	Choose an Action
Chris Bolton	Airius.com	Choose an Action
Doris Dooley	Airius.com	Choose an Action
Fred Thompson	Airius.com	Choose an Action
Michael Morton	Airius.com	Choose an Action

Customization

While designed to work right out of the box, Delegated Administrator is also highly customizable. Using instructions in this manual, you can modify the UI look and feel, and extend back-end functionality. The following are examples of ways you can customize Delegated Administrator to meet your company's needs:

- Modify HTML page layout and related directory attributes.
- Customize Delegated Administrator configuration in the directory.
- Extend or replace servlet functionality.

What's New in This Release

The following features are new in Delegated Administrator 4.5:

Flexible Directory Information Tree (DIT) support. The current release removes a restriction present in previous versions that required the use of a specific fixed DIT structure and attribute for the relative distinguished name of the base suffix in the directory. Delegated Admin 4.5 may now be installed against a variety of DIT structures and base suffixes including o=, ou=, dc=, l=, and c=.

Support for Netscape Messaging Server 4. Templates are available to support managing account options including access method (POP, IMAP, webmail), quota, vacation message, forwarding options, and end-user mailing list management. These templates are only installed when this option is chosen during installation.

Customized administrator roles. Added support for customized administrative roles. New roles can be built by creating new HTML templates, and modifying the Directory Server ACIs.

Class of Service (COS). Supports the ability to set the value of one or more directory attributes for large sets of users with a single write to the directory (for example, "email Bronze" sets those users up with 5mb mail quota and access to WebMail).

Configuration options can be set on a per-Organization basis. Many of the configuration options such as COS definitions and userid uniqueness can be set on a per-Organization (directory branch) basis.

Improved User Interface. New user interface includes navigation and ease-of-use enhancements.

JPEG image support. Capable of displaying JPEG images stored in the directory.

Support for SiteMinder Single Sign-On. iPlanet Delegated Administrator supports single sign-on via Netegrity SiteMinder 4.0 or higher.

SSL encryption performance enhancement. SSL communications are now up to 10 times faster.

What’s New in This Manual

Product information that was not available at the initial release of Delegated Administrator 4.5 has been added to this manual. These topics include:

- Appendix B, “Upgrading from Delegated Administrator Version 4.11”
- “Determining the Appropriate Template” in Chapter 13

Other modifications to the original manual include the following:

- Appendix B, “User Data Migration Scripts,” has been removed from this manual. It has been revised and is now a separate HTML document packaged with the actual scripts. For more information, see `http://docs.iplanet.com/docs/manuals/deladmin/45/related.htm`
- Appendix E, “Mapping Operations to Templates,” was removed from this manual. It is replaced by the section ““Determining the Appropriate Template” on page 302.
- Typographical errors have been corrected and other minor corrections have also been incorporated into this updated edition.

Chapter 2

Deployment Planning

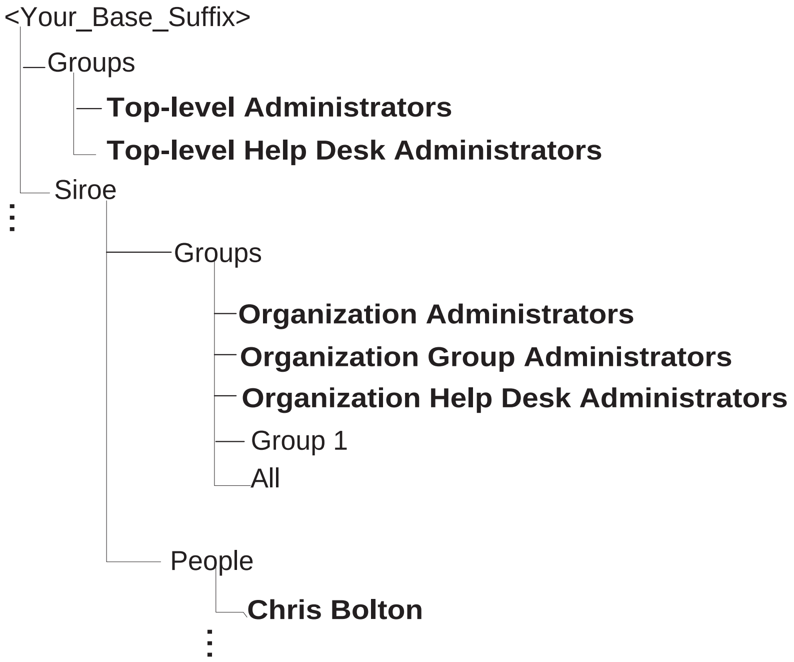
There are a number of issues you must resolve and options you can consider before you begin to install Delegated Administrator. This chapter provides information you'll need for planning and installing Delegated Administrator. The chapter includes the following sections:

- Determining Your Delegated Administrator Needs
- Flexible DIT Options
- Options to Consider Before Installation
- Implications of Customizing Delegated Administrator

Determining Your Delegated Administrator Needs

When you install Delegated Administrator, if you are provisioning a directory for the first time, a base suffix is automatically created for you. It is designed for storing and managing user data. Special object classes identify the user and group entries managed by Delegated Administrator. These object classes make it possible for Delegated Administrator to manage only selected data—user data—and not interfere with other aspects of your tree such as servers, services, or hardware. The way you use the default base suffix depends upon your company's current directory environment and your long-term directory needs.

Figure 2-1 Delegated Administrator Default Administrator Types.


<Your_Base_Suffix>
Groups
Top-level Administrators
Top-level Help Desk Administrators
Siroe
Groups
Organization Administrators
Organization Group Administrators
Organization Help Desk Administrators
Group 1
All
People
Chris Bolton

The following are common scenarios for Delegated Administrator 4.5 customers:

- You are provisioning a user database for the first time.
- You have already deployed a directory server and have provisioned it with user accounts, but have not deployed Delegated Administrator.
- You have already deployed a directory server with a pre-4.5 version of Delegated Administrator.

In any case, before attempting to install Delegated Administrator 4.5, you should plan or optimize your user directory structure for performance and extensibility. The following sections offer suggestions for effectively using the Delegated Administrator base suffix. For detailed information regarding general directory planning and implementation, see the Directory Server *Deployment Guide* available at the following URL: `http://home.netscape.com/eng/server/directory/4.1/deploy/contents.htm`.

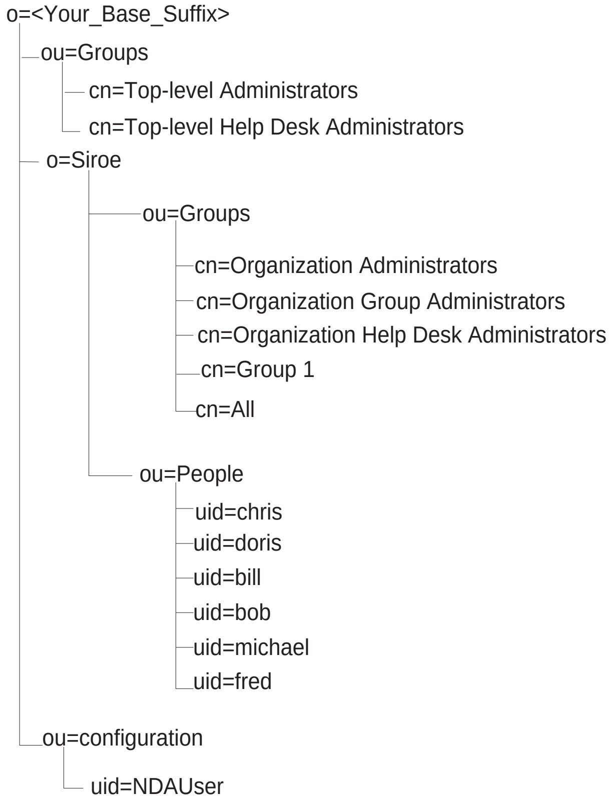
The Delegated Administrator DIT

The default Delegated Administrator base suffix contains directory entries and appropriate Access Control Instructions (ACIs) required to support seven types of administrators:

- Top-level Administrator
- Top-level Help Desk Administrator
- Organization Administrator
- Organization Help Desk Administrator
- Group Administrator
- End User (acting as an Administrator)
- Authentication Administrator

In Figure 2-2 on page 26, the End User is represented by a uid such as `uid=chris`. The Authentication Administrator is represented by `uid=NDAUser`.

Figure 2-2 Implementation of the Delegated Administrator DIT.


o=<Your_Base_Suffix>
ou=Groups
cn=Top-level Administrators
cn=Top-level Help Desk Administrators
o=Siroe
ou=Groups
cn=Organization Administrators
cn=Organization Group Administrators
cn=Organization Help Desk Administrators
cn=Group 1
cn=All
ou=People
uid=chris
uid=doris
uid=bill
uid=bob
uid=michael
uid=fred
ou=configuration
uid=NDAUser

Each administrator has specific privileges as defined in the Delegated Administrator ACIs (see Table 2-1). To see the actual ACIs, see Appendix , "Delegated Administrator Access Control Instructions (ACIs)," on page 427. The Top-level Administrator has the widest scope of access privileges. Administrators further down in the tree have a more narrow scope of administrative responsibilities.

Table 2-1 A summary of Administrator privileges.

		Can modify these directory entries				
Administrator	**Access Privileges**	**Root**	**Organi-zation**	**Group**	**Others' Accounts**	**Own Account**
Top-level	Can create, modify, and delete entries across all organizations; can change organizations size limits.Typically creates new organizations and groups; creates peer Top-level administrators.	✓	✓	✓	✓	✓
Organization	Can create, modify, and delete entries in all groups within own organization; cannot change organization size limits.Typically creates new organizations and groups; creates peer organization administrators.		✓	✓	✓	✓
Group	Can create, modify, and delete entries within own group; cannot change group size limits. Typically creates new groups and new user entries; creates peer group administrators.			✓	✓	✓
Top-level Help Desk	Can modify Password attribute for any user across all organizations.				✓	✓
Organization Help Desk	Can modify Password attribute for any user in own organization.				✓	✓
User Account	Can access own directory entry; can modify only selected user attributes.					✓
Authentication Administrator	Is not a real user, but a directory entry used only for authentication purposes.					

The Authentication Administrator

The Authentication Administrator is a user entry, `uid=NDAUser`, stored under `ou=config` in Directory Server. Its special purpose is to act as an agent for Delegated Administrator, binding to the directory during authentication when necessary.

Organizations and Groups

A Delegated Administrator *organization* (called a *domain* in previous versions of the program) is a container for multiple user-directory entries. It is similar to an administrative organization such as `o` in LDAP, but it is not exactly the same. It uses the object class `NSManagedDomain.` By default, each Delegated Administrator organization includes containers `ou=Groups` and `ou=People`. The information about each organization unit is stored in two subtrees. The Groups subtree stores group information, and the People subtree stores user entries.

When you create a Delegated Administrator organization, a new entry is created in the directory. The following is the directory entry for the default organization `Siroe.com`:

```
dn: o=Siroe, o=ISP
objectClass: top
objectClass: organization
objectClass: nsManagedDomain
# objectClass: nsUniquenessDomain
o: Siroe.com
nsMaxUsers: 1000
nsMaxDepts: 100
nsMaxMailLists: 1000
nsNumMailLists: 0
nsMaxDomains: 10
nsNumDepts: 0
nsNumUsers: 0
nsNumDomains: 0
```

A Delegated Administrator *group* (called a *department* in previous versions of Delegated Administrator) is similar to an administrative group such as ou in LDAP, but the two are not exactly the same. A Delegated Administrator group is a set of users that share a common value for the attribute `memberOf`. When you create a group, a new entry is added to the directory. Group entries include the object class `nsmanagedDeptAdminGroup`. For example, the following entry is located under `ou=Groups` in the Siroe organization.

```
dn: cn=Domain Administrators, ou=Groups, o=Siroe, o=ISP
objectClass: top
objectClass: groupOfUniqueNames
objectClass: nsManagedDeptAdminGroup
objectClass: inetAdmin
cn: Domain Administrators
adminRole: Domain Administrators
uniqueMember: uid=michael, ou=People, o=Siroe, o=ISP
```

When you add a user to a group, you are adding the group's name to the user's directory entry; the group name becomes a value for the attribute `memberOf`. For example, the following user entry is located in `ou=People` under the Siroe organization. The `memberOf` attribute indicates which groups the user belongs to. In this example, the user is a member of the Domain Administrators group.

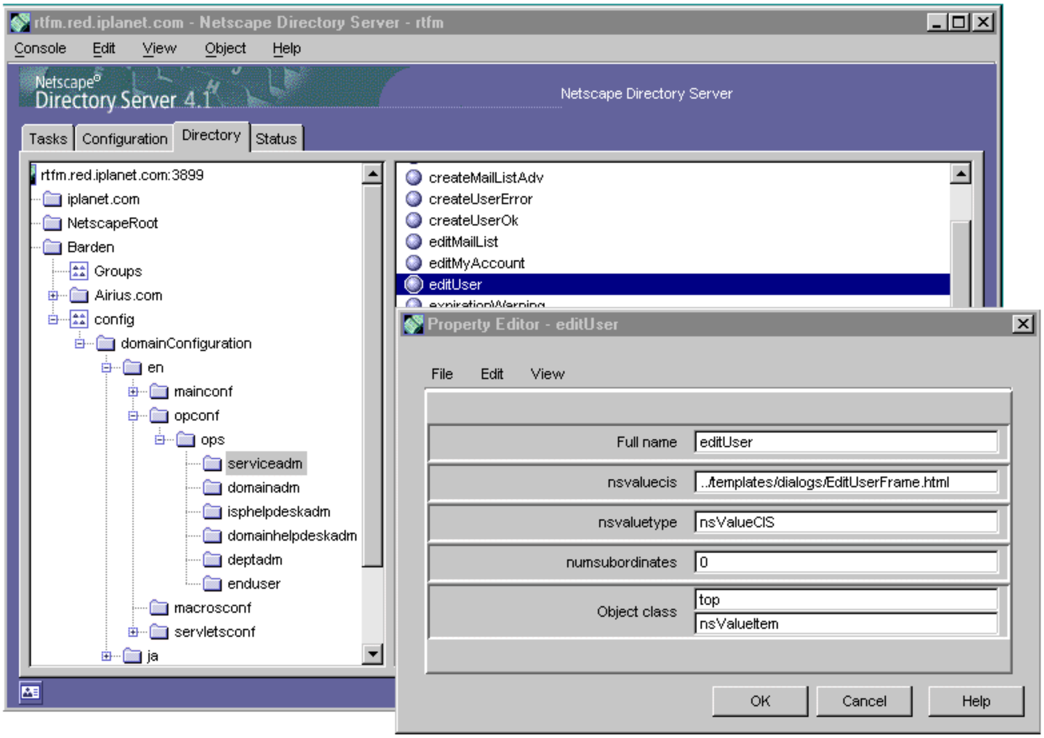
```
dn: uid=michael, ou=People, o=Siroe, o=ISP
objectClass: top
objectClass: person
objectClass: organizationalPerson
objectClass: inetOrgPerson
objectClass: nsManagedPerson
objectClass: mailRecipient
objectClass: nsMessagingServerUser
uid: michael
userPassword: morton
cn: Michael Morton
sn: Morton
givenName: Michael
telephoneNumber: 650.555.1212
mail: michael@Siroe.com
nsDADomain: Siroe
nsDACapability: mailListCreate
memberOf: cn=Domain Administrators, ou=Groups, o=Siroe, o=ISP
```

Figure 2-5 on page 34 illustrates the locations of the Siroe organization and the Organization Administrators' group in the default Delegated Administrator tree.

Configuration Branch

In the default Delegated Administrator base suffix, the configuration branch is located at the same level as the top-level organizations, although this is configurable during installation. In Figure 2-1 on page 24, the configuration branch is located at the same level as the default organization Siroe. It contains information about Delegated Administrator data types, servlets, macros, and operations mapping. You can see this information when you view the Directory Server through Netscape Console.

Figure 2-3 Use the Directory Server window to view Delegated Administrator configuration.



Full name: editUser

nsvaluecis: ../templates/dialogs/EditUserFrame.html

nsvaluetype: nsValueCIS

numsubordinates: 0

Object class: top
nsValueItem

Guidelines for Optimal Performance

While Delegated Administrator can handle millions of users, you can optimize search and page-handling performance if you design your directory tree using these guidelines:

- Delegated Administrator will easily handle a user directory with over 1,000,000 users. However, for best performance, iPlanet recommends that you plan for no more than 100 total organizations, and no more than 100 groups in a single organization.
- If possible, the directory tree should be designed with a minimal number of *hosting branches*. These are branches in the tree which have numerous hosted organizations beneath them. A flatter tree design requires fewer Delegated Administrator templates to be modified for use.
- Minimize the number of indexes within the directory server to just the indexes

which are going to be used. While it is possible to enable numerous attributes to search upon, this is not recommended. The maintenance of those additional attributes will have a negative impact upon performance.

- See the *Directory Server Deployment Guide* for more information about optimal performance and turning.

Provisioning a User Directory for the First Time

If you don't already have a directory deployed, you'll be installing Netscape Directory Server 4.12. You can use the Delegated Administrator tree as the base suffix in your new directory. Two groups of administrators are created at the top level of the tree. A default organization, named `Siroe`, was designed to help you get started right away. At the top-level of the Delegated Administrator suffix, the user `chris` is a member of the Service Administrators group. He can change the organization name, create new administrators, and create new organizations.

You can use the default tree whether yours is a hosting environment or an internal intranet. For example, Figure 2-4 illustrates how a hosting company might adapt the Delegated Administrator tree.

Figure 2-4 Delegated Administrator DIT in a hosting environment

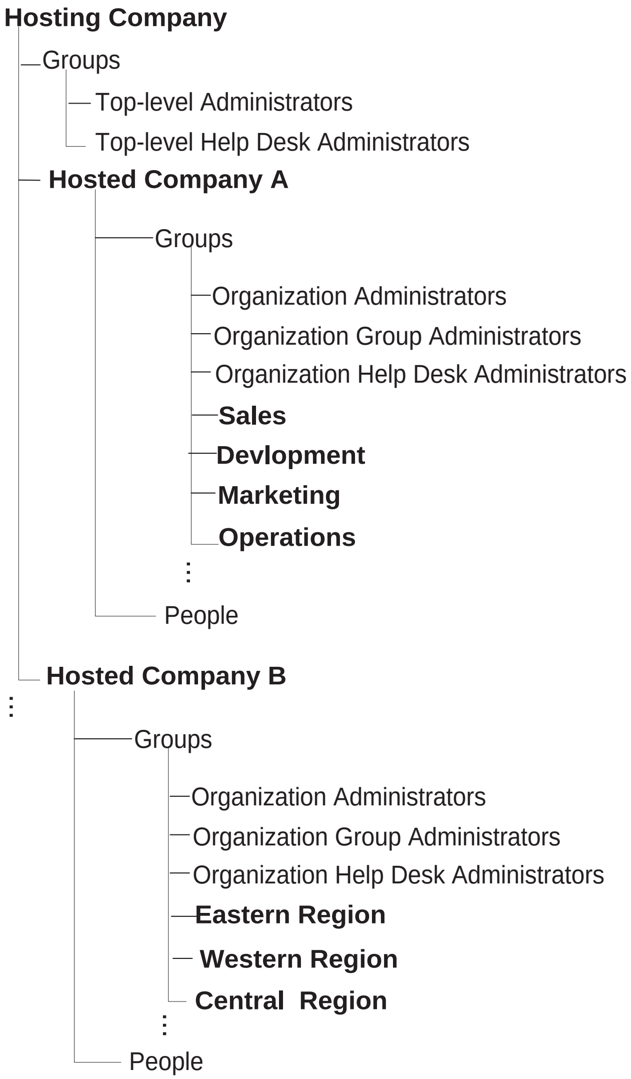
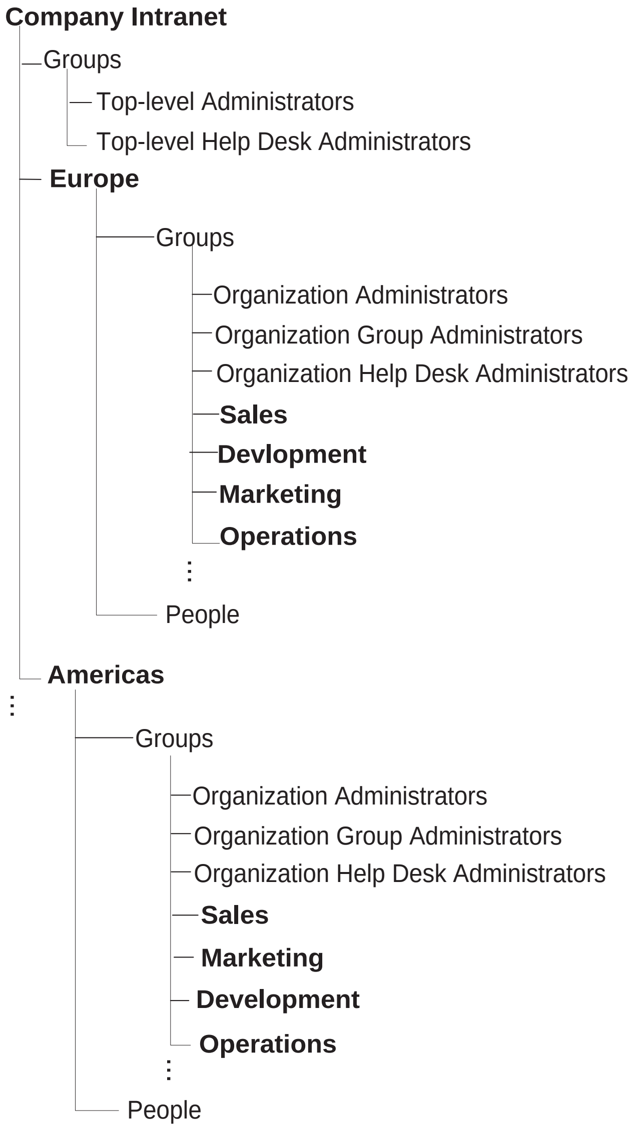

Hosting Company
Groups
Top-level Administrators
Top-level Help Desk Administrators
Hosted Company A
Groups
Organization Administrators
Organization Group Administrators
Organization Help Desk Administrators
Sales
Devlopment
Marketing
Operations
People
Hosted Company B
Groups
Organization Administrators
Organization Group Administrators
Organization Help Desk Administrators
Eastern Region
Western Region
Central Region
People

Figure 2-5 illustrates how a company might use the Delegated Administrator tree for its internal intranet. In any case, when provisioning your user directory for the first time, you should also follow the guidelines in the Directory Server *Deployment Guide*.

Figure 2-5 Delegated Administrator tree used in an intranet


Company Intranet
Groups
Top-level Administrators
Top-level Help Desk Administrators
Europe
Groups
Organization Administrators
Organization Group Administrators
Organization Help Desk Administrators
Sales
Devlopment
Marketing
Operations
People
Americas
Groups
Organization Administrators
Organization Group Administrators
Organization Help Desk Administrators
Sales
Marketing
Development
Operations
People

Using an Existing User DIT

If you’ve already deployed and provisioned a directory server, you’ll need to modify your existing DIT to include Delegated Administrator object classes, attributes, and Access Control Instructions (ACIs). Once you make the necessary changes, you can install Delegated Administrator and use it to add new organizations and suborganizations to your tree, create new administrators and administrator types. Depending upon your DIT, there may be additional customization work you have to do to make Delegated Administrator work with your directory.

For detailed information on reconciling your existing DIT and the Delegated Administrator DIT, see “Using an Existing User Directory” on page 363.

Upgrading an Existing Delegated Administrator Installation

When upgrading an existing instance of Delegated Administrator, you must reconcile your existing directory information tree (DIT) and the Delegated Administrator tree. Depending upon your existing DIT, this reconciliation may include:

- Modifying the user directory to include Delegated Administrator object classes, attributes, and Access Control Instructions (ACIs)
- Modifying Delegated Administrator attributes and ACIs to support your existing tree.
- If you’ve modified Delegated Administrator templates (the user interface), making those changes to the templates in the upgraded instance.
- Upgrading Delegated Administrator to version 4.5.

For detailed information on upgrading Delegated Administrator instances, see “Upgrading from Delegated Administrator Version 4.11” on page 387.

Flexible DIT Options

Delegated Administrator provides the means to create new containers and administrator roles in your directory. This makes it possible for you to design a tree that extends beyond the base suffix, or to adapt your existing user directory more easily to the Delegated Administrator tree.

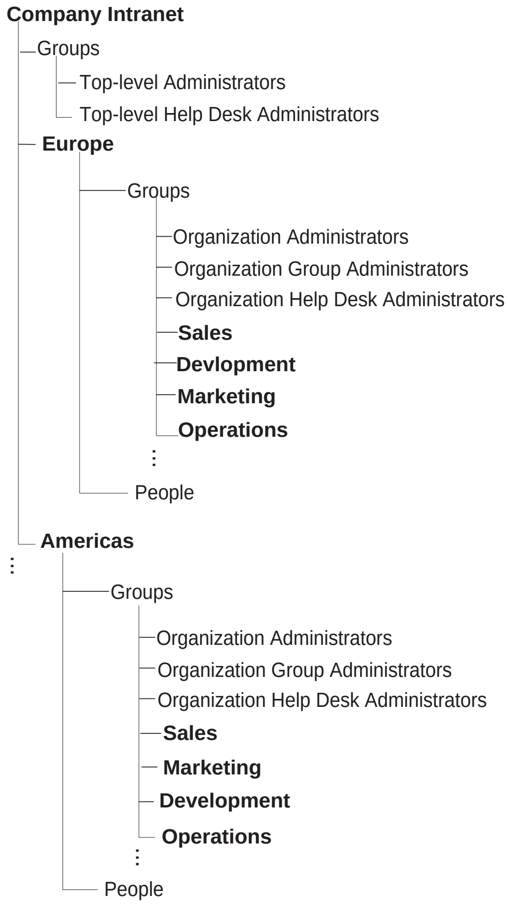
Nested Containers

The default Delegated Administrator tree uses a single level of organizations, and a single level of groups beneath each organization (see Figure 2-2 on page 26). However, you can add multiple levels of organizations and groups to the tree to meet your enterprise or hosting needs. A container can use any LDAP container attribute such as o, ou, or cn, as long as it conforms to these five rules:

- Each organization must include a container for user entries; groups cannot include containers for user entries.
- A group can be created beneath an organization.
- An organization can be created beneath an organization; it is called a *suborganization*.
- A group can be created beneath a group; it is called a *subgoup.*
- An organization cannot exist beneath a group.

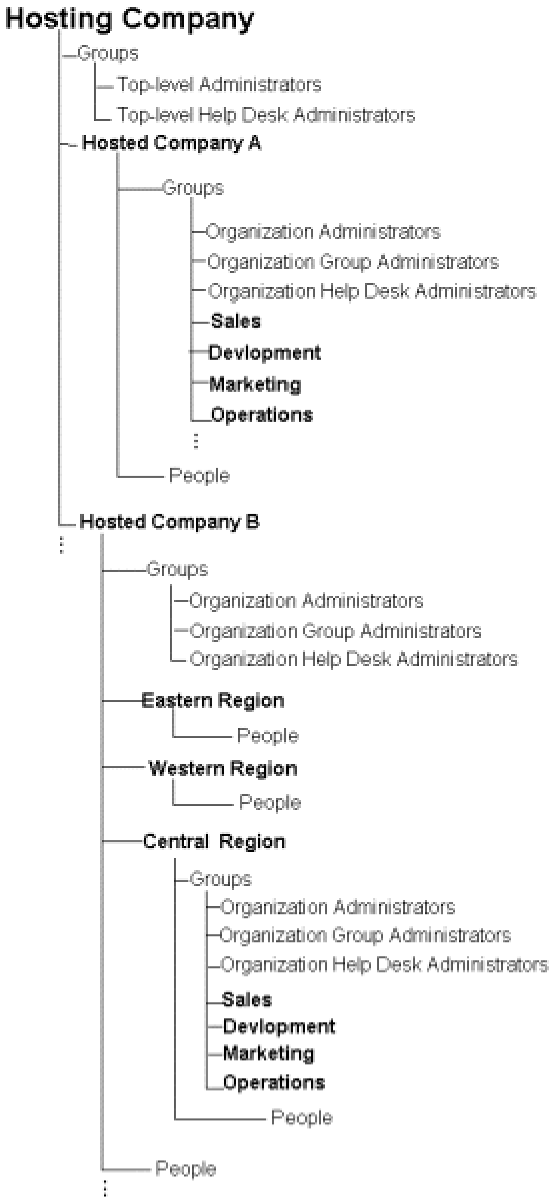
Whether you need to create nested containers depends upon your directory needs. For example, CompanyABC is a single company with offices worldwide. It's installing Directory Server for the first time, expressly for use with Delegated Administrator. It treats each of its office location as a separate operation. Although most day-to-day user lookups and data management happen within a single location, the CompanyABC must still be able to roll up financials and employee records for the entire company. CompanyABC easily adapts the Delegated Administrator default tree for its purposes.

Figure 2-6 This intranet uses Delegated Administrator default organizations and groups.


Company Intranet
Groups
Top-level Administrators
Top-level Help Desk Administrators
Europe
Groups
Organization Administrators
Organization Group Administrators
Organization Help Desk Administrators
Sales
Devlopment
Marketing
Operations
People
Americas
Groups
Organization Administrators
Organization Group Administrators
Organization Help Desk Administrators
Sales
Marketing
Development
Operations
People

CompanyXYZ hosts a number of companies, and uses an existing instance of Directory Server. Each company has its own unique tree structure, in some cases requiring multiple levels of organizations. Company XYZ uses Delegated Administrator to create suborganizations and subgroups that map to the existing directory instance (see Figure 2-7).

Figure 2-7 This hosting company created new suborganizations and subgroups to map to an existing user directory.


Hosting Company
Groups
Top-level Administrators
Top-level Help Desk Administrators
Hosted Company A
Groups
Organization Administrators
Organization Group Administrators
Organization Help Desk Administrators
Sales
Devlopment
Marketing
Operations
People
Hosted Company B
Groups
Organization Administrators
Organization Group Administrators
Organization Help Desk Administrators
Eastern Region
People
Western Region
People
Central Region
Groups
Organization Administrators
Organization Group Administrators
Organization Help Desk Administrators
Sales
Devlopment
Marketing
Operations
People
People

By default, both Top-level and Organizations Administrators can create organizations and suborganizations, groups and subgroups. Group Administrators can create only groups and subgroups.

Customized Administrator Types

The default Delegated Administrator types (Top-level, Organization, Help Desk, and Group) will meet basic directory needs. But you may find it necessary to modify one or more of these types, or to create a brand new type. For example, CompanyABC wants to restrict the access privileges of all Help Desk Administrators. After modifying the administrator type, the Help Desk Administrator will be able to initiate the edit password procedure, but he will not be able to access the password the user enters during the procedure. In this case, Company ABC modifies the Help Desk Administrator type by extending the SetPassword functionality.

In another example of customization, CompanyABC creates a new suborganization. Since Delegated Administrator does not have a Suborganization Administrator group, CompanyABC creates a new administrator type. For detailed information on creating new administrator types, see Chapter 14, “Customizing Configuration in the Directory.”

Options to Consider Before Installation

Before you begin to install Delegated Administrator, you should have a clear vision of the optional features you want to implement. The following custom configurations require the use of other servers working with Delegated Administrator, and may take extra preparation or time to deploy.

Directory Server Configuration and User Data

During installation, you’ll be asked to specify locations for two types of directory information: configuration data and user data. Delegated Administrator will store information about its datatypes, servlets, macros, and operations mapping in the configuration branch of the Directory Server. When you modify user and group information in Delegated Administrator, those changes are made in the user directory.

Both configuration directory and user directory must exist on the same computer system. If Delegated Administrator is configured to use a configuration suffix that differs from the user suffix, Top-level and Organization Administrators can not access the configuration files.

If you're deploying Directory Server with Delegated Administrator for the first time, follow the guidelines regarding directory configuration in the Directory Server *Deployment Guide*.

Optimizing Directory Searches

When performing a generic or too broadly defined search on a large directory, Delegated Administrator will time out. You can optimize Delegated Administrator page handling and search performance by modifying the Directory Server configuration. The following measures are necessary when any organization in your directory exceeds 5000 users:

- Add indexes for the *`nsdadomain`*, *`memberof`*, and `uid` attributes.
- Reset the `lookthroughlimit parameter`.
- Reset `sizelimit` parameters.
- Set the All ID Threshold value appropriately.

See "Chapter 3, “Basic Installation and Configuration" in the Delegated Administrator Deployment and Customization Guide for further instruction.

Messaging Server Support

You can configure Delegated Administrator so that when you create a user account, Messaging Server-related attributes are added to user's entry in the directory. This makes it possible for Messaging Server to deliver mail to the user. Delegated Administrator provides three levels of support for Messaging Server. During Delegated Administrator installation, you must choose one of the following:

- **No Messaging Server**
  Choose this option if you do not intend to use Netscape Messaging Server or iPlanet Messaging Server. For example, choose this option if you are using a different brand of server, or if you do not use Directory Server for managing Messaging Server configuration.

- **Netscape Messaging Server 4.1**
  Choose this option if you already have Messaging Server 4.1 deployed, or are planning to install it with Delegated Administrator.
- **iPlanet Messaging Server 5.0**
  Choose this option if you already have Sun Internet Messaging Server 4.x installed, or if you are planning to install iPlanet Messaging Server 5.0.

Although you don't have to have Messaging Server already installed, you'll save yourself a few steps later on if you can enter the Messaging Server URL during Delegated Administrator installation. After installing Delegated Administrator, you must configure the Messaging Server so the two will work together. For detailed information, see "Enabling Optional Features" on page 71.

NOTE Messaging Server does not support LDAP over an SSL connection at this time.

Certificate-based Authentication

Certificate-based authentication is a means of confirming a user's identity before allowing the user access to Delegated Administrator. When you configure Delegated Administration for certificate-based authentication, Administrators and End Users log in using digital certificates instead of user names and passwords. This provides an extra measure of security for your directory.

Certificate-based authentication is part of the Secure Sockets Layer (SSL) protocol. It requires the use of a Certificate Server—your own or one belonging to a trusted Certificate Authority. You should have a thorough knowledge of SSL and some experience using Certificate Server before attempting to enable this feature.
See "Enabling Optional Features" on page 71 for more information.

Class of Service

Class of Service (CoS) is an LDAP feature that enables you to manage a group of attributes that describe a category or *class* of service. Once you've defined the attributes and created the new classes in the directory, you can automatically assign a class of service to selected user entries. This eliminates having to store all service-related attributes in each user entry in the directory. It also makes it easier to make changes when necessary. If a class of service changes, you need only change its attributes in the class definition. You don't have to change the attribute values in each user entry.

Setting up this feature requires a special directory plugin. The Class of Service plugin is automatically installed when you install Delegated Administrator, but needs to be configured before it can be used. Detailed instructions are in "Step 2: Configure the Directory Server Plug-ins" on page 53.

Other Configuration Options

While planning your deployment, you should also consider a number of options that can be enabled after installing Delegated Administrator. You'll find detailed information about each of the following options in Chapter 4, "Enabling Optional Features." Topics include:

- Secure Sockets Layer (SSL)
- User ID Uniqueness
- User Directory Failover
- Password Reset Policy
- Single Sign-On with Netegrity SiteMinder

Implications of Customizing Delegated Administrator

You can customize Delegated Administrator in three ways:

- Modify templates.
- Modify the directory configuration.
- Extend the servlet functionality.

As you plan your Delegated Administrator deployment, be sure to think through the impact of your planned changes.

Modifying the templates. Many changes to the user interface require only minor changes in the template's HTML code. For example, to change a field in the Search interface, you need only copy a few lines of HTML code from an existing field, and paste them into an HTML template file. There are no back-end changes to make.

However, your modified template may cause inconsistencies throughout the user interface that you'll want to address. For example, any time you add an input field to the user interface, you may want the information that you entered into that field to display in other parts of the interface. You'll have to modify related templates, and perhaps also modify Help file that corresponds to each template you modify.

Modifying the directory configuration. Each time you add nested containers, or create a new administrator role, you'll be modifying ACI's and directory schema. These changes require changes in the directory configuration, more far-reaching than changes to the user interface. Additionally, you'll also have to create new templates that correspond to the Administrator or container.

Extending servlet functionality. Extending a servlet requires writing additional servlet code. For example, by default, the Help Desk Administrator has access privileges to read and write users' passwords. CompanyABC wants to customize the Help Desk Administrator role so that he can initiate setting the password, but cannot actually read the password that the user enters.

Since the servlet already exists, CompanyABC can simply extend the servlet functionality. You accomplish this by extending the base class, NDAServlet, and implementing the execute() method. The ACI entries for the Help Desk Administrator must also be modified.

If you're thinking of customizing Delegated Administrator at all, you should read Part 4, "Customizing Delegated Administrator," on page 285 of this manual.

Part 2

Installation & Configuration

Chapter 3, “Basic Installation and Configuration”

Chapter 4, “Enabling Optional Features”

Chapter 5, “Certificate-Based Authentication”

Chapter 3

Basic Installation and Configuration

This chapter provides instructions for installing and configuring Delegated Administrator to support the default directory information tree that ships with the product.

This chapter incldues the following sections:

- System Requirements
- Before You Begin
- Step 1: Install or Upgrade to iPlanet Directory Server 4.12.
- Step 2: Configure the Directory Server Plug-ins.
- Step 3: Configure the Directory Server
- Step 4: Install or Upgrade to iPlanet Web Server 4.1
- Step 5: Create a Web Server Instance
- Step 6: (Optional) Install or Upgrade to Netscape Messaging Server 4.1
- Step 7: Install Delegated Administrator
- Step 8: Configure Netscape Messaging Server
- Step 9: (Optional) Disable Anonymous Access to Your User Tree
- Getting Started
- Uninstalling Delegated Administrator

System Requirements

This section describes the minimum hardware and software requirements for installing and using Delegated Administrator 4.5.

Server Requirements

Web Server 4.1 and Delegated Administrator 4.5

Delegated Administrator and iPlanet Web Server 4.1 must be installed on the same computer system and must run a on supported platform (see Table 3-1). iPlanet highly recommends using Web Server 4.1 SP7, although versions 4.1 with SP2 through SP5 are also supported. To determine which patches you need, see the Web Server Release Notes at: http://docs.iplanet.com/docs/manuals/enterprise/41/rn41sp7.html#19292.

Delegated Administrator by itself requires a minimum of 20MB disk space after installation. An additional 5MB is required for each customized or localized organization you add to the Delegated Administrator tree. For example, you could add Organization A and Organization B under the Delegated Administrator root. If you then create a French version and an English version for each of these organizations, the result is a total four localized organizations. This would require 20MB additional disk space.

Directory Server 4.12

Netscape Directory Server 4.12 must be installed and running; it does not have to be installed on the same computer system as Delegated Administrator. In addition to the minimum system requirements for the server, the Directory Server host computer must have 200MB disk space free when preparing an empty directory for use with Delegated Administrator.

For complete Netscape Directory Server 4.12 installation requirements, see the Directory Server *Release and Installation Notes* available at

`http://home.netscape.com/eng/server/directory/4.12/installation.html.`

Supported Platforms

Table 3-1summarizes the hardware requirements for installing Delegated Administrator with iPlanet Web Server, Enterprise Edition 4.1 with SP2.

Table 3-1 Supported Platforms.

Vendor	Architecture	Operating System	Minimum Memory (RAM)	Minimum Disk Space After Installation
Sun	SPARC	Solaris 2.6, 2.8	128 MB	150 MB (300 MB during installation)
Hewlett-Packard	HP9000	HP-UX 11.0	128 MB	150 MB (300 MB during installation)
IBM	RS/6000	AIX 4.3.3	128 MB	150 MB (300 MB during installation)
Microsoft	Pentium	Windows NT 4.0 with SP5	128 MB	150 MB (300 MB during installation)

Additional System Requirements for Windows NT 4.0

- Paging space at least as large as the amount of RAM (twice the amount of RAM is recommended).
- 30 MB free disk space for the log files (for approximately 300,000 accesses per day).
- If you plan to run more than two separate instances of Web Server on the same computer system, each server will require an additional 16 MB RAM.

Software Compatibility

Delegated Administrator 4.5 works with the following servers and software:

- Required— iPlanet Web Server 4.1 with appropriate patches. See "Server Requirements" on page 48 for more information.
- Required—Netscape Directory Server 4.12
- Required—A browser such as Netscape Communicator or Microsoft Internet Explorer. See Table 3-2 for supported browser versions.
- Netscape Messaging Server 4.1x
- iPlanet Certificate Management System 4.1, 4.2
- Netegrity SiteMinder 4.0

Web Browser Requirements

Administrators and end users will use web browsers to perform user management tasks. Table 3-2 summarizes the web browsers supported for Delegated Administrator.

Table 3-2 Supported Browsers.

Operating System	For Administrators	For End Users
Unix	Netscape Communicator 4.72 Microsoft Internet Explorer 4.0 or 5.0	Netscape Communicator 4.51 or higher Microsoft Internet Explorer 4.0 or higher
Windows NT 4.0	Netscape Communicator 4.72 Microsoft Internet Explorer 4.0 or 5.0	Netscape Communicator 4.08 or higher Microsoft Internet Explorer 4.0 or higher

Before You Begin

Before you can install Delegated Administrator, you'll need to resolve the following:

- iPlanet Directory Server 4.12 and Web Server 4.1 with Service Pack 2 must be installed, configured, and running. Table 3-3 summarizes the installation steps you must take and where to find the detailed instructions you'll need in order to install these servers.
- If you plan to use a Directory Server that is already deployed and provisioned with users and groups, you must modify its entries to match the Delegated Administrator objectclasses and attributes. For detailed information, see Appendix , "Using an Existing User Directory."
- If you plan to use Netscape Messaging Server, you'll need to create a postmaster group and reconfigure the server. See "Step 8: Configure Netscape Messaging Server" on page 61 for more information.

Table 3-3 Summary of Delegated Administrator Installation Procedures

Installation Step	Where to Find Detailed Instructions
1. Install or upgrade to iPlanet Directory Server 4.12.	In this manual, see "Step 1: Install or Upgrade to iPlanet Directory Server 4.12" on page 52. For detailed Directory Server installation instructions, *Release and Installation Notes*, available at `http://home.netscape.com/eng/server/directory/4.12/`
2. Configure Directory Server plug-ins.	In this manual, see "Step 2: Configure the Directory Server Plug-ins" on page 53.
3. Configure Directory Server.	In this manual, see "Step 3: Configure the Directory Server" on page 55.
4. Install or upgrade to iPlanet Web Server 4.1.	During installation, you do not have to specify a Directory Server. For detailed installation instructions, see *Web Server 4.1 Installation Guide*, available at `http://docs.iplanet.com/docs/manuals/enterprise.html#41`
5. Create a new Web Server instance.	For detailed instructions, see *WebServer 4.1 Administrator's Guide*, `http://docs.iplanet.com/docs/manuals/enterprise.html#41`

Table 3-3 Summary of Delegated Administrator Installation Procedures *(Continued)*

Installation Step	Where to Find Detailed Instructions
6. (Optional) Install Netscape Messaging Server 4.1x.	During installation, when prompted for Directory Server information, specify your Directory Server 4.12 installation. For detailed instructions, see *Messaging Server 4.1 Administrator's Guide*, `http://docs.iplanet.com/docs/manuals/messaging.html#nms41`
7. Install or upgrade to Delegated Administrator 4.5.	For detailed instructions, see "Step 4: Install or Upgrade to iPlanet Web Server 4.1" on page 57 of this manual.
8. If using Netscape Messaging Server, create a postmaster account and modify the server configuration.	In this manual, see "Step 8: Configure Netscape Messaging Server" on page 61.
9. (Optional) Disable Anonymous Access if necessary.	For detailed information, in this manual, see "Step 9: (Optional) Disable Anonymous Access to Your User Tree" on page 64.
10. Access the Start Page to start using Delegated Administrator.	Delegated Administrator provides a Start Page to help you log in for the first time, and sample data that you can use to test and evaluate the program. For detailed information, in this manual, see "Getting Started" on page 67.

Step 1: Install or Upgrade to iPlanet Directory Server 4.12

If you do not have a directory server installed, you must install iPlanet Directory Server 4.12 now. If you already have a pre-4.12 directory server installed, you must upgrade to version 4.12. Follow the instructions in the *Release and Installation Notes*, available at `http://home.netscape.com/eng/server/directory/4.12/`. After you've followed the instructions in the *Release and Installation Notes*, return to this manual and continue with Step 2: Configure the Directory Server Plug-ins, below.

Step 2: Configure the Directory Server Plug-ins

Before you can install Delegated Administrator, you must configure four plug-ins that Delegated Administrator uses. The plug-ins are automatically installed for you when you install Directory Server 4.12.

Flexible Attribute Uniqueness. This plug-in enforces the uniqueness of an attribute within a subtree.

Class of Service. This plug-in determines a user's specific configuration values and resource limits based on a Class of Service attribute in the user entry.

Directory Entry Counts. This plug-in automatically maintains count values for organizations, groups, or users that are added to or deleted from the directory.

Referential Integrity Check. This plugin ensures that relationships between related entries are maintained.

To Configure the Directory Server Plug-ins

1. Stop the Directory Server.

2. In each instance of Directory Server that you plan to use with Delegated Administrator, modify the following file (where `<NSHOME>` is the Directory Server root):

   ```
   <NSHOME>/slapd-<host_identifier>/config/slapd.ldbm.conf
   ```

   a. Locate the line that begins with:

   ```
   plugin postoperation on "referential integrity postoperation"
   ```

   b. Add `member of` to the end of the line. For example (all one line):

   ```
   plugin postoperation on "referential integrity postoperation"
   /export2/brighton/ds412/lib/referint-plugin.so
   referint_postop_init 0
   /export2/brighton/ds412/slapd-rtfm/logs/referint 0 member
   uniquemember owner seeAlso memberof
   ```

   c. If your DIT is used in a hosting environment, perform this step to disable the UID Uniqueness plug-in. When this plug-in is disabled, you can have individuals with the same uid in different organizations. If your DIT is not used in a hosting environment, skip to step 2c.

   To disable the plugin, insert a comment character at the beginning of the following line:

   ```
   plugin preoperation on "uid uniqueness"
   ```

```
<Directory_root>/lib/uid-plugin.so NSUniqueAttr_Init uid
o=iplanet.com
```

d. If you want to enable the Class of Service feature, uncomment the following lines by deleting the pound sign (#) at the beginning of the lines:

```
#plugin postoperation on "Class of Service"
<Directory_root>/lib/cos-plugin.so cos_init o=iplanet.com

#plugin preoperation on "Class of Service init"
<Directory_root>/lib/cos-plugin.so cos_preop_init
```

If the above two lines are missing, add them to the file without the comment characters.

Initial configuration of Class of Service Directory Server Plugins causes the error message "plugin init failed". This is normal behavior. It is simply stating that there are no Class of Service definitions in the directory at the time.

e. If the following line exists in the file, be sure it is commented out:

```
#include
"<Directory_root>/slapd-rtfm/config/counters.ldbm.conf"
```

f. Add the contents of this file:
`<Directory_root>/slapd-<identifier>/config/counters.ldbm.conf`

3. Start the Directory Server.

Step 3: Configure the Directory Server

In this step, modify the Directory Server configuration and user entries to meet your needs. Optimizing page handling and search performance is recommended, but not required, for all Delegated Administrator installations. Modifying the user entries is absolutely required if you've already provisioned your directory with users and groups.

Optimizing Page Handling and Search Performance

You can optimize Delegated Administrator page handling and search performance by modifying the Directory Server configuration. The following measures are necessary when any organization in your directory exceeds 4000 users.

- Add indexes for the `nsdadomain`, `memberof,` and `uid` attributes.
- Reset the `lookthroughlimit` parameter.
- Reset `sizelimit` parameters.
- Set the All ID Threshold value appropriately.

To add appropriate indexes to your Directory:

1. Using Netscape Console, in the Directory Server window, select the Configuration tab and then click the Database icon.
2. Select the Indexes tab in the right pane.
3. To add the `nsdadomain` attribute, click Add Attribute, and then do the following.
   a. In the Select Attributes window, select the `nsdadomain` attribute and then click OK.
   b. In the Additional Indexes list, select the `nsdadomain` attribute and then check the boxes for Equality, Presence, and Substring.

4. To add the `memberof` attribute, click Add Attribute, and then do the following:

   a. In the Select Attributes window, select the `memberof` attribute and then click OK.

   b. In the Additional Indexes list, select the nsdadomain attribute and then check the boxes for Equality, Presence, and Substring.

5. To add a substring index for the `uid` attribute, in the Additional Indexes list, select the `uid` attribute. Then check the boxes for Equality, Presence, and Substring.

6. Click Save.

To reset the lookthroughlimit:

1. Using Netscape Console, in the Directory Server window, select the Configuration tab and then select Database in the left pane.

2. Select the Performance tab in the right pane.

3. In the Look Through Limit field, enter a number greater than the number of entries that the Directory Server will check in response to a search request.

4. Click Save.

To reset the sizelimit parameter:

1. Using Netscape Console, in the Directory Server window, select the Configuration tab and then select the root entry in the navigation tree in the left pane.

2. Select the Performance tab in the right pane.

3. In the Size Limit field, enter -1.

4. Click Save.

Setting the All IDs Threshold Value

By default, the directory server is set to an All IDs threshold of 4000. For Delegated Administrator, this value should be just higher than the number of users in your directory. For detailed information on changing this value, see the *Directory Server Administrator's Guide* at the following URL:

```
http://home.netscape.com/eng/server/directory/4.1/admin/index1.htm#
1053642
```

Modifying an Existing User Directory

If you have already deployed Netscape Directory Server and provisioned it with users and groups, you must modify your user directory tree before going any farther with installation. If you have already deployed Netscape Directory Server, but have not installed Delegated Administrator 4.51 to work with it, follow the instructions in Appendix , “Using an Existing User Directory.” After you’ve modified your directory tree, return to this manual and continue with Step 4 below.

Step 4: Install or Upgrade to iPlanet Web Server 4.1

iPlanet Web Server 4.1 and Delegated Administrator must be installed on the same computer system. If you do not have iPlanet Web Server 4.1 installed, install it now. If you have a pre-4.1 Web Server installed, you must upgrade the server to the 4.1 version. Follow the instructions in the *Web Server 4.1 Installation Guide*, available at `http://docs.iplanet.com/docs/manuals/enterprise.html#41`. During installation, you do not have to specify a Directory Server when prompted for one.

NOTE The system users for both Web Server and Delegated Administrator must be the same. To remedy the conflict in a Unix installation of Delegated Administrator you must change the ownership of two `resource.properties` files to nobody. These files are located in the Delegated Administrator Server root directory.

To Make the System Users for Web Server and Delegated Administrator the Same

1. In the directory `nda/classes/netscape/nda/pagegen/`, at the command line, enter:
   `chown nobody resource.properties`.

2. In the directory `nda/classes/netscape/nda/servlet/`, at the command line, enter:
   `chown nobody resource.properties`.

Step 5: Create a Web Server Instance

For best results, you should create a new instance of Web Server to work with Delegated Administrator. Follow the instructions in the *Web Server 4.1 Administrator's Guide*, available at `http://docs.iplanet.com/docs/manuals/enterprise.html#41`.

Step 6: (Optional) Install or Upgrade to Netscape Messaging Server 4.1

If you don't have Messaging Server installed, installing it now will save you a step later as you install Delegated Administrator. If you have a pre-4.1 Messaging Server already installed, you must update it to version 4.1 before installing Delegated Administrator. See the *Messaging Server 4.1 Installation Guide*, available at `http://docs.iplanet.com/docs/manuals/messaging.html#nms41` for detailed information.

Step 7: Install Delegated Administrator

Before you can install Delegated Administrator, you must install Directory Server and Web Server, and resolve related server issues. See "Before You Begin" on page 51.

To install Delegated Administrator:

1. Run the Delegated Administrator install program.
   - In Unix, in the Delegated Administrator root, enter `./setup`.
   - In Windows NT, in the Delegated Administrator directory, double-click the self-extracting icon.
2. When prompted, enter the following:

   Would you like to continue with setup? Enter `Yes`.

   Do you agree to the license terms? Enter `Yes`.

   Install location: Enter the path to the directory where Delegated Administrator will be installed.

Select one of the following options:

- **No Messaging Server Support**
  Select this option if you do not intend to use Delegated Administrator with a messaging server.
- **Support for Netscape Messaging Server**
  Select this option if you intend to use Delegated Administrator with Netscape Messaging Server 4.1x.

If you selected "No Messaging Server Support" above, skip to **Specify Enterprise Server configuration directory.**

If you selected "Support for Netscape Messaging Server, Delegated Administrator prompts you for the following:

- **Manage Messaging Server?** This step is optional. If you intend to use Delegated Administrator with either Netscape Messaging Server 4.1, the setup program can store the appropriate Administration Server URL for future reference. Enter `Yes`.
- **Specify Host Name:** Enter the fully qualified host name the Administration Server that manages the Messaging Server.

  Example: `miriam.mcom.com.` If you don't know this information at the time of installation, you can enter it later. See "To Configure Delegated Administrator to Work with Messaging Server" on page 63.
- **Specify Admin URL:** Enter the fully qualified host name and port number of the Administration Server that manages the Messaging Server.

  Example: `http://miriam.mcom.com:400`. If you don't know this information at the time of installation, you can enter it later. See "To Configure Delegated Administrator to Work with Messaging Server" on page 63

Specify Enterprise Server configuration directory: Enter the path to the directory that contains the file `magnus.conf`.

Specify LDAP URL: Enter the URL to the instance of Directory Server you're using with Delegated Administrator. Use the following form:

`ldap://<host_name>:<port_number>`

Example: `ldap://siroe.mcom.com:8000`

Specify Directory Manager: Enter the DN of the user with Directory Manager privileges on the configuration directory.

Password: Enter the Directory Manager password you used when you installed the Directory Server.

NOTE	In this next part of the installation program, you are asked twice to specify a suffix: one for user data, and one for configuration data.

Specify Suffix: Enter a base suffix using the form `o=<your_suffix>`.

Delegated Administrator requires a suffix to store its user data. Examples: `o=ISP` or `dc=ISP, dc=com`

All organizations, groups, and user to be managed by Delegated Administrator will be created under this base suffix.

- If you specify a suffix in an existing Delegated Administrator 4.5 user tree, no new user information will be written into that tree at this time. The installation program will continue.
- If you specify a suffix in a pre-4.5 Delegated Administrator user tree, or in an existing DIT, the installation program will not allow you to continue. You'll be asked to update your directory entries to include Delegated Administrator 4.5 objectclasses and attributes. For more information, see "Using an Existing Directory Tree." This document will be available at the location where you downloaded Delegated Administrator.

Specify Suffix: Delegated Administrator requires a suffix to store its configuration data. Enter a base suffix using the form `o=<your_suffix>`

Examples: `o=ISP` or `dc=ISP, dc=com`

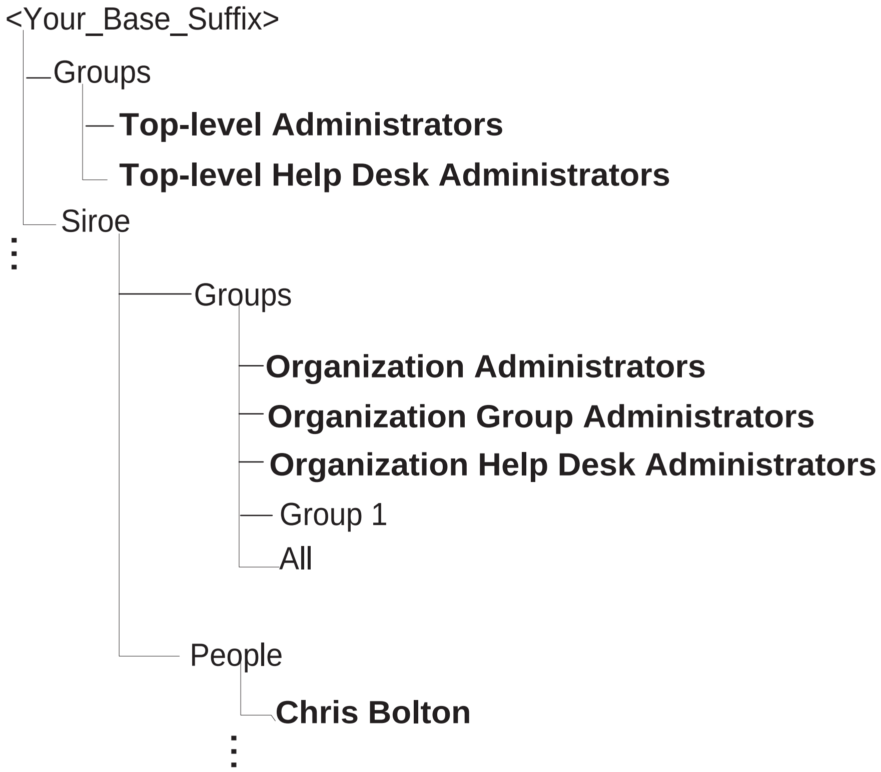
Delegated Administrator automatically creates a new base suffix for you containing the following default directory entries and their respective ACIs:

- One Top-level Administrators group
- One Top-level Help Desk Administrators group
- One Organization named `Siroe`
- One users group named `Group 1`
- Six user accounts

3. When prompted, press Enter to continue and exit the installation program.

   Figure 3-1 illustrates the base suffix that Delegated Administrator creates at installation. In the figure, the user `Chris Bolton` is a member of the Service Administrators group and can create new administrators and new organizations.

Figure 3-1 Delegated Administrator automatically creates a base suffix with default data you can use to get started.


<Your_Base_Suffix>
Groups
Top-level Administrators
Top-level Help Desk Administrators
Siroe
Groups
Organization Administrators
Organization Group Administrators
Organization Help Desk Administrators
Group 1
All
People
Chris Bolton

Step 8: Configure Netscape Messaging Server

Messaging Server will not recognize the Delegated Administrator base suffix until you create a postmaster group and change the Messaging Server configuration.

Creating a Postmaster Group

Create a postmaster group in the base suffix you specified when you installed Delegated Administrator. In Netscape Console, when you click the Users and Groups tab, the current base suffix is displayed. If the Delegated Administrator base suffix is not displayed, you must change to the appropriate directory. To change to the Delegated Administrator Directory, click Directory.

To create a postmaster group:

1. In Netscape Console, in the Users and Groups tab, use the drop-down list in the lower-right corner to choose New Group. Then click Create.
2. In the Select Organizational Unit window, choose Base DN, and then click OK.
3. In the Create Group window, in the Group Name field enter `Postmaster`.
4. Click the Account tab, and then click the Mail Account checkbox until a checkmark is displayed. After a moment, the Mail tab is added to the window.
5. Click the Mail tab. Enter a primary email address using the form `postmaster@<your_host>.<your_domain>`.
6. Click OK.

Changing the Messaging Server Configuration

Once you change the configuration, Messaging Server will recognize the mail accounts for any users you create.

To Configure Messaging Server to Work with Delegated Administrator

1. In Netscape Console, open the Messaging Server window.
2. In the Messaging Server window, click the Configuration tab, and in the navigation tree click Services.

3. Click the LDAP tab. In the section "LDAP connection for user lookup," select "Use messaging server specific directory settings." Verify the following Directory Server information, and modify the Base DN:

   Host name: Displays the name of the computer where the Directory Server is installed.

   Port number: Displays the port number for the Directory Server.

   Base DN: Enter the base suffix you used when you installed Delegated Administrator. Example: o=ISP

   Bind DN: Displays the Distinguished Name (DN) for the user who has appropriate permissions to make changes to the configuration directory.

4. Click Change Password, and then change the password for the Bind DN.

5. Click Save. In the Restart Services window, click to select "Restart all services now."

6. Click Restart.

To Configure Delegated Administrator to Work with Messaging Server

You need to perform this step only if you did not specify the Messaging Server URL when you ran the installation program for Delegated Administrator.

1. In the Delegated Administrator root, locate the following file:

   ```
   ...nda/classes/netscape/nda/servlet/resource.properties
   ```

2. Modify the following line to include the fully qualified host name the of Administration Server that manages the Messaging Server:

   ```
   MsgSvr0-name=<server_identifier>
   ```

   Example: `MsgSvr0-name=miriam.mcom.com`

3. Modify the following line to include the fully qualified host name and port number of instance of Administration Server that manages the Messaging Server:

   ```
   MsgSvr0-adminurl=http://<host_name>:<port_number>
   ```

   Example: `http://miriam.mcom.com:400`.

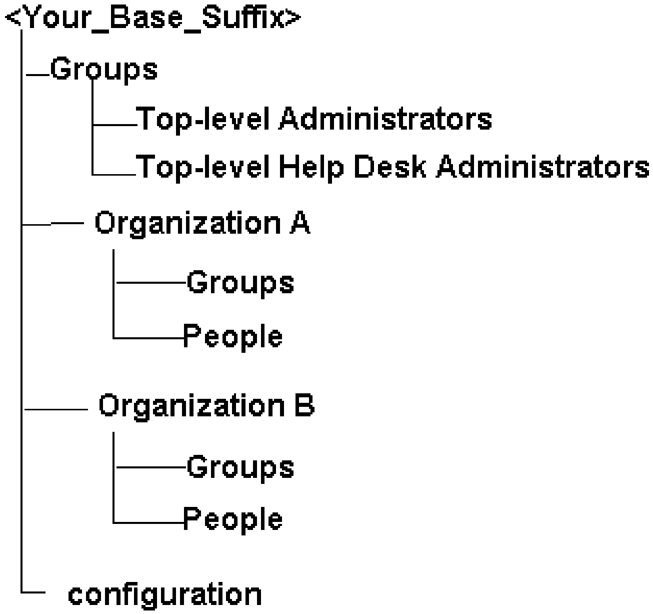
Step 9: (Optional) Disable Anonymous Access to Your User Tree

By default, Delegated Administrator uses a special Access Control Instruction (ACI) for *anonymous access*. Anonymous access allows any user to search all user entries in the directory. Many applications that use Directory Server data cannot work without anonymous access.

However, Delegated Administrator customers who provide internet service to multiple companies may want to disable anonymous access. When you disable anonymous access, for example, users in organization A can search the user directory and never see users in organization B; users in organization B will never see the users in organization A.

You can disable anonymous access by running a script provided for you in the `<DelegatedAdmin_root>/nda/ldif` directory. The script removes the ACI which allows anonymous access.

Figure 3-2 By default, anonymous access is enabled and users in organization A can see users in organization B.



To Disable Anonymous Access

1. If you've installed Delegated Administrator using the default base suffix (`o=ISP`), skip to Step 3.

2. In the file `<DelegatedAdmin_root>/nda/ldif,`change the base suffix `o=ISP` to your base suffix as appropriate.

3. In the Directory Server, in `<NSHOME>/shared/bin`, execute `ldapmodify` with the `anon.ldif` file.

   For example, you can enter:

   ```
   ldapmodify -h <host> -p <port> -D "cn=directory manager" -w
   <password> -f <DelegatedAdmin_root>/nda/ldif/anon.ldif
   ```

Changing the NDAUser Password

Delegated Administrator uses the NDAUser entry under `ou=config` for resolving uids at login. You can change the password for this user as an added security measure.

To change the password for the NDAUser:

1. Go to the directory where the file `resource.properties` is stored:

   ```
   <DelegatedAdmin_root>/nda/classes/netscape/nda/servlet/
   ```

2. In the file `resource.properties`, change the password for the following entry:

   ```
   NDABasicAuth-uidrespw=auth
   ```

   Be sure that only authorized personnel have access to this password!

3. Use ldapmodify to change the password for the NDAUser entry. In the directory `<DirectoryServer_root>/shared/bin`, enter the following:

   ```
   ldapmodify -h <host_name> -p <port_number> -D "cn=directory
   manager" -w <password>
   ```

4. At the prompt, enter the following:

   ```
   dn: uid=NDAUser, ou=config, o=<base_suffix>

   changetype: modify

   replace: userpassword

   userpassword: <newpassword>
   ```

5. To complete the command:
   - On Unix, enter `<Ctrl-D>.`
   - On Windows NT, enter `<Ctrl-Z>.`
6. Restart Web Server.

Silent Installation

If you plan to install more than one instance of Delegated Administrator, you can save a cache file that contains all of the parameters you specify during the first installation. Then, after you've installed Delegated Administrator once, you can use the cache file to quickly install additional Delegated Administrator instances. All of your responses to the installation prompts are recorded in the cache file. When you use a cache file in a new installation you are not asked any questions. Instead, all of the cache file responses are automatically applied as the new installation parameters. This type of installation is known as *silent installation*.

Saving the Cache File

To save the cache file, you must run the installation program with the -k command line option.

Examples:

Windows NT. Choose Run, and then enter `setup -k`.

DOS command line. Enter `setup -k`.

Unix. Enter `setup -k`.

The cache file from an installation is saved with the name `install.inf` in the server-root/setup directory. For example, if you installed the server into `/home/deladmin`, the cache file for that installation is: `/home/deladmin/setup/install.inf`.

To Use the Cache File for Installation

1. Copy the `install.inf` cache file to the installation directory that you are using for the new installation.
2. Review and edit the install.inf cache file as necessary.

   You will probably want to change some of the parameters and specifications in the cache file. For example, the host name for this installation will likely be different than the host name recorded in the cache file. Remember that the parameters listed in the cache file will be automatically applied to this installation.
3. Run setup with the `-s -f` filename options. The filename is the full path identifying the cache file you wish to use. For example:

   ```
   setup -s -f /home/deladmin/setup/install.inf
   ```

   When you use a cache file in this way, no new cache file is created from this installation. If you have many similar server configurations to set up, you can place the configuration file plus the server installation package on each machine. You execute the setup program on each machine; it then extracts all information it needs from the configuration file as it performs the installation.

Getting Started

The Start Page was designed to provide all the information you need to quickly begin using Delegated Administrator with the sample organization `Siroe`. You can access the Start Page at any time by pointing a web browser to `http://<host:webserver_port>/nda/start.htm`.

You can use the Start Page to log in as any level of administrator named in the page. The user ID and password you use to log in determines your administrator role and determines which branches of the directory you have access to.

To Use the Start Page

1. In a browser, enter the URL for the Delegated Administrator host using the form `http://<host:webserver_port>/nda/start.htm`.
2. Click Login.
3. In the Delegated Administrator Login window, using the information on the Start Page, enter an administrator's system user ID and password. For example, to log in as the Service Administrator, Chris Bolton, you would enter the following:

   User ID. chris

   Password. bolton
4. Click Login.

Delegated Administrator displays the administration page that is appropriate for the User ID you entered.

Using the Default Organization

You can use the default organization, `Siroe`, to perform the first few administration tasks, and then reconfigure it to meet your own requirements. For example, you can log in with the user ID `chris` and create as many organizations and administrators as you need. You can continue to use the default data and administration pages for learning or testing purposes. Once you've put your own directory structure in place, you can edit the default organization and group name, and delete the original six users from the directory.

If you've created a new organization at the same level as `Siroe` in the Delegated Administrator user tree, you'll have to create a new `start.htm` page and a new `login.htm` page for that organization. For more information, see the "Customizing Delegated Administrator." It will be available at the location where you downloaded the application.

Uninstalling Delegated Administrator

You can remove Delegated Administrator from your computer system. Both Directory Server and Web Server should be installed and running when you uninstall Delegated Administrator.When you run the Uninstall program, the following occurs:

- All Delegated Administrator binaries are removed.
- The web server configuration reverts to the way it was before Delegated Administrator was installed.
- The web server is restarted.
- All Delegated Administrator files that were generated after initial installation remain on your computer system.
- All data that was added to the directory when Delegated Administrator was installed, and any data that was added subsequently, remains in the directory.

To uninstall Delegated Administrator, run the Uninstall program:

- In Unix, enter `./uninstall`
- In Windows NT, in the Delegated Administrator root, double-click the Uninstall icon.

Chapter 4

Enabling Optional Features

Once you've completed the basic installation, you can configure Delegated Administrator to use one or more optional features. This chapter provides instructions for enabling the following:

- The Sample LDIF Data File
- Secure Sockets Layer (SSL)
- UserID Uniqueness
- User Directory Failover
- Password Reset Policy
- Single Sign-On

The Sample LDIF Data File

Directory Server uses the LDAP Data Interchange Format (LDIF) to describe a directory and directory entries in text format. An LDIF file is commonly used to initially build a directory database or to add large numbers of entries to the directory all at once.

Delegated Administrator comes with a sample LDIF file describing 20 domains and containing 50 users. The data in the sample LDIF file is entirely distinct from the default data that is created at installation. It is much larger by comparison, and requires some extra steps before you can use it.You can use this sample data for testing purposes or for learning how to use the product. Installing and using this sample data is entirely optional.

In order to use the contents of the sample LDIF file, use these instructions to do the following:

- Download the sample LDIF file.
- Add a base suffix in the directory for the sample data.
- Import entries from the sample LDIF to the directory.
- Modify the Delegated Administrator `resource.properties` file.

Downloading the Sample LDIF File

Go to the Delegated Administrator Documentation website at:

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

Follow instructions for downloading the file `ds_big.ldif.`

To Add the LDIF Base Suffix to the Directory

1. On the Directory Server Console select the Configuration tab.
2. Select the Database icon in the navigation tree.
   This displays the database settings in the right pane.
3. Select the Settings tab.
   This tab contains a list of all the current suffixes in your directory.
4. Click Add, and enter the new suffix `o=ISP` (or whatever you chose as the root of the installation).
5. Click Save.

To Import the Sample LDIF Using the Directory Server Console

1. On the Directory Server Console select the Configuration tab.
2. From the Console menu, select Import.
3. If you are running the Directory Server Console on the server's host machine, skip to step 4. Otherwise, if you want to import a file from the local machine, select "From local machine." If you want to import a file from the server's host, select "From server machine."
4. Enter the full path to the file `ds_big.ldif`.
5. Select Append Data to Database.
   When you import using this option, the server does not delete the contents of the directory before adding the entries from the LDIF file.
6. Click OK.

To Modify the Properties File

1. In the Delegated Administrator root, locate the file

   ```
   <DelegatedAdmin_root>/nda/classes/netscape/nda/servlet/resource.
   properties
   ```
2. In the line `NDAServlet-ldapsuffix=o=<your_suffix>,` change the base suffix to `o=ISP` (or whatever you chose as the root of the installation).
3. Save the file.
4. Restart the Web Server.

Secure Sockets Layer (SSL)

Delegated Administrator can be configured to use SSL-based connections, called *LDAPS connections*, to Directory Server in its default `DatabaseInterface.` These instructions refer to the back-end connections between the Delegated Administrator servlet engine and the directory. The front-end connections between the client browser and the web server that serves Delegated Administrator are another matter. To configure the front-end connections between the client browser and the web server, see the documentation that came with your Web Server.

The default behavior of Delegated Administrator is to use non-SSL-based LDAP connections between the servlet engine and Directory Server.

To Use SSL-based LDAPS Connections

1. Configure Directory Server and Web Server to support SSL-based LDAPS connections between them, following the instructions in the *Directory Server Administrator's Guide*.
2. Open the file `<DelegatedAdmin_root>/nda/classes/netscape/nda/servlet/resource.properties`, and make the following changes:
   - Change the line `LDAPDatabaseInterface-ldapssl=false` to `LDAPDatabaseInterface-ldapssl=true`.
   - Modify the line `LDAPDatabaseInterface-ldapsslport=<port number>` to reference the new Directory Server LDAPS port as configured in step 1.
3. Save the file.
4. Restart the Web Server.

UserID Uniqueness

Delegated Administrator supports a flexible userID uniqueness policy. UserID uniqueness may be enforced within each organization, or across all organizations in the Delegated Administrator tree.

When userIDs are enforced to be unique only *within each organization*, then a userID such as `bob` can exist in multiple organizations without conflict. For example, there can be a `bob` in the Siroe organization and a `bob` in the Airius organization even though both organizations are managed by Delegated Administrator.

However, when userIDs are enforced to be unique *across all organizations*, if the userID `bob` exists in the Siroe organization, you cannot create a userID `bob` in the Airius organization. By default, userID uniqueness is enforced across all organizations.

The UserID Uniqueness Plug-In

Netscape Directory Server comes with a plug-in that you can use to enforce uniqueness of an attribute within a subtree such as an organization. The plug-in can be configured through a marker— an entry above the insertion point of a new entry. The entry has an object class that identifies it as the top of a uniqueness tree.

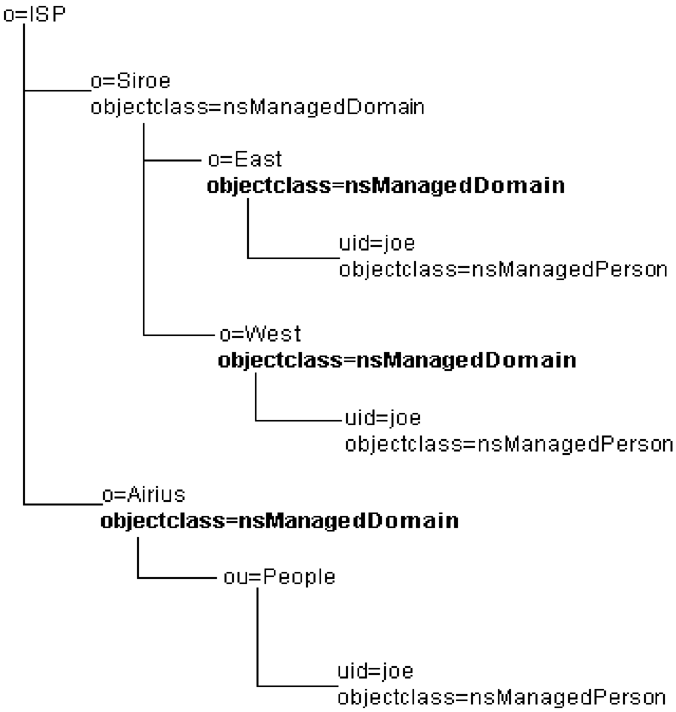
How it Works

In the following example (see Figure 4-1), `nsManagedDomain` is the object class used as the marker of the uniqueness tree. Uniqueness is enforced within each of the following organizations:

- `o=East,o=Siroe,o=ISP`
- `o=West,o=Siroe,o=ISP`
- `o=Airius,o=ISP`

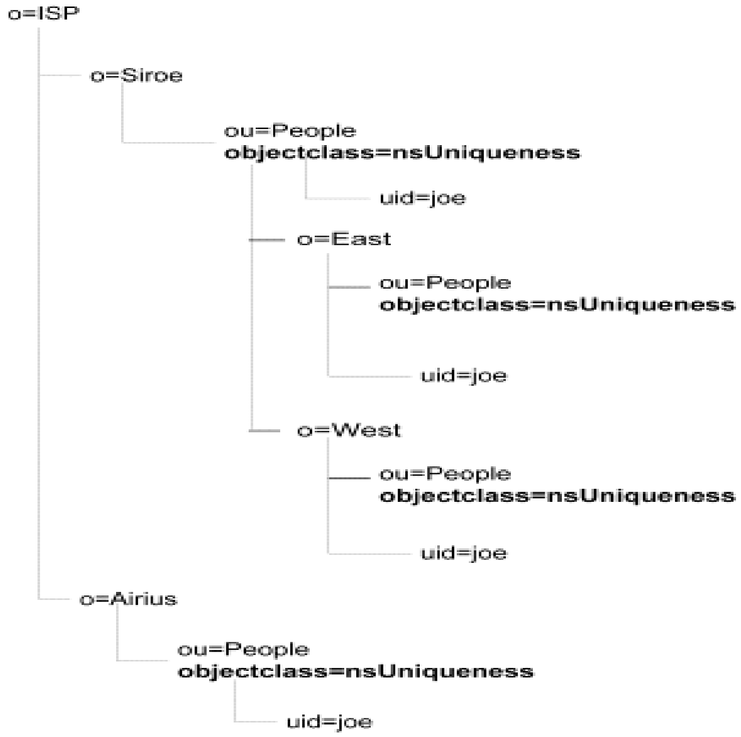
`o=Siroe,o=ISP` could be a uniqueness domain, but its only container children also have the marker object class, and uniqueness is enforced from the bottom up.

Figure 4-1 The objectclass nsManagedDomain marks the top of each uniqueness tree.


o=ISP
o=Siroe
objectclass=nsManagedDomain
o=East
objectclass=nsManagedDomain
uid=joe
objectclass=nsManagedPerson
o=West
objectclass=nsManagedDomain
uid=joe
objectclass=nsManagedPerson
o=Airius
objectclass=nsManagedDomain
ou=People
uid=joe
objectclass=nsManagedPerson

If you want to enforce uniqueness across non-nested suborganizations, you can use a configuration such as in Figure 4-2. In this example, `nsUnique` is the marker objectclass and `person` (for uid=joe) is the objectclass to enforce uniqueness on.

Figure 4-2 The objectclass nsUnique marks each ou=People container as the top of a uniqueness tree.



This configuration has a separate uniqueness domain for each `ou=People` container. There are four uniqueness domains, with no overlap.

Configuring the UserID Plug-in

If you're installing Delegated Adminstrator against an existing directory information tree (DIT), you must first add the appropriate objectclasses to your existing directory entries. See Appendix , "Using an Existing User Directory," for more information. Then use the following instructions to configure the plug-in. Once the plug-in is configured, the necessary object classes are automatically added each time you use Delegated Administrator to create new objects.

To Configure the UserID Plug-in

1. Stop Directory Server.
2. In the Directory Server root, locate the following file:

   `<Directory_root>/slapd-<identifier>/config/slapd.ldbm.conf`
3. Be sure that the following line is commented out (begins with a pound sign). Example:

```
#plugin preoperation on “uid uniqueness”
“<Directory_server_root>lib/uid-plugin.so” NSUniqueAttr_Init
“uid” “o=iplanet.com”
```

4. Modify the following plug-in invocation line to meet your needs;:

```
plugin preoperation on “attribute uniqueness”
<Directory_server_root>/lib/uid-plugin.so NSUniqueAttr_Init
“attribute=uid” “markerObjectClass=nsUniquenessDomain”
“requiredObjectClass=nsManagedPerson”
```

The plug-in invocation line takes the following:

- **attribute.** Specifies the attribute name.
- **markerObjectClass.** Specifies the object class that marks the top of the uniqueness tree.
- **requiredObjectClass.** Optinal. Specifies an object class which must be present in an entry in order for uniqueness to be enforced.

Example:

To enforce uid uniquness within a tree with the object class `nsManagedDomain` at the top (Figure 4-1), and where only entries with the object class nsManagedPerson are considered, modify the entry as follows:

```
plugin preoperation on “attribute uniqueness”
<Directory_server_root>/lib/uid-plugin.so NSUniqueAttr_Init
“attribute=uid” “markerObjectClass=nsManagedDomain”
“requiredObjectClass=nsManagedPerson”
```

5. Save the file.

6. Restart Directory Server.

User Directory Failover

After you’ve installed Delegated Administrator for the first time, the Directory server you used during installation becomes the “master” Directory server. You can set up other Directory servers that use the same base suffix as the master Directory server so that if the master fails for any reason, then Delegated Administrator *fails over* or uses a backup of the master.

Before you can enable user directory failover in Delegated Administrator, you must set up Server-Initiated Replication (SIR) agreements in each Directory server that you will use as a backup. For detailed information about directory replication, see the documentation that comes with Directory server:

- *Directory Server Administrator’s Guide* at `http://docs.iplanet.com/docs/manuals/directory/41/admin/replicat.htm`

- *Directory Server Deployment Guide* at `http://docs.iplanet.com/docs/manuals/directory/deploy30/rep.htm#1013789`

Setting up the Directory Servers

In each Directory server you plan to use for Delegated Administrator directory failover, make sure the server uses the same Base DN, Bind DN and Bind Password. After you've set up the Directory servers for SIR agreements, then you can enable user directory failover in Delegated Administrator.

NOTE If the Directory servers are in SSL mode, and you are using multiple Certificate Manangers to import certificates, be sure that each certificate manager has a different name.

To Set Up the Directory Servers for Failover

1. In each of the Directory servers you want to use as backup directories, manually create the same base suffix that you created in the master Directory server when you first installed Delegated Administrator.

   a. On the Directory Server Console select the Configuration tab.

   b. Select the Database icon in the navigation tree. This displays the database settings in the right pane.

   c. Select the Settings tab. This tab contains a list of all the current suffixes in your directory.

   d. To add the new suffix, click Add and enter the suffix in the field that appears.

   e. To modify an existing suffix, double-click the suffix in the list and make your changes.

   f. Click Save.

2. Follow the instructions in the Directory Server Administrator's Guide for creating a supplier-initiated replication (SIR) agreement. (See `http://docs.iplanet.com/docs/manuals/directory/41/admin/replicat.htm#1047117.`) As you follow the instructions:

   - The master Directory server is the *supplier* server, and the backup servers are the *consumer* server.

   - When prompted, select the base suffix you used when you installed Delegated Administrator for the first time (the suffix in the master Directory server.)

Enabling User Directory Failover in Delegated Administrator

Once you've set up replication agreements between the master Directory server and all backup servers, you must configure Delegated Administrator.

To Enable User Directory Failover in Delegated Administrator

1. Locate the following file:

   ```
   <DelegatedAdmin_root>/nda/classes/netscape/nda/servlet/resource.
   properties
   ```

2. Modify the variable `LDAPDatabaseInterface-ldaphost` variable to include a space-separated list of backup servers. Example:

   ```
   LDAPDatabaseInterface-ldaphost=<host1>:<port1>
   <host2>:<port2> <host3>:<port3>
   ```

   Providing a port number is optional. However, if the the port number is missing, it will default to the LDAP port value obtained from the same `resource.properties` file. If security is turned off, the value is obtained from `LDAPDatabaseInterface-ldapport.` If security is turned on for the LDAP connection, the value is obtained from `LDAPDatabaseInterface-ldapsslport` .

3. If you want to establish an SSL connection between the Directory server and Delegated Administrator, you must also add this line to the `resource.properties` file:

   ```
   LDAPDatabaseInterface-ldapssl=true  ###*
   ```

4. Restart the Web Server against which Delegated Administrator was installed .

Password Reset Policy

A password policy is a set of rules that govern how passwords are evaluated in the user directory. The password policy mechanism provided by the Directory Server allows you to dictate such things as minimum password length or when users' passwords expire. When a user attempts to bind to the directory, the Directory Server uses the rules defined by the password policy to ensure that the password is valid before allowing the user to bind to the directory.

Delegated Administrator extends the password reset and expiration policies to the users it manages. To make this work, you must modify the password policies in Directory Server, and then modify the Delegated Administrator configuration.

To Modify the Password Policy

1. In the Directory Server Console, click the Configuration tab, and then click the Database folder.

2. Select the Passwords tab in the right pane. The following password parameters are configurable. For detailed information about these parameters, see the *Directory Server 4.11 Administrator's Guide*. The first parameter listed here is the one that can be extended to Delegated Administrator.

   User must change password after reset. To specify that users must change their password the first time they log on, select this option.

   User May change password. To specify that users can change their own passwords, select this option.

   Allow Changes in X Day(s). To specify that users cannot change their password for a specified number of days, enter the number of days they cannot change their passwords.

   Keep Password History. To configure the server to maintain a history list of passwords used by each user, select this option.

   Remember X Passwords. If you configure the server to keep password histories (above), specify the number of passwords you want the server to keep for each user.

   Password never Expires. If you do not want user passwords to expire, select this option..

   Password Expires After X Days. If you want users to have to change their passwords periodically, select this option, and then enter the number of days that a user password is valid.

   Send Warning X Days Before Password Expires. If you have turned password expiration on (above), you need to enter the number of days before the password expires to send a warning to the user.

   Check Password Syntax. If you want the server to check the syntax of a user password to make sure it meets the minimum requirements, select this option.

   Password Minimum Length. If you turn password syntax checking on (above), you need to specify the minimum acceptable length.

Password Encryption. Use the drop-down list to specify what encryption method you want the server to use when storing passwords.

3. When you have finished making changes to the password policy, click Save.

To Modify the Delegated Administrator Configuration

1. In the directory where Delegated Administrator is installed, locate this file:

   ```
   <DelegatedAdmin_root>/nda/classes/netscape/nda/servlet/resource.
   properties
   ```

2. In the following property, the default value is `false`. To enable password change after reset, set this property to `true`:

   ```
   LDAPDatabaseInterface-ldapenablepasswordreset
   ```

3. This property specifies the correction to be added to GMT to obtain local (standard) time on the server:

   ```
   LDAPDatabaseInterface-ldapservertimeoffset
   ```

   The Delegated Administrator servlets may be running at a location other than where the Directory Server is installed. If the servlets are running in the same time zone as the Directory Server, this property need not be set. Otherwise, set it to a string of the form: `[-]HH:MM`. For example, for the Pacific Time Zone, this string would be `-8:00`. This property uses standard time only and so corrections should not be made for Daylight Savings Time.

4. This property specifies the OS type of the host running the Directory Server. This is required to handle the different password expiration times used by the iPlanet Directory Server, based upon the type of OS. Set this property to either `unix` (the default) or `nt` as appropriate.

   ```
   LDAPDatabaseInterface-ldapserverostype
   ```

5. In order for the changes to this file to take effect, restart the Web Server.

Single Sign-On

Delegated Administrator supports Single Sign-On through the use of Netegrity SiteMinder. Single Sign-On is a means for a user to log in once, using a single password, and obtain authenticated access to all servers that user is authorized to use. This feature has a number of benefits to both users and administrators including the following:

- Ease of use.

  Users can log in once and not be interrupted by repeated requests for passwords.

- Password are limited to local machine.

  To log in, the user types a single password that protects the private-key database on the local machine. Passwords are not sent over the network.

- Simplified management.

  Administrators can control who is allowed access to which servers by controlling the lists of certificate authorities maintained by client and server software. These lists are shorter than lists of user names and passwords and don't change as often.

- Access control is not affected.

  Single sign-on involves replacing client authentication mechanisms, not access-control mechanisms. Administrators don't need to change existing ACLs that may have been originally set up to work with basic password authentication.

Before You Begin

Before installing and configuring SiteMinder Policy Server to work with Delegated Administrator, the following must be installed and running:

- Directory Server 4.12
- Enterprise Server 4.1SP2
- iDA 4.5

Installing Siteminder on Windows NT

- When installing Siteminder on Windows NT, you must log into a Windows NT 4.0 account with local administrator privileges.
- For detailed installation instructions, see the *SiteMinder Installation Guide* that comes with the product.

Installing the Siteminder on Solaris

SiteMinder requires Solaris 2.5.1 or later. The following patches are required and recommended for the following versions of Solaris2.6

- Solaris 2.6 kernel update = 105181-17
- C++ shared library = 105591-07
- libc = 105210-25
- libthread = 105568-14
- patchadd = 106125-08

For detailed installation instructions, see the *SiteMinder Installation Guide* that comes with the product.

Configuring SiteMinder

To configure SiteMinder to work with Delegated Administrator, use the instructions in this section and the Netegrity SiteMinder manual entitled *SiteMinder Policy Server Operation Guide* to perform the following:

- Log in to SiteMinder
- Create Agents
- Create a User Directory
- Create a Domain Policy
- Create a Realm
- Create a Rule
- Create Policies from a Domain

To Log in to SiteMinder

1. Start your browser and enter the URL for the Policy Server you'll be using with Delegated Administrator. The URL should contain the hostname of the computer system on which the Policy Server is installed, and the port number that you used when you installed Web Server. The URL should take the following form:

   `http: //<hostname:portname>/siteminder`

   Example: `http://interlaken.red.iplanet.com:85/siteminder`

2. In the Administrator login page, click Administer SiteMinder.

3. In the SiteMinder Administration window, enter the following:

   User Name. Enter SiteMinder. This user name is the default Super User for which you entered a password during the installation.

   Password. Enter the password you defined in step of Installing the Policy Server .

4. Follow the instructions in the next section, "To Create Agents."

To Create Agents

1. In the SiteMinder Administration window, from the Edit menu, choose System Configuration, and then choose Create Agent. Enter the following:

   Name. Enter the name of the Agent. This is the the same as the name of the host computer system where SiteMinder is installed. The Agent name must correspond to the Agent name that you entered when you installed the Agent.

   Description. (Optional) Enter a brief description of the Agent.

   Agent Type. Select SiteMinder.

   IP Address or Host Name. Enter the IP address or name of the computer system where SiteMinder is installed.

   Shared Secret. Enter an alphanumeric Shared Secret.

   Confirm Shared Secret. Enter the Shared Secret again to confirm it.

   Shared Secret Assigned to. Enter the name of the Agent used when the Agent was installed on the Web server.

2. Click Apply to save the changes, or click OK to save the changes and return to the SiteMinder Administration window. Then follow the instructions in the in the next section, “To Create a User Directory.”

To Create a User Directory.

1. In the SiteMinder Administration window, from the Edit Menu, choose System Configuration, and then choose Create User Directory. In the SiteMinder User Directory dialog box enter the following:

   Name. Enter the name of the user directory. Example: `ldap`

2. Click **Directory Setup** , and enter the following:

   Server. Enter the IP address for computer system where the user directory is installed. Example: 192.18.122.91

   LDAP Search:

   In Root: Enter the Delegated Administrator root DN. Example: `o=ISP`

   LDAP User DN Lookup

   In Start: Enter `"uid="`

   In End: Enter `",ou=People,o=Siroe,o=isp`

3. Click Apply to save the changes, or click OK to save the changes and return to the SiteMinder Administration window. Then follow the instructions in the next section, “To Create a Policy Domain.”

To Create a Policy Domain

1. In the SiteMinder Administration window, from the Edit menu, choose System Configuration, and then choose Create Policy Domain. In the SiteMinder Policy Domain window, enter the following:

   Name. Enter a name for the policy domain. Example: nda and servlet.

   Description. Enter a brief description of the policy domain.

2. Click User Directory.
3. From the drop-down list at the bottom of the tab, select a user directory you want to include in the policy domain, and then click the Add button.

   SiteMinder adds the directory you’ve specified to the list displayed in the User Directory tab. User directories that serve as the authentication directores in a directory mapping are displayed as well.

4. Click Apply to save the changes.
5. Follow the instructions in the next section, “To Create a Realm.”

To Create a Realm

1. In the Siteminder Administration window, click the Policies Domain icon
2. In the Policies Domain window, click the Realms tab, and then click Create.
3. In the Realms window, enter the following:

   Name. Enter a name for the policy domain. Example: `nda`.

   Description. Enter a brief description of the policy domain.

4. Click Resource, and enter the following:

   Agent. Displays the agent name. Example: winnie

   Resource. Enter a resource name. Example `/nda/`

   - Make sure authentication scheme shows "Basic"
   - Make sure Default Resource Protection sellected "Protected" .

5. Click OK to save the data.

6. Repeat steps 1 through 4 to create another realm for the servlet, then follow the instructions in the next section, “To Create a Rule.”

To Create a Rule

1. In the Siteminder Administration window, click the Domain tab.
2. Click Policy Domain, and then click the plus symbol (+) to expand the list of policy domains which you want to add a rule.
3. Right click the realm/nested realm to which you want to add a rule. From the pop-up menu, select Create Rule under Realm and the SiteMinder dialog box opens
4. In the SiteMinder Rule window, enter the following:

   Name. Enter the name of the new rule. Example: nda rule.

   Description. (Optional) Enter a brief description of the new rule.

   Realm and Resources. From the drop-down list, select the name of the realm that includes the resources to which this rule will apply. Example: nda.
5. By default, the Realm drop-down list is set to the name of the realm you selected when you opened the SiteMinder Realm dialog box.
   - Make sure Resource: shows "*" .
   - Make sure that under Allow/Deny and Enable/Disable, the Allow Access option is selected.
   - Make sure that under Enable or Disable this rule, the Enabled option is selected.
6. In theAction group box, select Web Agent Actions.
7. Select all Get Put Post.
8. Click Apply to save the rule, or click OK to save the rule and return to the SiteMinder Administration window .
9. Repeat steps 1 through 7 to create a rule for servlet rule, and then follow the instructions in the next section, “To Create Policies from Domains.”

To Create Policies from Domains

1. In the SiteMinder Administration window, click Domain.
2. Click Policie Domains, and then click the name of the policy you created.

3. In the Policy Properties window, enter the following:

   Name. Enter the name of the policy. Example: nda and servlet.

   Description. Enter a brief description of the Agent.

4. Click Users.

5. Use ldapmodify to add the proxy account entry .

   dn: uid=proxy, ou=people, o=iplanet.com

6. In the Policy User/Groups, from Available member side, select the user and group you want to move to current members areas. If you do not see the users you want to move, select **Search Sign-on.**

   a. In the Search Sign-on window, select Attribute-Value Pair, and enter the following:

      Attribute. Add “uid”

      Value. Add “*”

   b. Click OK.

7. A list of users is generated. Use the arrows to move all Delegated Administrator users.

8. Click Rules.

9. Select Add/Remove Rules, and then select Rules from Available Member. Use the arrows to move to the current member. Move each policy you’ve created.

10. Click Apply

11. Click OK to save the data.

Configuring the Directory Server

The proxy user account will be used to bind to the Directory for proxied authentication. This user account must be created in a base suffix other than the Delegated Administrator base suffix. The following is an an example of a proxy user account entry:

```
dn: uid=proxy, ou=people,o=Siroe, o=iplanet.com
objectclass: top
objectclass: person
objectclass: organizationalperson
objectclass: inetorgperson
objectclass: proxy
uid: proxy
givenname: Proxy
sn: Auth
cn: Proxy Auth
```

To create a proxy account

1. Go to the <Directory_server_root>/shared/bin directory where Directory server is installed. Examples:

   Unix. cd /usr/netscape/server4/shared/bin

   Windows NT. cd \netscape\server4\shared\bin

2. Use `ldapmodify` to add the proxy account entry. For example:

```
ldapmodify -h <host_name> -p <port_number> -D “cn=directory
manager” -w password -a

dn: uid=proxy, ou=people,o=Siroe, o=iplanet.com
objectclass: top
objectclass: person
objectclass: organizationalPerson
objectclass: inetOrgPerson
uid: proxy
givenname: Proxy
sn: Auth
userpassword: proxypassword
cn: Proxy Auth


Ctrl-D   (UNIX)
Ctrl-Z   (NT)
```

To Create an ACI for proxied authorization

1. Go to the <Directory_server_root>/shared/bin directory where the Directory Server 4.1 is installed Examples:

   Unix. cd /usr/netscape/server4/shared/bin

   Windows NT. cd \netscape\server4\shared\bin

2. Use ldapmodify to add an ACI to the base entry. For example:

```
ldapmodify  -h <host_name> -p <port_number> -D “cn=directory
manager” -w password

dn: o=ISP
changetype: modify
add: aci
aci: (target=”ldap:///o=ISP”)(targetattr=”*”)(version 3.0; acl
“proxy”;allow (proxy) userdn=”ldap:///uid=proxy,
ou=people,o=iplanet.com”;)

Ctrl-D   (UNIX)
Ctrl-Z   (NT)
```

Configuring Delegated Administrator

Once the proxy user account has been created in the Directory, you must configure Delegated Administrator for proxied authentication. Use the instructions in this section to add the proxy user DN and password to the resources.properties file.

To Configure Delegated Administrator for Proxied Authentication

In the file `<DelegatedAdmin_root>/nda/classes/netscape/nda/servlet/resources.properties`, remove the comment character (#) from the following entries, and modify appropriately:

```
#LDAPDatabaseInterface-ldapauthdn=<Proxy Authentication DN>
```

```
#LDAPDatabaseInterface-ldapauthpw=<Proxy Authentication Password>
```

Examples:

```
LDAPDatabaseInterface-ldapauthdn=uid=proxy,o=people, o=iplanet.com
```

```
LDAPDatabaseInterface-ldapauthpw=proxypassword
```

Restarting the Web Server

For the changes to take effect, restart the Web Server.

Chapter 5

Certificate-Based Authentication

Certificate-based authentication is a means of confirming a user's identity before allowing the user access to Delegated Administrator. When you configure Delegated Administration for certificate-based authentication, administrators and end users log in using digital certificates instead of user names and passwords. Certificate-based authentication is part of the Secure Sockets Layer (SSL) protocol.

This chapter provides instructions for setting up certificate-based authentication in iPlanet Delegated Administrator 4.5. It contains the following sections:

- Before You Begin
- Step 1: (Optional) Install and Configure Netscape Certificate Server
- Step 2: Configure Web Server 4.1
- Step 3: Issue Certificates for Delegated Administrator Users
- Step 4: Configure the Directory Server
- Step 5: Configure Delegated Administrator
- Step 6: Restart Web Server

Before You Begin

- Before you can begin setting up certificate-based authentication, Directory Server 4.11, Web Server 4.1, and Delegated Administrator 4.5 must be installed. For detailed information, see Chapter 3, "Basic Installation and Configuration" in this manual.
- Do not disable anonymous access to the Delegated Administrator tree. By default, anonymous access is enabled. It must remain enabled in order for certificate-based authentication to work properly.
- You can obtain certificates from a public or third-party Certificate Authority (CA) such as VeriSign™. Or you can install a certificate server such as Netscape Certificate Management System and issue your own user certificates.
- To request certificates from a public or third-party CA, see the documentation provided by the CA, and then skip to Step 2. If you want to use Certificate Server Management System to issue your own certificates, continue to the next section, Install and Configure Certificate Management System.
- The examples in this chapter provides instructions for using Certificate Management System 4.1. If you plan to set up certificate-based authentication using Certificate Management System 4.2, then see the documentation that comes with the server for detailed instructions. You can find online documentation for Certificate Management System at this site: `http://docs.iplanet.com/docs/manuals/cms.html`

Step 1: (Optional) Install and Configure Certificate Management System

When you use Certificate Management System to issue client certificates, you can configure the server to automatically copy the certificates to the Directory Server so that authentication can occur. Use the instructions provided in the following sections to:

- Install Certificate Management System
- Configure Certificate Management System to work with the Directory

Installing Certificate Management System

Follow the instructions in the *Netscape Certificate Management System 4.1 Installation and Deployment Guide* to install Certificate Management System.

When you install Certificate Management System, you specify configuration Directory Server information and related settings for the Certificate Management System.

Configuration Directory Server	**Description**
Port name and number	Enter the computer host name and port number for the directory server. Example: `spock:489`
Admin ID	Enter the user ID for the administrator who can access the directory server with full privileges. Example: `admin`
Admin Port	Enter the port number of the Administration server that manages the Directory Server. Example: `10310`
Suffix	Enter the root suffix in the Directory Server. Example: `o=siroe.com`
Directory Manager DN	Enter the DN of the administrator who has rights to modify directory entries. Example: `cn=Directory Manager`
Directory Manager Password	Enter the password of the administrator above. The password must be at least 8 characters in length.
Administration domain	Enter the name of the administration domain this directory server belongs to. Example: `siroe.com`

Certificate Management System	Description
CMS ID	Enter a unique identifier for the CMS server instance. Example: myCA
	Enter LDAP server information for the CMS internal database. Examples:
• Instance ID	• myCA-db
• Port number	• 38900
• Directory manager DN	• cn=Directory Manager
• Directory manager password	• password
	Enter information about the Administrator with access to CMS window. Examples:
• Admin ID	• certadmin
• Full name	• CMS Administrator
• Organizational unit suffix	• ou=cert
• Organization suffix	• o=siroe.com
• Admin password	• password
	Enter CMS configuration settings. Examples:
• SSL admin port	• 8200
• SSL agent port	• 8100
• SSL end-entity port	• 443
Certificate subject DN	Example: CN=Certificate Manager, OU=cert, O=siroe.com, L=Santa Clara, ST=California, C=US
Single sign-on password	Example: password

Configuring Certificate Management System

When the Certificate Management System is configured to work with the Directory Server, each time you create a new certificate, Certificate Management System automatically copies it to the Directory Server. After configuration is done, you can use the directory-based enrollment feature in Certificate Management System to automatically request, issue, and copy the new certificate into the directory server user entry.

To Configure Certificate Management System to Work with Directory Server:

1. Log in to the CMS window from within Netscape Console.
2. Click the Configuration tab.
3. In the navigation tree, select Certificate Manager, then select LDAP Publishing.
   a. To enable LDAP publishing, check the Enable LDAP Publishing option.
   b. In the Destination section, modify settings as follows:

      Host Name. Enter Delegated Administrator’s Directory Server host name. The Certificate Management System uses this name to locate the Directory Serve. The format for the host name must be as follows: `<machine_name>.<your_domain>.<domain>`. For example, `spock.siroe.com`.

      Port Number. Enter Delegated Administrator’s Directory Server port number. For example, `4890`.

      Use SSL communication. If Directory Server is configured for SSL-enabled communication, select this option.

      Directory Manager DN. Enter the DN of the Directory Manager for the Directory Server. For example, `cn=directory manager`.

      Password. Enter the password of the Directory Manager for the Directory Server.

      Version. Select the LDAP protocol version. For Netscape Directory Server 3.x and later select 3. For earlier versions, select 2.

      Client certificate. No change is required, make sure it is set to `Server-Cert`, if you checked the “Use SSL communication” option.

Authentication. Select the authentication type. The choices are “Basic authentication” and “SSL client authentication.” If you select “Basic authentication,” you must specify the Bind as parameter. If you select “SSL client authentication,” you must check the “Use SSL communication” box and identify the certificate that the Certificate Manager must use for SSL client authentication to the directory.

c. Click Save.

d. Configure mapping rules for the CA certificate. Within Configuration / Certificate Manager / LDAP Publishing, click the CA Certificate tab.

Mapping Rules. Click on Configuration and specify the parameters so that the Certificate Management System can locate the CA’s entry in the directory.

filterComps: Enter `CN`.

dnComps. Delete the entry so that the value field is empty.

baseDN. Set this to the Delegated Administrator root. For example, `o=ISP`.

Publishing Rules. Leave this as it is; no changes are required.

e. Configure mapping rules for user certificates so that components match attributes in the directory entry. Within Configuration / Certificate Manager / LDAP Publishing, click the User Certificate tab.

Mapping Rules. Click on Configuration and specify the parameters so that the Certificate Management System can locate the user entry in the directory.

filterComps. Enter `UID`.

dnComps. Delete the entry so that the value field is empty.

baseDN. Set this to the Delegated Administrator root. For example, `o=ISP`.

Publishing Rules. Leave this as it is; no changes are required.

4. In the navigation tree, select Authentication.

a. Click Add

b. Select `uidPwdDirAuth`.

c. Click Next, and then set the values of the following configuration parameters:

Authentication Instance ID. Make sure this field has `UserDirEnrollment`.

dnPattern. Set the dnpattern so that it is identical to the user's full DN in the Delegated Administrator base suffix:

```
UID=$attr.uid, CN=$attr.CN, E=$attr.mail, OU=people, o=Siroe,
o=ISP
```

Note that `CN` and `E` are optional.

ldapStringAttributes. Leave this blank.

ldapByteAttributes. Leave this blank.

ldap.ldapconn.host. Enter Delegated Administrator's Directory Server host name. For example, `spock.siroe.com`.

ldap.ldapconn.port. Enter Delegated Administrator's Directory Server port number. For example, `4890`.

ldap.ldapconn.secureConn. Enter `fasle`.

ldap.ldapconn.version. If the directory is based on Directory Server 1.x, enter 2. For Directory Server versions 3.x and later, enter 3.

ldap.baseDN. Set this to the Delegated Administrator root. For example, `o=ISP`.

ldap.minConns. Enter a value between 1 to 3, indicating the minimum number of connections permitted to the Directory Server.

ldap.maxConns. Enter a value between 3 to 10, indicating the maximum number of connections permitted to the Directory Server.

d. Click OK.

5. Click Refresh.

6. Restart Certificate Management System.

Step 2: Configure Web Server 4.1

Configure Web Server to work with Directory Server so that proxied authentication can occur. In proxied authentication, the Web Server looks up the user certificate in the Directory, and provides user authentication throughout an entire Delegated Administration session. This saves the user from having to re-authenticate before performing each Delegated Administrator operation. Use the instructions provided in the following sections to:

1. Enable SSL
2. Configure Web Server to work with the Directory Server
3. Modify the certmap.conf file
4. Create ACIs that restrict access to Delegated Administrator servlets
5. Define a servlet alias
6. Restart the Web Server

Enabling SSL

Follow the instructions in the Web Server Administrator's Guide to enable SSL. The instructions include sections on:

- Installing a server certificate
- Trusting the new Certificate Authority
- Turning on encryption

Once SSL is enabled for Web Server, you can follow the steps in the next section to Configure Web Sserver to work with Directory Server.

Installing a server certificate on Web Server 4.1

1. If you have not done so, create a trust database for the Web Server Instance.
2. Request a Certificate; this will generate a server certificate request.
3. Request a Server Certificate using the request code. You can use Certificate Management System to do this.
4. After you received the certificate, install it in the certificate database of the Web Server instance.

Trusting the new Certificate Authority

In Certificate Management System

1. Open a web browser window.
2. Access Certificate Management System on SSL end-entity port, for example on port 443.
3. In the Retrieval tab, select Import CA Certificate Chain.
4. Select “Display the CA certificate chain in PKCS#7 for importing into a server.”
5. Click Submit. You should see the CA certificate chain.
6. Copy the CA certificate chain to the clipboard, including headers such as:

   `----BEGIN CERTIFICATE----` and

   `----END CERTIFICATE----`

In Web Server

1. Access the Web Server instance.
2. In the Security tab select Install Certificate.
3. In the section “Certificate for,” select Trusted Certificate Authority CA, and specify the Key Pair File Password.
4. Select Message Text (with headers).
5. Paste the CA certificate chain that you copied into the edit field (make sure headers are included).
6. Click OK. The trusted CA certificate is displayed.
7. Click Add Server Certificate.
8. Restart your Web Server Instance.

Turning on encryption

Turn encryption on for your Web Server Instance. See the *Web Server Administrator’s Guide* for detailed information.

Configuring Web Server to Work with Directory Server

This configuration tells Web Server where to search for user certificates during the authentication process.

To Configure Web Server to work with Directory Server

1. In Web Server, in the General Administration page, click Global Settings.
2. In the Global Settings page, click Configure Directory Service.
3. In the Configure Directory server page, modify the settings as follows:

   Host Name. Enter the host name for the Delegated Administrator Directory Server. For example, `spock`.

   Port. Enter the port number for the Delegated Administrator Directory Server. For example, `4890`.

   Sockets Layer (SSL). If Directory Server is SSL-enabled, select Yes.

   Base DN. Enter the base DN you selected when you installed Delegated Administrator. For example, `o=ISP`.

   Bind DN (optional). Specify the DN that will use to initially bind. For example, `cn=Directory Manager`.

   Bind Password (optional). Specify the password for the given base DN.
4. Click Save Changes.

Modifying the certmap.conf File

The file certmap.conf maps certificates to user entries in the Directory. It is stored in the Web Server installation at `<server_root>/userdb`, for example `/usr/netscape/server/userdb`. The following is an example of a default certmap.conf entry:

```
certmap default  default
#default:DNComps
#default:FilterComps e, uid
#default:verifycert on
```

To enable Web Server to work with Directory Server, the entry is changed to the following:

```
certmap default default
default:DNComps ou, o, o
default:FilterComps uid
default:verifycert on
```

Restricting Access to Delegated Administrator Servlets

In the Web Server, append an appropriate ACL rule into this file:

`<server_root>/httpacl/generated.https-<hostname>.acl`

The following is an example of an appropriate ACL rule:

```
acl “uri=/servlet/”;
      authenticate (user, group) {
            database = “default”;
            method = “ssl”;
            prompt = “iPlanet Delegated Administrator4.5”;
      };
      allow absolute (read,execute)(user = “all”);
      deny (all)(user = “anyone”);
```

The important components of this ACL are the resource (`uri=/servlet/`) and the access control method corresponding to certificate authentication (method="ssl"). In this example, whenever a client request includes `uri=/servlet`, Web Server requires certificate authentication before the request can be fulfilled.

Defining a Servlet Alias

1. In the file

   `<ES Server_Root>/<Server_Instance>/config/servlet.properties`

   make sure the following is uncommented:

```
servlet alias definition:

servlet.cauth.code=netscape.nda.servlets.NDACertAuth
servlet.cauth.args=
servlet.cauth.preload=true
```

2. In the file

   `<ES Server_Root>/<Server_Instance>/config/rules.properties`,

   make sure the following entry within the rules section exists:

   `/servlet/cauth=cauth`

Restart the Web Server

In order for the changes to become effective, you must restart the Web Server.

Step 3: Issue Certificates for Delegated Administrator Users

Follow these steps for each Delegated Administrator user:

1. Request a user certificate from a trusted CA such as VeriSign, or from Certificate Management System.
2. If you are using Certificate Management System 4.1, follow these steps:
   a. Open a web browser window.
   b. Access the Certificate Management System on the SSL end-entity port. The default port number is 443.

   c. Make sure Certificate Management System is configured correctly for directory-based enrollment and publishing.

   d. From the Enrollment tab, select Directory Based.

   e. Specify User ID and Password of the user to who you want to issue a certificate. For example, `id=chris, password=bolton`.

3. If you've properly configured Certificate Management System to work with Directory Server, the Certificate Management System automatically copies the user certificate it issues to the user's entry in the directory. No action is required on your part here. But if you obtained the certificate from another Certificate Authority (such as VeriSign), you must manually copy the certificate to the directory.

4. In Directory Server, you can verify that certificates have been added to the directory.

   a. Go to the `<Directory_server-root>/shared/bin` directory where the Directory Server 4.1 is installed. Examples:

   Unix. cd /usr/netscape/server4/shared/bin

   NT. cd \netscape\server4\shared\bin

   b. Use `ldapsearch` to search for entries with certificates. For example,

```
servlet alias definition:


servlet.cauth.code=netscape.nda.servlets.NDACertAuth
servlet.cauth.args=
servlet.cauth.preload=true
```

```
dn: uid=chris-Siroe.com, ou=Users, o=Siroe.com,o=sundance
usercertificate;binary::
```

The following is an example of a user's certificate in the directory:

```
MIICSDCCAbGgAwIBAgIBBDANBgkqhkiG9w0BAQQFADBCMQswCQYD
VQQGEwJVUzERMA8GA1UEChMIbmV0c2NhcGUxDDAKBgNVBAsTA21jYzES
MBAGA1UEAxMJaHVycmljYW5lMB4XDTk5MDQxMjIxMTc1M1oXDTk5MTAw
OTIxMTc1M1owWjERMA8GA1UEChMIc3VuZGFuY2UxEzARBgNVBAoTCkFpc
ml1cy5jb20xDjAMBgNVBAsTBVVzZXJzMSAwHgYKCZImiZPyLGQBARMQY2h
yaXMtQWlyaXVzLmNvbTCBnzANBgkqhkiG9w0BAQEFAAOBjQAwgYkCgYEA
tMabUpJuab3hd/jqhopuhwNyRVSVYmJTFmN7af/vQgKoitDXNt3oo9xxuvf3Pyo
6s4gKfWlKu4oC1dnDWj8fNy1kA5K9/wX/T3lEiDhzK2a7ynlxJQg6NAv6uUkHU
Rfovw92UhqgZxm5yxNbIvFMAKwpbVd+dOU+1KkGlhjkOw8CAwEAAaM2MD
QwEQYJYIZIAYb4QgEBBAQDAgCgMB8GA1UdIwQYMBaAFEKI8NkBSTsMWi
O9cOlXDU7un/avMA0GCSqGSIb3DQEBBAUAA4GBAD697bhr0g91nqdmoiGM
+BixYCB88/rZp0F4jG3a7AIPmPX+z82u++HJISg+UZHfAdk5+C+OhfwAPsrLBC
Y2RrecRR7U7+/AUPZk8e0IIemaC7AdcsEH4+4N0ONeSxMWikg2UDcPTmNKK
NVe13C0t0ynnRs2O0zKxEZk+tJOBJPv
```

Step 4: Configure the Directory Server

Follow the instructions in this section to:

- Create a proxy user account
- Create an ACI for proxied authentication

Creating a Proxy User Account

The proxy user account will be used to bind to the directory for proxied authentication. This user account must be created in a base suffix other than the Delegated Administrator base suffix.

The following is an example of a proxy user account entry:

```
dn: uid=proxy, ou=people, o=mcom.com
objectclass: top
objectclass: person
objectclass: organizationalperson
objectclass: inetorgperson
objectclass: proxy
uid: proxy
givenname: Proxy
sn: Auth
cn: Proxy Auth
```

To Create a Proxy User Account

1. Go to the `<Directory_server_root>/shared/bin` directory where the Directory Server 4.1 is installed. Examples:

   Unix. `cd /usr/netscape/server4/shared/bin`

   Windows NT. `cd \netscape\server4\shared\bin`

2. Use `ldapmodify` to add the entry. For example:

```
ldapmodify -h <host_name> -p <port_number> -D
“cn=directory manager” -w password -a
dn: uid=proxy, o=iplanet.com
objectclass: top
objectclass: person
objectclass: organizationalPerson
objectclass: inetOrgPerson
uid: proxy
givenname: Proxy
sn: Auth
userpassword: proxypassword
cn: Proxy Auth

Ctrl-D   (UNIX)
Ctrl-Z   (NT)
```

Create an ACI for proxied authentication

1. Go to the `<Directory_server_root>/shared/bin` directory where the Directory Server 4.1 is installed.
2. Use `ldapmodify` to add an ACI to the base entry. For example:

```
ldapmodify  -h <host_name> -p <port_number> -D
“cn=directory manager” -w password
dn: o=ISP
changetype: modify
add: aci
aci: (target=”ldap:///o=ISP”)(targetattr=”*”)(version 3.0;
acl
“proxy”;allow (proxy) userdn=”ldap:///uid=proxy,
o=iplanet.com”;)

Ctrl-D   (UNIX)
Ctrl-Z   (NT)
```

Step 5: Configure Delegated Administrator

Once the proxy user account has been created in the Directory, you must configure Delegated Administrator for proxied authentication. Use the instructions in this section to add the proxy user DN and password to the resources.properties file. In the file

`<DelegatedAdmin_root>/nda/classes/netscape/nda/servlet/resources.properties`,

uncomment and modify the following entries:

`LDAPDatabaseInterface-ldapauthdn=<Proxy Authentication DN>`

`LDAPDatabaseInterface-ldapauthpw=<Proxy Authentication Password>`

For example:

`LDAPDatabaseInterface-ldapauthdn=uid=proxy, o=iplanet.com`

`LDAPDatabaseInterface-ldapauthpw=proxypassword`

Step 6: Restart the Web Server

For the changes to take effect, restart the Web Server instance.

Chapter 6

Class of Service

Class of Service (CoS) is a feature of Netscape Directory Server that enables you to manage a group of service-related attributes. These related attributes form a category or *class* of service. Once you've defined attributes and created new classes in the directory, you can assign a class of service to individual user entries. This eliminates having to store multiple service-related attributes in each user entry in the directory. It also makes it easier to make changes when necessary. If a class of service changes, you need only change its attributes in the CoS templates. You don't have to change the attribute values in each user entry.

This chapter provides an overview the CoS feature, and includes examples for setting up CoS with Delegated Administrator. Topics included in this chapter:

- How CoS Works
- Setting Up CoS in Delegated Administrator

How CoS Works

Directory Server clients such as Delegated Administrator read attributes stored in user entries. A user entry typically contains attributes that describe the user's basic information such as name, department, phone number and so on. An entry can also contain a number of related attributes. For example, a user entry might include a number of attributes that desrcibe the hosting services provided to the individual. These attributes might include the cost of the service, amount of storage space, access to email, and access to calendaring. With the CoS feature, you can define service classes that automatically specify values for each of these attributes (see Table 6-1). Once you create these CoS classes, instead of storing four different attributes in a user's entry, you can store a single CoS attribute that contains one of these values: Premium, Deluxe, Promotional, or Basic.

Table 6-1 Siroe customers can choose from four service plans associated with their individual home page.

Class of Service	Cost	Storage	Webmail	Calendar
Premium	$30/mo	30MB	Yes	Yes
Deluxe	$20 /mo	20MB	Yes	Yes
Promotional	$15/mo	10MB	Yes	No
Basic	None	5MB	Yes	No

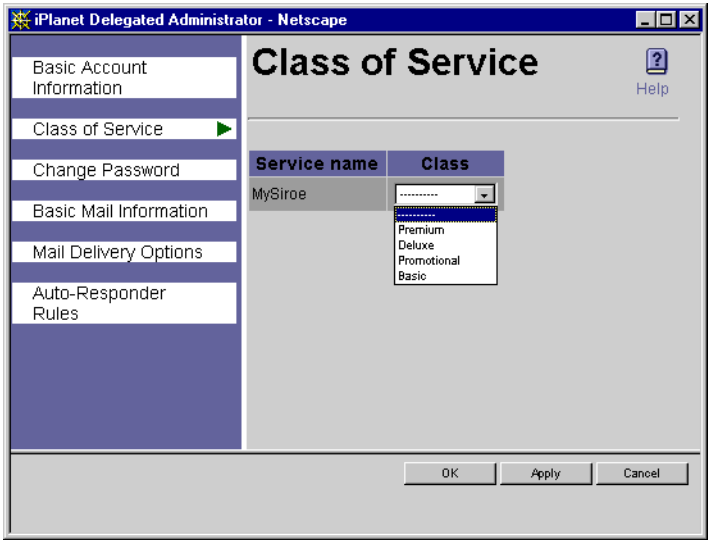
The CoS logic generates the user entry that is sent to the client. The values returned for these attributes are determined by :

- The entry's DN.
- The objectclass of the entry.
- A service class attribute value stored with the entry. (The absence of the attribute altogether can also imply a specific default class of service.)
- The attribute values stored in a service class template entry.

If schema checking is turned on, CoS attribute values will only be generated where the entry has an objectclass that allows the attribute. If schema checking is turned off, this is not enforced. Multiple class of service schema may be defined within a server, although it is illegal to define schema that conflict with each other.

The following scenario illustrates how CoS works with Delegated Administrator. The Siroe company proivdes its customers the means to create their own home pages. The home page, named MySiroe, is the first page the user sees when he or she logs in to the Siroe internet service. The customer can configure the page to display information such as local news, stock quotes, and links to other sites that may be of special interest to him or her. The customer can also choose from four service plans related to his or her home page: Premium, Deluxe, Promotional, and Basic. These service plans correspond to Siroe's fee structure, which is summarized in Table 6-1. When a customer signs up for a service plan, an administrator uses Delegated Administrator to assign the appropriate class of service to the user's account.

In the Delegated Administrator front end, Class of Service is one category of user account information. If the Class of Service plugins are not properly installed and configured, the message "No services available" will appear in the Service Name column.



Service name	Class
MySiroe	---------

When a class of service is assigned to a user, Delegated Administrator adds the CoS objectclass and attributes to the user's directory entry. In this example, the objectclass `calUser`, and the attribute `calclass` are added.

Figure 6-1 CoS objectclass and atributes are added to the directory.

```
dn: uid=bill, ou=People, o=Siroe, o=ISP
objectclass: top
objectclass: person
objectclass: organizationalPerson
objectclass: inetOrgPerson
objectclass: nsManagedPerson
objectclass: mailRecipient
objectclass: nsMessagingServerUser
objectclass: calUser
uid: bill
userpassword: {SHA}rOiT+yyVU6OKhz+wPQ4hpAazUaE=
cn: Bill Johnson
sn: Johnson
givenname: Bill
telephonenumber: 650.555.1212
mail: bill@Siroe
nsdadomain: Siroe
memberof: cn=Group1, ou=Groups, o=Siroe, o=ISP
owner: cn=Department Administrators, cn=Group1, ou=Groups,
 o=Siroe, o=ISP
calclass: Premium
```

Class of Service Definition

Class of service definitions include all the information required to generate specific attribute values. These definitions are stored in directory entries, and can be located anywhere in the DIT. All CoS definition entries contain the objectclass `cosDefinition`. In the following examples, the service classes apply only to entries within the portion of the tree under `ou=People`, `o=Siroe`. In the following example, the service class is defined by specifying the attribute `calClass`.

Figure 6-2 A CoS definition entry.

```
dn: cn=MySiroeClasses, ou=COS, o=Siroe
objectclass: top
objectclass: account
objectclass: cosDefinition
cosTargetTree: o=Siroe
cosTemplateDn: ou=MySiroeClasses, ou=COS, o=Siroe
cosSpecifier: calClass
cosAttribute: cost
cosAttribute: diskspace
cosAttribute: webamil
cosAttribute: calendar
```

Defining a Class of Service Schema

A class of service schema is defined by an entry with the cosDefinition objectclass. This entry may reside anywhere in the DIT. The following attributes are required by the `cosDefinition`:

CosTargetTree. This determines the subtrees of the DIT to which this class of service schema applies. The values for this attribute for this schema and for multiple class of service schema may overlap their target trees in an arbitrary fashion.

CosTemplateDn. This is the DN where the Cos templates are stored. The templates may reside anywhere in the subtrees, and other entries unrelated to class of service may also be contained therein. The caveat is that if any unrelated entry in the target tree contains even one attribute that the class of service schema generates, then that entry is determined to be a class of service template.

CosSpecifier. This is the attribute stored in a user entry that specifies a particular class of service for this schema. In the absence of a default service class this attribute is required for all entries that are to be part of the schema.

CosAttribute. This is a list of the attributes that are provided by the class of service schema. Each of the attribute values may be qualified by either `override` or `default`. These qualifications are added to the end of the attribute value, separated by a single space. The override directive makes the attribute value in the class of service schema override any attribute value in the entry being queried for the value. The default directive makes any attribute value in the entry being queried, if one exists, be used instead of the value that would have been supplied by its service class - this is the default behavior in the absence of a qualifier. This directive can be used to allow individual exceptions to the service class.

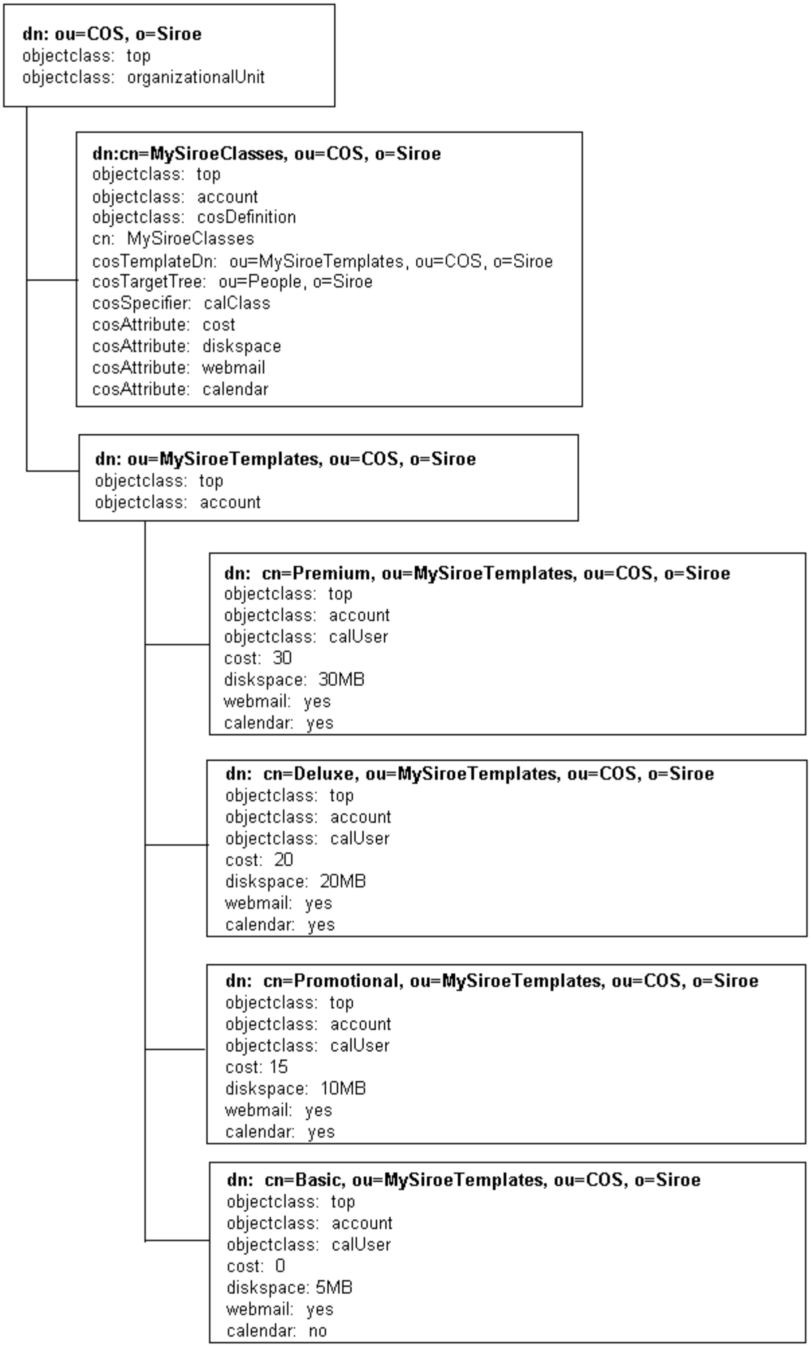
Templates

Service-class templates define the service classes you want to create for the entries in your directory. Each template corresponds to a single service class. A service class template for a schema is any entry that exists in any of the subtrees in the COS schema's cosTargetTree attribute, and that contains at least one of the attributes the schema generates (CosAttribute).

The template entries for a given class of service schema are all stored in the Directory Information Tree (DIT) as children of a common parent entry. The relative DNs of the template entries are the respective values of the service class attribute, plus the special RDN cosSpecifier-default.

The object class cosSpecifier is the value of the cosSpecifier attribute in cosDefinition. This is used when the service class attribute value is NULL or not present. For example, a cosDefinition with a cosSpecifier value of calClass, has a default template of calClass-default.

Figure 6-3 CoS objectclasses and templates are stored in the directory.



```
dn: ou=COS, o=Siroe
objectclass:  top
objectclass:  organizationalUnit

dn:cn=MySiroeClasses, ou=COS, o=Siroe
objectclass:  top
objectclass:  account
objectclass:  cosDefinition
cn:  MySiroeClasses
cosTemplateDn:  ou=MySiroeTemplates, ou=COS, o=Siroe
cosTargetTree:  ou=People, o=Siroe
cosSpecifier:  calClass
cosAttribute:  cost
cosAttribute:  diskspace
cosAttribute:  webmail
cosAttribute:  calendar

dn: ou=MySiroeTemplates, ou=COS, o=Siroe
objectclass:  top
objectclass:  account

dn:  cn=Premium, ou=MySiroeTemplates, ou=COS, o=Siroe
objectclass:  top
objectclass:  account
objectclass:  calUser
cost:  30
diskspace:  30MB
webmail:  yes
calendar:  yes

dn:  cn=Deluxe, ou=MySiroeTemplates, ou=COS, o=Siroe
objectclass:  top
objectclass:  account
objectclass:  calUser
cost:  20
diskspace:  20MB
webmail:  yes
calendar:  yes

dn:  cn=Promotional, ou=MySiroeTemplates, ou=COS, o=Siroe
objectclass:  top
objectclass:  account
objectclass:  calUser
cost: 15
diskspace:  10MB
webmail:  yes
calendar:  yes

dn:  cn=Basic, ou=MySiroeTemplates, ou=COS, o=Siroe
objectclass:  top
objectclass:  account
objectclass:  calUser
cost:  0
diskspace: 5MB
webmail:  yes
calendar:  no
```

Interaction with Stored Attribute Values

If the class of service logic detects that it is generating an attribute value already stored on the entry, the default action is to supply the stored value to the client. However, the server's behavior can be controlled by means of the `cosDefinition` entry. The `cosAttribute` values allow an additional qualifier appended after the attribute type name. Valid qualifier values are `override` and `default`. An absent qualifier means the same as `default`. `Override` means that the server will always return the value generated by the class of service logic even when there is a value stored with the entry. `Default` means that the server will only return a generated value if there is no corresponding attribute value stored with the entry. For example:

Figure 6-4 Qualifiers are appended to cosAttribute values.

```
dn: ou=MySiroeClasses, ou=COS, o=Siroe
objectclass: top
objectclass: account
objectclass: cosDefinition
cosTargetTree: ou=People, o=Siroe
cosTemplateDn: ou=MySiroeClasses, ou=COS, o=Siroe
cosSpecifier: calClass
cosAttribute: cost
cosAttribute: diskspace override
cosAttribute: webmail default
cosAttribute: calendar default
```

Configuration and Management

Because all the configuration information and template data are stored as entries in the directory, standard LDAP tools can be used for CoS configuration and management. Specialized scripts, command-line tools, and graphical UI could be developed. These would use the LDAP SDK to inspect and change the configuration. For detailed information, see Netscape Directory Server 4.12 documentation.

Setting Up CoS in Delegated Administrator

In order to use the Class of Service (CoS) feature, you must first make changes in both Directory Server and in Delegated Administrator. The following examples illustrate how you can set up the classes of services described in the Table 6-1. The changes you'll make include:

- Adding CoS Schema
- Modifying user entries
- Modifying Delegated Adminstrator configuration

NOTE Before you can enable the Class of Service feature, its special directory plugin must be installed and configured. This must be done prior to installing Delegated Administrator. For detailed information, see "Step 2: Configure the Directory Server Plug-ins" on page 53.

Adding COS Schema

Create a new object class and new attributes for each Class of Service you want to use. The following examples correspond to the classes described in Table 6-1 on page 110.

To Add CoS Schema

1. Stop the Directory Server.
2. In the file `<server_root>/slapd-<identifier>/config/slapd.user_at.conf`, add the attritbutes that descibe the class of service. Include a unique oid number for each attribute you add. In the following example, the attributes `cost`, `diskspace`, `webmail`, and `calendar` will be used to describe various aspects of the new service classes. The attribute `calClass` is used to define the MySiroe class.

Figure 6-5 Adding CoS attributes to Directory schema.

```
attribute cost 2.16.840.1.113730.3.1.554 cis
attribute diskspace 2.16.840.1.113730.3.1.555 cis
attribute webmail 2.16.840.1.113730.1.556 cis
attribute calendar 2.16.840.1.11370.1.557 cis
attribute calClass 2.16.840.1.11370.1.558 cis
```

3. In the file `<server_root>/slapd-<identifier>/config/slapd.user_oc.conf`, add a new Class of Service objectclass at the end of the file. In the Siroe example, the new object class is `calUser`.

Figure 6-6 Adding a CoS objectclass to Directory schema..

```
objectclass calUser
    oid 2.16.840.1.11370.3.2.116
    superior top
    allows
    cost,
    diskspace,
    webmail,
    calendar,
    calclass
```

4. Start Directory Server.

Modifying Existing User Entries

Define the Class of Service and modify Access Control Instructions (ACIs) as necessary. The changes you make will depend upon the classes you're setting up. To implement the classes of service for the Siroe company (Table 6-1 on page 110), the following entries were added to the directory using the `ldapmodify` utility.

Figure 6-7 The following entry adds the top of the Class of Service template tree to `o=ISP`

```
dn: ou=COS, o=ISP
objectclass: top
objectclass: organizationalunit
```

Figure 6-8 The following entry adds the COS schema named MySiroe to the directory.

```
dn: uid=MySiroe, ou=COS, o=ISP
objectclass: top
objectclass: account
objectclass: cosDefinition
cosTargetTree: ou=People, o=Siroe
cosTemplateDn: ou=MySiroeClasses, ou=COS, o=ISP
cosSpecifier: calClass
cosAttribute: cost
cosAttribute: diskspace
cosAttribute: webmail
cosAttribute: calendar
```

In Figure 6-8, the following CoS classes and attributes are defined as follows:

Object Class or Attribute	Description
`cosDefinition`	Object class that defines the COS schema entry.
`cosTemplateDN`	Multi-valued attribute that contains the subtree under which the service class templates for this schema are stored.
`cosSpecifier`	Multi-valued attribute that contains the name of another attribute in the directory schema. For Directory server 4.1x, you can only use one `cosSpecifier` per COS schema.
`cosAttribute`	Attribute that conains the attributes you want the COS plug-in to dynamically add to entries.

Figure 6-9 The following entry adds appriopriate ACI to `o=Siroe` that allows all administrators to view the new class of service.

```
dn: o=ISP
changetype: modify
add: aci
aci: (target=”ldap:///ou=COS, o=ISP”)(targetattr=”*”)(version
 3.0; acl
“Access to all for read/search”; allow (read,search)
 userdn=”ldap:///all”;)
```

Figure 6-10 The following entry adds the Premium CoS to Bill Johnson’s entry.

```
dn: uid=bill,ou=People,o=Siroe,o=ISP
changetype: modify
add: objectclass
objectclass: calUser
-
add: calclass
calclass: Premium
```

The examples used in this section affects existing user entries only. To automatically include the new attributes and classes to all new user entries, you must change the Delegated Administrator configuration. For more information, see Chapter 14, “Customizing Configuration in the Directory.”

Adding CoS Templates

Figure 6-11 The following entry creates the top of the MySiroeClasses template tree.

```
dn: ou=MySiroeClasses, ou=COS, o=ISP
objectclass: top
objectclass: organizationalUnit
```

Figure 6-12 The following template adds the Premium class to MySiroeClasses.

```
dn: uid=Premium, ou=MySiroeClasses, ou=COS, o=ISP
objectclass: top
objectclass: account
objectclass: calUser
cost: 30
diskspace: 30MB
webmail: yes
calendar: yes
```

Figure 6-13 The following template adds the Deluxe class to MySiroeClasses:

```
dn: uid=Deluxe, ou=MySiroeClasses, ou=COS, o=ISP
objectclass: top
objectclass: account
objectclass: calUser
cost: 20
diskspace: 20MB
webmail: yes
calendar: yes
```

Figure 6-14 The following template adds the Promotional class to MySiroeClasses:

```
dn: uid=Promotional, ou=MySiroeClasses, ou=COS, o=ISP
objectclass: top
objectclass: account
objectclass: calUser
cost: 0
diskspace: 10MB
webmail: yes
calendar: no
```

Figure 6-15 The following template adds the Basic class to MySiroeClasses:

```
dn: uid=calclass-default, ou=MySiroeClasses, ou=COS, o=ISP
objectclass: top
objectclass: account
objectclass: caluser
cost: 0
diskspace: 5MB
webmail: yes
calendar: no
```

Part 3

User Data Management

Chapter 7, “Top-level Administrators”

Chapter 8, “Top-level Help Desk Administrators”

Chapter 9, “Organization Administrators”

Chapter 10, “Organization Help Desk Administrators”

Chapter 11, “Group Administrators”

Chapter 12, “End Users as Administrators”

Chapter 7

Top-level Administrators

This chapter provides step-by-step instructions that a Top-level administrator will need on a day-to-day basis. The topics included in this chapter are:

- Logging In
- The Top-level Administration Page
- Managing the Top Level
- Managing Organizations
- Managing Groups
- Managing User Accounts
- Mail Lists
- My Account

Logging In

The user ID and password you use to log in determines your administrator role and determines which branches of the directory you have access to. There are two ways you can log in to Delegated Administrator.

- If you are using the default Delegated Administrator tree, and you are using the sample data that shipped with the product, you can use the Start Page to help you get started. See "The Start Page" on page 43 for more information. Once you're familiar with the product and with your administrator role, you can bypass the Start Page you go directly to the Login window to log in.
- If you have modified the Delegated Administrator tree, or you are not using the sample data that shipped with the product, you will not see the Start Page. You must log in using the Login window. See "Using the Login Window" on page 128 for more information.

Using the Start Page

The Start Page was designed to provide all the information you need to quickly begin using Delegated Administrator with sample data and the default organization `Siroe.com`.

NOTE If you installed Delegated Administrator against an existing directory, this sample data was not automatically installed. Skip to the next section, "Using the Login Window" on page 128.

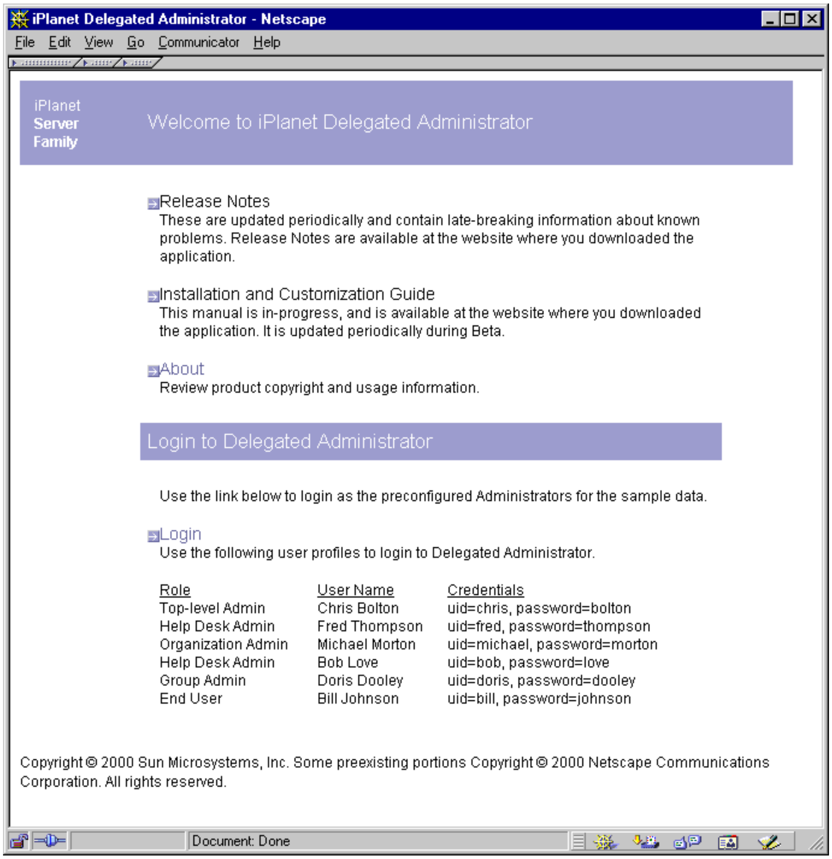
You can access the Start Page at any time by pointing a web browser to `http://<host_name>:<port>/nda/start.html`

You can use the Start Page to log in as any level of administrator named in the page. The user ID and password you use to log in determines your administrator role and determines which branches of the directory you have access to.

To start Delegated Administrator from the Start Page

1. Point a browser to the URL for the Delegated Administrator host using the form `http://<host:webserver_port>/nda/start.html`.

Figure 7-1 The Start Page



iPlanet Delegated Administrator - Netscape
File Edit View Go Communicator Help

iPlanet **Server Family**

Welcome to iPlanet Delegated Administrator

Release Notes
These are updated periodically and contain late-breaking information about known problems. Release Notes are available at the website where you downloaded the application.

Installation and Customization Guide
This manual is in-progress, and is available at the website where you downloaded the application. It is updated periodically during Beta.

About
Review product copyright and usage information.

Login to Delegated Administrator

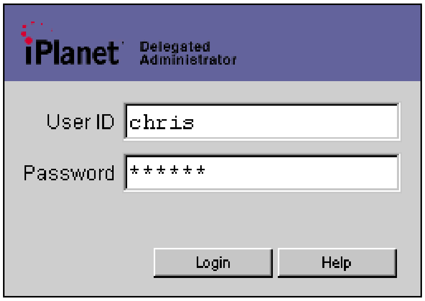
Use the link below to login as the preconfigured Administrators for the sample data.

Login
Use the following user profiles to login to Delegated Administrator.

Role	User Name	Credentials
Top-level Admin	Chris Bolton	uid=chris, password=bolton
Help Desk Admin	Fred Thompson	uid=fred, password=thompson
Organization Admin	Michael Morton	uid=michael, password=morton
Help Desk Admin	Bob Love	uid=bob, password=love
Group Admin	Doris Dooley	uid=doris, password=dooley
End User	Bill Johnson	uid=bill, password=johnson

Copyright © 2000 Sun Microsystems, Inc. Some preexisting portions Copyright © 2000 Netscape Communications Corporation. All rights reserved.

2. Click Login.



User ID chris

Password ******

In the Delegated Administrator Login window, using the information on the Start Page, enter an administrator's system user ID and password. For example, to log in as the Service Administrator, Chris Bolton, enter the following:

User ID. chris

Password. bolton

3. Click Login.

   Delegated Administrator displays the administration page that is appropriate for the User ID you entered. By default, your Delegated Administrator session will time out after thirty minutes of inactivity.

Using the Login Window

If you want to bypass the Start Page, or if the Start Page is not available to you, you can start Delegated Administrator and go directly to the Login window in one step.

To Start Delegated Administrator and Log In:

1. Point a browser to the URL for the Delegated Administrator host. Example:

   ```
   http://<host_name>:<port>/nda/default/en/login.html
   ```

2. In the Login window, enter your system user ID and password.

3. Click Login.

   Delegated Administrator displays the administration page that is appropriate for your administrator role. By default, your Delegated Administrator session will time out after thirty minutes of inactivity.

The Top-level Administration Page

The Top-level administrator page provides access to all features and functions you're allowed to access. Figure 7-2 provides a quick tour of the page.

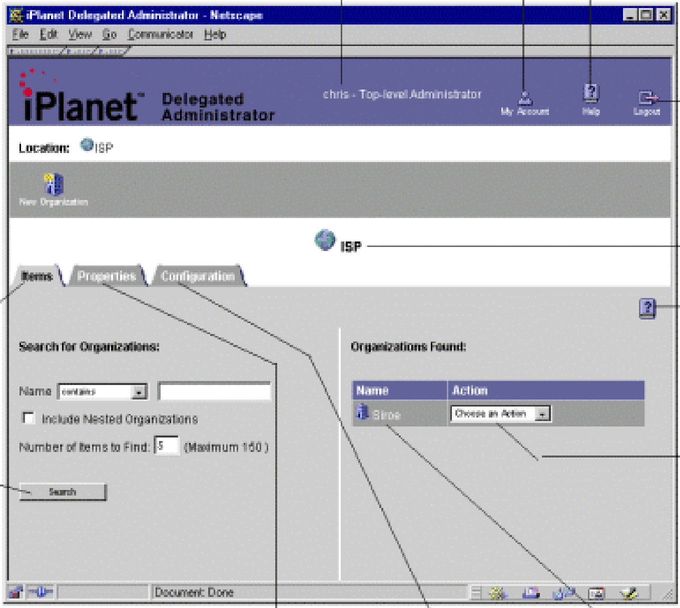
Figure 7-2 The Top-level administration page.

Location Bar.
The last object listed here is the level you're at in the Delegated Administrator tree. To navigate to another level in the list, click its name.

Administrator Name.
Displays the user ID and the administrator role of the person who logged in.

My Account.
Click this icon when you want to modify your own user account information.

Help.
Click this icon when you want information about all the tasks the Top-level administrator can perform.



Location: ISP

ISP

Search for Organizations:

Name contains

□ Include Nested Organizations

Number of Items to Find: 5 (Maximum 150)

Organizations Found:

Name	Action
Siroe	Choose an Action

Logout.
Click this icon when you want to end the current Delegated Administrator session

Task Bar.
Displays only the tasks you're allowed to perform. To begin a task, click its icon.

Object Name.
Indicates the organization or group managed by this administration page.

Items.
Click this tab when you want to locate an organization, group or user.

Help.
Click this icon when you need information about the data that's displayed or to be entered under this tab

Search.
Enter search criteria, and then click this button to generate a list of organizations within the Top Level.

Action.
Use the drop-down list to edit or remove the organization, group, or user named in the left column.

Properties.
Click this tab when you want to add administrators to or remove administrators from the Top Level, or when you want to change settings for the Top Level.

Configuration.
Click this tab when you want to modify configuration information used by Delegated Administrator.

Name.
Click the name of an organization, group or user to display its administration page.

Using the Location Bar

The Location Bar indicates you where you are in the directory tree. The last object listed indicates the object that is managed by the administration page. Objects are also represented by the following icons:

Base suffix. There is only one base suffix. This icon represents the top level of the Delegated Administrator tree.

Organization. This icon represents an organization or suborganization.

Group. This icon represents a group or subgroup.

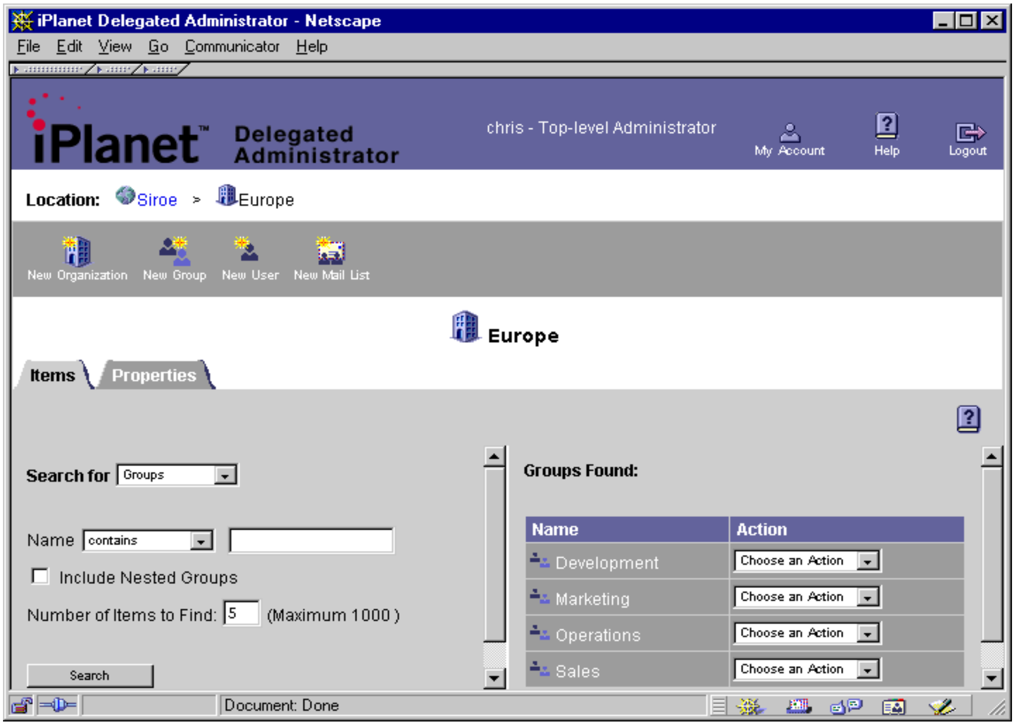
To navigate to the administration page for a different organization or group, click its name or icon in the Location Bar.

NOTE Do not use the Back and Forward buttons in your browser to navigate to administration pages in Delegated Administrator. If you use the Back and Forward buttons in your browser, the Location Bar will not properly display your location in the Delegated Administrator tree.

Using the Search Feature

You'll see two forms of the Search feature, but they work similarly. Figure 7-3 illustrates the Search feature embedded in the Items tab. Use the Search feature in the Items tab when you want to navigate further down in the tree, or when you want to edit or delete a user, group, or organization. Figure 7-4 shows a discrete Search window invoked when performing a task such as adding a new administrator from within the Properties Tab.

Figure 7-3 The Search feature embedded in the Items tab.


iPlanet Delegated Administrator - Netscape
File Edit View Go Communicator Help
iPlanet™ Delegated Administrator
chris - Top-level Administrator
My Account
Help
Logout
Location: Siroe > Europe
New Organization
New Group
New User
New Mail List
Europe
Items
Properties
Search
Document: Done

Search for: Groups

Name: contains

☐ Include Nested Groups

Number of Items to Find: 5 (Maximum 1000)

Groups Found:

Name	Action
Development	Choose an Action
Marketing	Choose an Action
Operations	Choose an Action
Sales	Choose an Action

To Locate a Directory Object From the Items Tab

1. Enter the following search criteria:

   Search for. Use the drop-down list to indicate whether you're searching for an organization, group, user, or mail list.

   Name. Enter the name of the directory object. Use the drop-down list to narrow your search criteria.

   Include Nested Organizations. If you want to search recursively through all suborganizations under the selected organization, select this option.

   Number of Items to Find. Enter the number of search results you want to see displayed. The default is 5, but you can enter a number up to 150.

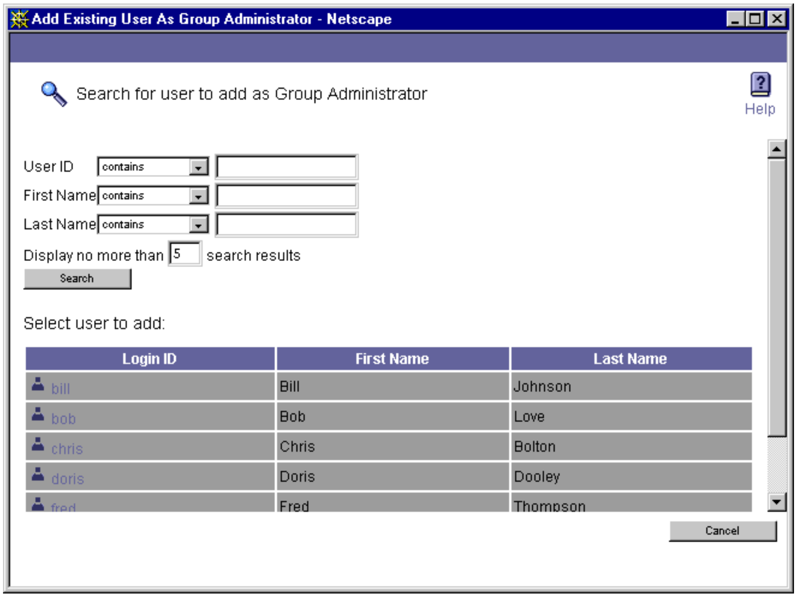
2. Once you locate a user, group, or organization in the results list, do one of the following:

- Click the object’s name to view and edit its settings or properties.
- Choose an action from the corresponding Action drop-down list.

To Locate a User Using a Search Window

A Search window is automatically displayed when you want to add an existing user to a group.

Figure 7-4 A Search window is invoked when adding an administrator to a group.



Add Existing User As Group Administrator - Netscape

Search for user to add as Group Administrator

User ID contains

First Name contains

Last Name contains

Display no more than 5 search results

Select user to add:

Login ID	First Name	Last Name
bill	Bill	Johnson
bob	Bob	Love
chris	Chris	Bolton
doris	Doris	Dooley
fred	Fred	Thompson

1. Enter one or more of the following, using the drop-down lists to narrow your search criteria:

   User ID. Enter the user’s system user ID as assigned by a network administrator.

   First Name. Enter the user’s given name as it appears in official records.

   Last name. Enter the user’s surname as it appears in official records.

NOTE If you do not enter information in any of these fields, Delegated Administrator will generate a list of all user entries within the level, organization, or group you’ve selected. If there are more than 5000 users within this scope, the search could take a long time.

Display no more than. Enter the number of search results you want to see displayed. The default is 5, but you can enter a number up to 150.

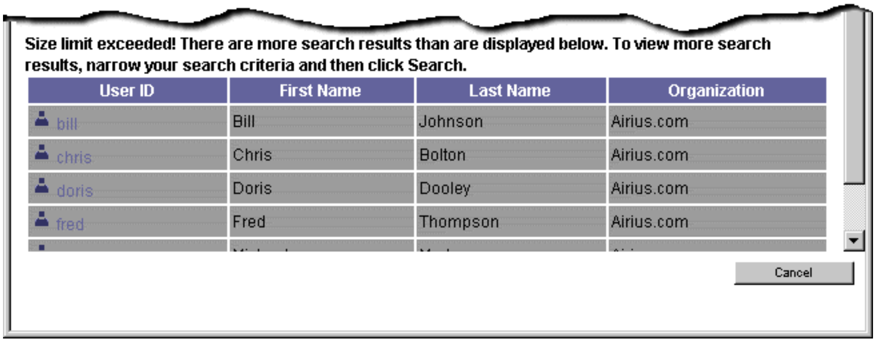
2. Click Search.

   Delegated Administrator generates a list of users within your scope of responsibility that match the criteria you've specified.

Exceeding the Search Results Size Limit

If you see the message regarding size limit (see Figure 7-5), the search operation found more results than the number you specified above, and cannot display all the results. When this happens, you can either enter a greater number in the **Display no more than....** field above, or you can enter more specific search criteria and begin the search again.

Figure 7-5 Size limit message.



Size limit exceeded! There are more search results than are displayed below. To view more search results, narrow your search criteria and then click Search.

User ID	First Name	Last Name	Organization
bill	Bill	Johnson	Airius.com
chris	Chris	Bolton	Airius.com
doris	Doris	Dooley	Airius.com
fred	Fred	Thompson	Airius.com

Managing the Top Level

The Top-level administrator has unlimited access privileges, and can modify any organization, group, or user account within the Delegated Administrator tree. This administrator typically is the person who deploys Delegated Administrator and who creates the first level of administrators and organizations.

NOTE **A Top-level administrator cannot create new user accounts or new mail lists at the top level of the tree. To create a new user or mail list, you must navigate down to an organization or group administration page, and then create the user or mail list at that level.**

The Top-level administrator can delegate his or her responsibilities to other Top-level administrators. This is done by adding users to the Top-level Administrator groups.

Adding Top-level Administrators

Add an existing user to the Top-level Administrators group if you want the user to share the Top-level administration duties. When you add a user to the Top-level Administrators group, you extend to that user all the access privileges accorded the group.

NOTE	**You cannot create a new user at the top level of the tree. To create a new user, you must navigate down to an organization or group administration page, and then create the user at that level.**

To Add a Top-level Administrator

1. In the Top-level administration page, click the Properties tab.
2. In the Properties tab, click the Add button beside the list of Top-Level Administrators.
3. In the Add Existing User window, use the Search feature to locate and select the user you want to add to the Top-level administrator’s group.
4. In the UserID column, click the user you want to add to the Top-level Administrators group.
5. In the Status window, click Continue.

   The user is added to the Top-level Administrators group, and now has all access privileges accorded this group. The administrator’s user ID is displayed in the Top-level Administrators list.

Removing Top-Level Administrators

When you remove a member of the Top-level Administrators group, that user no longer has access privileges accorded to the group. The user’s account is not deleted from the user directory.

To Remove a Top-Level Administrator

1. In the Top-level administrator page, click the Properties tab.
2. In the Properties tab, in the Top-level Administrators list, click the user ID of the administrator you want to remove.
3. Click the Remove button beside the Top-level Administrators list.
4. In the Status window, click Continue.

   The user is removed from the Top-level Administrators list, and no longer has the access privileges accorded this group.

Adding Top-Level Help Desk Administrators

Add an existing user to the Top-level Help Desk Administrators group if you want the user to be able to modify users’ passwords. When you add a user to the Top-level Help Desk Administrators group, you extend to that user all the access privileges accorded the group. Help Desk Administrators, by default, can modify only user passwords within their scope of access.

To Add a Top-level Help Desk Administrator

1. In the Top-level administration page, click the Properties tab.
2. In the Properties tab, click the Add button beside the list of Top-Level Help Desk Administrators.
3. In the Add Existing User window, use the Search feature to locate the user you want to add to the Top-level Help Desk Administrator’s group.
4. In the UserID column, click the user you want to add to the Top-level Help Desk Administrators group.
5. In the Status window, click Continue.

   The user is added to the Top-level Help Desk Administrators group, and now has all access privileges accorded this group. The administrator’s user ID is displayed in the Top-level Help Desk Administrators list.

Removing Top-Level Help Desk Administrators

When you remove a member of the Top-level Help Desk Administrators group, that user no longer has access privileges accorded to the group. The user's account is not deleted from the user directory.

To Remove a Top-Level Help Desk Administrator

1. In the top-level administrator page, click the Properties tab.
2. In the Properties tab, in the Top-level Help Desk Administrators list, click the user ID of the administrator you want to remove.
3. Click the Remove button beside the Top-level Help Desk Administrators list.
4. In the Status window, click Continue.

   The user is removed from the Top-level Administrators list, and no longer has the access privileges accorded this group.

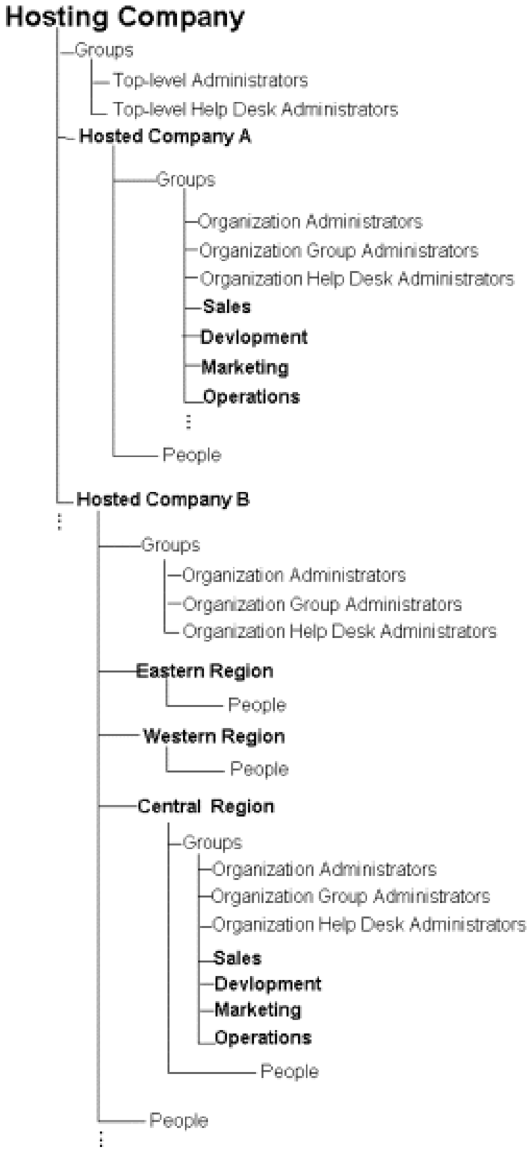
Managing Organizations

As a Top-level administrator, you can perform any tasks that an organization administrator can perform. Use the Search feature to locate the organization you want to manage, and then navigate to its administration page.

Creating a New Organization

Create a new organization when you want to manage a large number of user accounts in one container in the directory. You can create an organization at the top level of the Delegated Administrator tree; you can create an organization within another organization. You cannot create an organization within a group. When you create a new organization, the new organization is located one level down in the directory. For example, see Figure 7-6 on page 137. A company creates two levels of organizations. At the top level, a Top-level administrator creates two organizations, Hosted Company A and Hosted Company B. These are *peer* organizations because they are created at the same level in the directory tree. Under Hosted Company B, an Organization Administrator creates three new organizations, one level down in the directory: Eastern Region, Western Region, and Central Region. Each contains a separate People container.

Figure 7-6 Peer organizations.


Hosting Company
Groups
Top-level Administrators
Top-level Help Desk Administrators
Hosted Company A
Groups
Organization Administrators
Organization Group Administrators
Organization Help Desk Administrators
Sales
Devlopment
Marketing
Operations
People
Hosted Company B
Groups
Organization Administrators
Organization Group Administrators
Organization Help Desk Administrators
Eastern Region
People
Western Region
People
Central Region
Groups
Organization Administrators
Organization Group Administrators
Organization Help Desk Administrators
Sales
Devlopment
Marketing
Operations
People
People

Limiting the Number of Objects in an Organization

You can limit the number of suborganizations, groups, or user accounts that may be included in the new organization. Limits are useful for two reasons. First, they optimize Delegated Administrator performance. Searches performed on organizations with fewer than 5000 users, or fewer than 50 suborganizations, take less time to process.

Secondly, limits can help you comply with parameters set by your company. For example, the Siroe company's fee structure is based on the number of users in an organization; organizations with more than 5000 users are charged more for service than organizations with fewer than 5000 users. When creating new organizations, the Siroe administrator limits the number of organizations to 5000.

To Create a New Organization

1. In the Top-level administration page, in the task bar, click the New Organization icon.
2. In the Create Organization window, enter the following:

   Organization name. Enter a name as you want it to appear in your company's official records. The name can include spaces and numbers.

   Suborganization limit. Enter the maximum number of suborganizations allowed in the organization.

   Group limit. Enter the maximum number of groups allowed in the organization.

   Mail list. Enter the maximum number of mail lists allowed in the organization.

   User account limit. Enter the maximum number of user accounts allowed in the organization.
3. Click OK.
4. In the Status window, click Continue.

   The new organization is created one level down in the directory tree.

To Edit Organization Limits

1. Navigate to the top-level or organization administration page under which the organization was created.
2. Use the Search feature to generate a list of organizations.

3. In the Search results, in the right pane, click the name of the organization you want to edit.
4. In the Organization administration page, click Properties.
5. In the Properties tab, modify the following as necessary:

   Suborganizations. Indicates the number of suborganizations that currently exist under the organization.

   Suborganization limit. Enter the maximum number of suborganizations allowed in the organization.

   Groups. Indicates the number of groups that currently exist under the organization.

   Group limit. Enter the maximum number of groups allowed in the organization.

   User accounts. Indicates the number of user accounts that currently exist under the organization.

   User account limit. Enter the maximum number of user accounts allowed in the organization.

   Mail lists. Indicates the number of mail lists that currently exist under the organization.

   Mail list limit. Enter the maximum number of mail lists allowed in the organization.
6. Click Save.

Creating a Suborganization

When you create an organization within another organization, the new object is called a *suborganization*.

To Create a Suborganization

1. Navigate to the administration page of the organization under which the suborganization will be created.
2. In the organization administration page, in the task bar, click the New Organization icon.
3. In the Create Organization window, enter the following:

Organization name. Enter a name as you want it to appear in your company's official records. The name can include spaces and numbers.

Suborganization limit. Enter the maximum number of suborganizations allowed in the organization.

Group limit. Enter the maximum number of groups allowed in the organization.

User account limit. Enter the maximum number of user accounts allowed in the organization.

4. Click OK.
5. In the Status window, click Continue.

Adding Organization Administrators

Add an existing user to the Organization Administrators group if you want the user to share the administration duties at the organization level. When you add a user to the Organization Administrators group, you extend to that user all the access privileges accorded the group.

To Add an Organization Administrator

1. Navigate to the organization under which the Organization Administrators group is located.
2. In the Top-level administration page, click the Properties tab.
3. In the Properties tab, click the Add button beside the list of Organization Administrators.
4. In the Add Existing User window, use the Search feature to locate and select the user you want to add to the Organization Administrator's group.
5. In the UserID column, click the user you want to add to the Organization Administrators group.
6. In the Status window, click Continue.

The user is added to the Organization Administrators group, and now has all access privileges accorded this group. The administrator's user ID is displayed in the Organization Administrators list.

Removing Organization Administrators

When you remove a member of the Organization Administrators group, that user no longer has access privileges accorded to the group. The user's account is not deleted from the user directory.

To Remove a Organization Administrator

1. Navigate to the organization under which the Organization Administrators group is located.
2. In the organization administrator page, click the Properties tab.
3. In the Properties tab, in the Organization Administrators list, click the user ID of the administrator you want to remove.
4. Click the Remove button beside the Organization Administrators list.
5. In the Status window, click Continue.

The user is removed from the Organization Administrators list, and no longer has the access privileges accorded this group.

Adding Organization Help Desk Administrators

Add an existing user to the Organization Help Desk Administrators group if you want the user to be able to modify the passwords of other users in the organization. When you add a user to the Organization Help Desk Administrators group, you extend to that user all the access privileges accorded the group. Help Desk Administrators, by default, can modify only user passwords within their scope of access.

To Add an Organization Help Desk Administrator

1. In the Organization administration page, click the Properties tab.
2. In the Properties tab, click the Add button beside the list of Organization Help Desk Administrators.
3. In the Add Existing User window, use the Search feature to locate and select the user you want to add to the Organization Help Desk Administrator's group.
4. In the UserID column, click the user you want to add to the Organization Help Desk Administrators group.

5. In the Status window, click Continue.

The user is added to the Organization Help Desk Administrators group, and now has all access privileges accorded this group. The administrator's user ID is displayed in the Organization Help Desk Administrators list.

Removing Organization Help Desk Administrators

When you remove a member of the Organization Help Desk Administrators group, that user no longer has access privileges accorded to the group. The user's account is not deleted from the user directory.

To Remove an Organization Help Desk Administrator

1. Navigate to the organization under which the user is located.
2. In the organization administration page, click the Properties tab.
3. In the Properties tab, in the Organization Help Desk Administrators list, click the user ID of the administrator you want to remove.
4. Click the Remove button beside the Organization Help Desk Administrators list.
5. In the Status window, click Continue.

The user is removed from the Organization Help Desk Administrators list, and no longer has the access privileges accorded this group.

Deleting an Organization

When you delete an organization, its entry is deleted from the directory.

To Delete an Organization

1. Navigate to the organization administration page that manages the organization you want to delete.
2. Use the Search feature to locate the organization you want to delete.
3. In the Search results list, in the right pane, find the organization you want to edit, and then from its drop-down list, choose Delete.
4. When you see the confirmation message, click OK.

Managing Groups

As a Top-level administrator, you can also perform any task that a Group administrator can perform.

Creating a New Group

Create a new group when you want to associate a number of users under one name. For example, in the Siroe company, all Sales employees are considered members of the Sales Department even though their user accounts might be stored in other parts of the organization. You can create a group within an organization; you can create a group within another group. You cannot create a new group at the top level of the Delegated Administrator tree.

Limiting the Number of Objects in an Group

You can limit the number of groups, or user accounts that may be included in the new groups. Limits are useful for two reasons. First, they optimize Delegated Administrator performance. Searches performed on groups with fewer users take less time to process.

Secondly, limits can help you comply with parameters set by your company. For example, the Siroe company’s fee structure is based on the number of users in an group; groups with more than 5000 users are charged more for service than groups with fewer than 5000 users. When creating new groups, the Siroe administrator limits the number of users to 5000.

To Create a New Group

1. Navigate to the administration page for the organization in which the group will be created.
2. In the organization administration page, in the task bar, click New Group.
3. In the Create Group window, enter the following:

   Group name. Enter a name as you want it to appear in your company's official records. The name can include spaces and numbers.

   Nested group limit. Enter the maximum number of subgroups allowed in the group.

   User account limit. Enter the maximum number of user accounts allowed in the group.
4. Click OK.
5. In the Status window, click Continue.

To Edit Group Limits

1. Navigate to the organization administration page that manages the group you want to edit.
2. In the organization administration page, use the Search feature to generate a list of groups within the organization.
3. In the Search results, in the right pane, locate the group you want to edit, and then use its drop-down list to choose Edit.
4. Modify the following as necessary:

   Nested groups. Indicates the number of subgroups that currently exist under the group.

   Nested group limit. Enter the maximum number of subgroups allowed in the group.

   User accounts. Indicates the number of user accounts that currently exist under the group.

   User account limit. Enter the maximum number of user accounts allowed in the group.
5. Click Save.

Creating a Subgroup

When you create a group within another group, the new object is called a *subgroup*. Create a subgroup when you want to associate a number of users under one name.

1. Navigate to the administration page for the group in which the subgroup will be created.
2. In the group administration page, in the task bar, click New Group.
3. In the Create Group window, enter the following:

   Group name. Enter a name as you want it to appear in your company's official records. The name can include spaces and numbers.

   Nested group limit. Enter the maximum number of subgroups allowed within the subgroup.

   User account limit. Enter the maximum number of user accounts allowed in the subgroup.
4. Click OK.
5. In the Status window, click Continue.

Adding a User to a Group

Top-level and Organization Administrators have appropriate access permissions to add any user to one or more groups. For example, a Top-level or Organization administrator can add the user named Jayne Doe to the Human Resources group and to the Executives group. However, the Group administrator's access permissions are limited in two respects:

- The Group administrator cannot add the same user to two different groups. For example, a Group administrator cannot add the user Jayne Doe to both the Human Resources group and to the Executives group; the Group administrator can only add Jayne Doe to the Human Resources group *or* to the Executives group.
- The Group administrator cannot add members of Top-level or Organization administrator groups to another group. For example, if Jayne Doe belongs to the Top-level Administrators group or to the Organization Administrators group, a Group administrator cannot add her to a any other group.

Group administrators add users to groups in one of two ways: by adding a new user to the group, or by adding an existing user to a group.

To Add an Existing User to a Group

1. Navigate to the administration page for the organization under which the group was created.
2. Use the Search feature to locate and select the group to which the user will belong.
3. In the group administration page, in the task bar, click Add Existing User.
4. In the "Search for user to add as Group Member" window, locate and click the User ID of the user you want to add to the group.
5. Click OK.

To add a New User to a Group

1. Navigate to the administration page for the organization under which the group was created.
2. Use the Search feature to locate and select the group to which the new user will belong.
3. In the group administration page, in the task bar, click New User.
4. In the New User window, click Basic Account Information. Skip to step 4 of To Create a New User Account in the section "Managing User Accounts."

Adding Group Administrators

Add an existing user to the Group Administrators list if you want the user to be able to create new groups or modify the user accounts within a group. When you add a user to the Group Administrators list, you extend to that user all the access privileges accorded the group. Group Administrators, by default, can modify most information in the User Account Information window.

To Add a Group Administrator

1. In the organization administration page, under the Items tab, search for the group to which the new Group Administrator will belong.
2. In the Properties tab, click the Add button beside the list of Group Administrators.
3. In the Add Existing User window, use the Search feature to locate and select the user you want to add to the Group Administrators list.

4. In the UserID column, click the user you want to add to the Group Administrators list.
5. In the Status window, click Continue.

The user is added to the Group Administrators list, and now has all access privileges accorded this group. The administrator's User ID is displayed in the Organization Administrators list.

Removing Group Administrators

When you remove a member of the Group Administrators group, that user no longer has access privileges accorded to the group. The user's account is not deleted from the user directory.

To Remove a Group Administrator

1. In the Organization administration page, under the Items tab, search for the group to which the Group Administrator belongs.
2. In the Properties tab, in the Group Administrators list, click the UserID of the administrator you want to remove.
3. Click the Remove button beside the Group Administrators list.
4. In the Status window, click Continue.

The user is removed from the Group Administrators list, and no longer has the access privileges accorded this group.

Removing a User from a Group

When you remove a user from a group, the individual's user ID is no longer associated with the group; the user entry remains in the directory. This is not the same as *deleting* a user account. When you delete a user account, the individual's entry is deleted from the user directory. (See Deleting a User Account.)

To Remove a User from a Group

1. Navigate to the administration page for the organization under which the group was created.
2. Use the Search feature to generate a list of groups within the organization.

3. In the Search results, in the right pane, locate the name of the user you want to remove, and then use its drop-down list to choose Remove.
4. When you see the confirmation message, click OK.

Deleting a Group

When you delete a group, its entry is deleted from the user directory.

To Delete a Group

1. Navigate to the organization or group administration page that manages the group.
2. Use the Search feature to generate a list of groups within the organization or group.
3. In the Search results, in the left pane, locate the group you want to delete, and then use its drop-down list to choose Delete.

Managing User Accounts

As a Top-level administrator, you cannot create user accounts in the top level of the Delegated Administrator tree. You must navigate to the administration page of the organization or group where the new user account will be created.

Creating a New User Account

Create a new account when you want to add a user to the directory.

To Create a New User Account

1. Navigate to administration page for the organization or group to which the user will belong.
2. In organization or group administration page task bar, click New User.
3. In the New User window, in the Basic Account Information pane, enter the following required information:

   Login ID. Enter the user’s system user ID as assigned by a network administrator.

First name. Enter the user's given name as it appears on official company records.

Last name. Enter the user's surname as it appears in company records.

Password. Enter the user's password.

Confirm password. Enter the user's password again to confirm it.

Organization. Enter the published name of the organization the user belongs to. Example: Sales Department.

Title. Enter the user's job title as it appears on official company records. Example: Sales Associate.

Manager. Enter the distinguished name (DN) of the user's manager. Example: cn=Babs Jensen.

Email address. Enter the user's email address. Example: ginac@siroe.com.

Telephone number. Enter the user's phone number as it appears in company records. Example: 454-555-4444.

Fax number. Enter the user's fax number as it appears in company records. Example: 454-555-4444.

Mobile number. Enter the user's mobile or cell phone number as it appears in company records. Example: 454-555-4444.

Pager number. Enter the user's pager number as it appears in company records. Example: 454-555-4444.

Mailing address. Enter a street address where the user can receive print mail or packages. Example: 1234 Main Street, Anytown, AnyState.

Web Page URL. Enter the URL for a web page that contains more information about the user. Example: http://www.siroe.com/sales/reps

Description. Enter a word or phrase that describes the web page above. Example: Sales Reps.

Preferred Language. Use the drop-down list to indicate the user's preferred language. Delegated Administrator will display the user interface localized for the preferred language. For example, the Siroe company has employees in Japan, and they have indicated they prefer to conduct business in Japanese. When the Siroe administrator sets this preference to Japanese for a user, Delegated Administrator displays the Japanese version of the user interface.

4. If Class of Service is used, click it and enter the appropriate information.

5. If Basic Mail Information is displayed, click it and then enter the following information:

   Mail host: Enter the Messaging Server host name. This is the machine hosting the Messaging Server that will process this user's mail. This must be the fully-qualified domain name (FQDN) known to the Messaging Server on that machine.

   Alternative email addresses: An alternate address is essentially an alias for the user's primary address. You can use this feature to:

   - Ensure proper delivery of frequently misspelled addresses (such as "Smith" as an alias for "Smithy").
   - Enable host name hiding in outgoing mail headers. To do so, supply an alternate address that includes the host name and do not include the host name in the primary email address (see step 3).
   - You can specify any number of alternate addresses for a particular user, as long as each address is unique. Messages that arrive for any of these aliases are directed to the primary address.

   Access domains: Lists the access domains from which the user can retrieve mail.

NOTE If no access domains are specified in the Access domain field, the user can retrieve mail from any domain.

   To add an access domain:

   a. Click Add (next to the Access domains field) to open the Set Domain window, and then enter either a regular domain name or an IP address. You must enter only one access domain each time you open the Access Domain name window. If you specify a domain that does not exist, or enter none, you effectively block access for the user.

   b. Click OK.

   Allow following service(s): To enable mail services for a specific type of server, select one or more of the available options: IMAP, POP, and HTTP. Netscape Messaging Server supports the Post Office Protocol 3 (POP3), the Internet Mail Access Protocol 4 (IMAP4), and the HyperText Transfer Protocol (HTTP) for client access to mailboxes. IMAP and POP are both Internet-standard mailbox protocols. Messenger Express, a web-enabled electronic mail program, lets end users access their mailboxes using a browser running on an Internet-connected computer system using HTTP.

Can Create E-mail Lists. This option applies only to Group administrators and individual users. All higher-level administrators, by default, have full mail list privileges regardless of whether this option is selected for them. When you select this option for a Group administrator or individual user, the Manage Mail Lists option is displayed when the individual edits his own account information.

6. If Mail Delivery Options is displayed, click it and then enter the following information:

Deliver incoming messages to:

POP3/IMAP4 mailbox. Select this option if you want to configure delivery and access to an individual user's POP or IMAP mailboxes.

Message store name. Enter the name (nickname, not pathname) of the message store partition to which the user's incoming mail should be delivered, if other than the current default primary partition. The name must represent an existing partition. For information on the message store and instructions for creating partition nicknames, see the *Messaging Server Administrator's Guide*.

Mailbox disk quota. Specify an allocated storage limit for this user. Enter a number in the field and select the appropriate unit (KB or MB). The disk quota or allocated storage limit you specify applies to this user alone.

Unix mailbox. Select this option if you want messages to be delivered to the user's designated Unix mailbox. Unix delivery is available only to users whose Messaging Server runs on a Unix host machine.

Process incoming messages through one or more programs:

By default, incoming messages are put in the inbox of the mail account the message is addressed to. Accounts can be configured to perform various operations with the messages it receives. Examples include putting incoming messages in particular mail folders, forwarding them somewhere else, or generating an automatic response. For detailed information, see Chapter 12, "Program Delivery" in *Netscape Messaging Server Administrator's Guide*.

Enable the following programs: If you want to specify a mechanism for forwarding messages to an external application for processing before delivery to the user, select this option. Then enter the external application command(s) to be used for processing this user's mail.

Forward a copy of each message to: Enter another address instead of or in addition to the primary address for the user. This enables mail to automatically be forwarded to the specified address.

7. Click OK.

To Edit a User Account

1. Navigate to the administration page of the organization or group under which the user account was created.
2. Use the Search feature to generate a list of user accounts within the organization or group.
3. In the Search results, in the right pane, locate the user ID of the account you want to modify, and then use the drop-down list to choose Edit.
4. Modify the user account information as necessary. See Creating a New User Account for detailed information about each of the fields in this window.
5. Click OK.

Deleting a User Account

You cannot delete a user account at the top level. As a Top-level administrator, to delete a user account from the Delegated Administrator tree, you must navigate to the administration page for the organization or group under which the user account was created. When you delete a user account, his or her entry is deleted from the user directory.

To Delete a User Account

1. Navigate to the administration page for the organization or group under which the user account was created.
2. Use the Search feature to generate a list of users within the organization or group.
3. In the Search results, in the right pane, locate the name of the user name for the account you want to delete, and then use its drop-down list to choose Delete.
4. When you see the confirmation message, click OK.

Mail Lists

Mail lists make it possible for a user to send the same message to a number of other users at one time. A mail list specifies the email addresses (users) that receive all messages sent to a single email address. For example, in the Siroe company, if you send one email to the address `sales@Siroe.com`, each employee in the Sales Department will receive the email.

NOTE You cannot use Delegated Administrator to manage mail lists unless Netscape Messaging Server 4.x is installed and properly configured. See the *Installation and Customization Guide* for detailed information.

By default, only Top-level Administrators, Organization Administrators and Help Desk Administrator have access permissions to create and manage mail lists. Top-level and Organization administrators can extend mail list management privileges to other users by modifying their individual user accounts. See the field Can Create E-mail Lists in the section “To Create a New User Account.”

Mail List Owners

A mail list may have one or more owners assigned to it. The owner can perform all operations on the mail list including creating new mail lists and assigning owners. The owner can edit the properties of any mail list that he or she owns. If the owner is a properly authorized administrator or user, he or she can create mail lists and assign owners to the lists.

Moderated Mail Lists

You can assign a moderator to filter messages sent to the mail list. This is useful in preventing unrelated messages from being distributed to members of the mail list. When you designate a moderator, the mail list is known as a *moderated lis*t. In a moderated mail list, all messages sent by members of the mail list are sent to the moderator. The moderator either approves or rejects the messages, and then sends only approved messages to all members of the mail list.

Managing Mail Lists

By default, the following administrators have access privileges for managing mail lists:

- Top-level
- Organization
- Top-level Help Desk
- Organization Help Desk

Their access privileges allow them to create and delete mail lists, subscribe to mail lists, or unsubscribe from them. In contrast, Group administrators and individual users cannot create or manage mail lists until they are granted sufficient privileges by a Top-level or Organization administrator. There are three different paths to managing your mail lists. Your role as administrator or as an individual user determines which path you should use. Table 7-1 provides a summary of administrator mail management privileges and the paths they must take to manage mail lists.

Table 7-1 Accessing Mail List Management Options

Administrator	Default Mail List Privileges	Go To
Top-level	Can create, edit, delete lists; subscribe to or unsubscribe from lists.	Organization administration page
Organization	Can create, edit, delete lists; subscribe to or unsubscribe from lists.	Organization administration page
Help Desk	Can create, edit, delete lists; subscribe to or unsubscribe from lists.	My Account page
Group	Can subscribe to or unsubscribe from mail lists. Cannot create or edit mail lists until granted privileges by Top-level or Organization administrator.	My Account page
User Account	Can subscribe to or unsubscribe from mail lists. Cannot create or edit mail lists until granted privileges by Top-level or Organization administrator.	User Account administration page

Top-level and Organization Administrators' Mail Lists

Top-level and Organization administrates use organization administration pages to manage their mail lists.

To Create a New Mail List

1. Navigate to the administration page of the organization in which the mail list will be created.
2. In the task bar, click New Mail List.
3. In the New Mail List window, enter Mail List information. Skip to step 4 of To Create a New Mail List in the section "Managing Mail Lists."

To Edit a Mailing List

1. Navigate to the administration page for the organization in which the mailing list was created.
2. Use the Search feature to generate a list of mail lists in the organization.
3. In the Search results, in the right pane, locate the mailing list you want to edit. In the drop-down list, choose Edit.
4. In the Edit Mail List window, make changes as necessary. For detailed information about each field, see step 4 of To Create a New Mail List in the section "Managing Mail Lists."
5. Click OK.

To Subscribe to a Mailing List

1. Navigate to the administration page for the organization in which the mailing list was created.
2. Use the Search feature to generate a list of mail lists in the organization.
3. In the Search results, in the right pane, locate the mailing list you want to subscribe to. Use the drop-down list to choose Edit.
4. In the Edit Mail List window, click the Add button beside the Members list.
5. In the Add Members window, use the Search feature to locate your own user ID, and then click it. Your user ID is added to the Members list.
6. In the Edit Mail List window, click OK.

To Unsubscribe from a Mailing List

1. Navigate to the administration page for the organization in which the mailing list was created.
2. Use the Search feature to generate a list of mail lists in the organization.
3. In the Search results, in the right pane, locate the mailing list you want to unsubscribe from. Use the drop-down list to choose Edit.
4. In the Edit Mail List window, locate your user ID in the Members list, and then click it to select it.
5. Click the Remove button beside the Members list. Your user ID is deleted from the Members list.
6. In the Edit Mail List window, click OK.

To Delete a Mailing List

1. Navigate to the administration page for the organization in which the mailing list was created.
2. Use the Search feature to generate a list of mail lists in the organization.
3. In the Search results, in the right pane, locate the mailing list you want to delete. In the drop-down list, choose Delete.
4. When you see a confirmation message, click OK.

Help Desk Administrator's Mail Lists

Top-level Help Desk administrators and Organization Help Desk administrators manage mail lists through the My Account page.

To Create a New Mail List

1. Click My Account in the upper banner of your administration page.
2. In the My Account window, click Manage Mail Lists.
3. In the My Account Mail window, click Create Mail List.
4. In the New Mail List window, provide the following mail list information:

   Mail List Name. Enter a name that describes the mailing list. Example: Sales

Description. Enter a description of the purpose or nature of the mailing list. You can use this field to enter a URL to an HTML page providing additional information about the mailing list. This is for informational purposes only; the URL is not used by Messaging Server or by Delegated Administrator.

Primary Email Address. Enter the publicized address where mail for the mail list can be sent. There can be only one primary address, which must be a valid, correctly formatted SMTP address conforming to RFC 821 specifications.

Alternate Email Addresses. This field displays a list of alternate email addresses, or aliases to the primary email address. Click Add to modify the information in this field. Then, in the Set Mail Address window, provide the following information:

- Enter an alternate address. This is essentially an alias for the mail list's primary address. For example, if a user's primary address is `humanresources@siore.com`, you can enter `hr@siroe.com` as an alternate address. This ensures that list members will receive messages that are mistakenly addressed to "hr."
- You can specify any number of alternate addresses as long as each address is unique. Messages that arrive for any of these aliases are directed to the primary address.

Owners. To add an existing user to the Owners list, click the corresponding Add button. Then use the Search for User window to locate and select the user.

Members. To add a user to the mail list, click the corresponding Add button. Then use the Add Member window to locate and select the user.

Person for Bounced Messages. Enter the email address of the person, possibly a list owner or system administrator, to whom error messages should be sent when mail sent to the list bounces. The address you enter in this field must be a correctly-formatted, valid SMTP address conforming to RFC 821 specifications.

Allow users to join. If you want to allow users to add themselves to the mail list, choose Yes. If you want to restrict users from adding themselves to the mail list, choose No.

Show Members of List To. If you want the owners and members of this list to be able to view the members' names, choose All. If you want no owners or members to be able to view members' names, choose None.

Hide Mail List. If you want to make a mailing list visible to all users for subscription purposes, choose No. To make the mailing list visible to only Top-level and Organization Administrators, choose Yes.

Authorized Senders to List. Enter information regarding users, groups of users or specific domains that are allowed to post messages to the mailing list:

Anyone. Any user may contribute to the mailing list.

Anyone in the Mailing List. Only users included in the mailing list may contribute to the mailing list.

Anyone in the following list. If you want to allow specific individuals or groups of individuals to be able to post messages to the mailing list, click the associated radio button. Then specify the following:

Users and Groups. This fields displays the list of individual users and groups from which messages will be accepted for posting to this mailing list. To Add a user or group to the list, click the corresponding Add button. If no user or group is specified, there is no sender-user restriction.

DNS Domains. This fields displays the list of domains from which messages will be accepted for posting to this mailing list. To Add a domain name to the list, click the corresponding Add button. If no domain is specified, there is no sender-domain restriction.

When Message to this List is rejected:

Send message to Moderator(s). If you want to automatically forward rejected messages to the mailing-list moderator or moderators for further action, select this option. If you select this option, you must add at least one entry in the List moderators field. To add a user to the moderator list, click the corresponding Add button. Then use the Add Moderator window to locate and select a user.

5. Click OK.

To Edit a Mailing List

1. Click My Accounts in the upper banner of your administration page.
2. In the My Account window, click Manage Mail Lists.
3. In the Manage Mail Lists window, click Owned Mail Lists.
4. Use the Search feature to generate a list of your mail lists.
5. In the Search results, locate the mail list you want to edit, and click its name.
6. In the Edit Mail List window, make changes as necessary, and then click OK.

To Subscribe to a Mailing List

1. Click My Account in the upper banner of your administration page.
2. In the My Account window, click Manage Mail Lists.
3. Use the Search feature to generate a list of mail lists in the organization.
   a. Select Subscribe to generate a list of mail lists that you currently subscribe to.
   b. Select Unsubscribe to generate a list of available mail lists that you can subscribe to.
4. In the Search results, locate the mailing list you want to subscribe to, and then click Subscribe.
5. In the Subscribe Mail List window, click Subscribe.
6. In the Status window, click Continue.

To Unsubscribe from a Mailing List

1. Click My Account in the upper banner of your administration page.
2. In the My Account window, click Manage Mail Lists.
3. Use the Search feature to generate a list of mail lists in the organization.
   a. Select Subscribe to generate a list of mail lists that you currently subscribe to.
   b. Select Unsubscribe to generate a list of available mail lists that you can subscribe to.
4. In the Search results, locate the mailing list you want to unsubscribe from, and then click Unsubscribe.
5. In the Unsubscribe Mail List window, click Unsubscribe.
6. In the Status window, click Continue.

To Delete a Mailing List

1. In your administration page, use the Search feature to generate a list of Mail Lists.
2. In the Search results, in the right pane, locate the mailing list you want to delete. In the drop-down list, choose Delete.
3. When you see a confirmation message, click Continue.

Group and User Account Administrators' Mail Lists

Group administrators and individual users can create and manage mail lists only if they are granted mail list privileges from a Top-level or Organization administrator. Once a user is granted mail list privileges, the Manage Mail Lists option is displayed in their account information window.

To Create a New Mail List

1. In the top of the Group administration page, click My Account.
2. In the My Account window, click Manage Mail Lists.
3. In the My Account Mail window, click Create Mail List.
4. In the New Mail List window, provide the following mail list information:

   Mail List Name. Enter a name that describes the mailing list. Example: Sales

   Description. Enter a description of the purpose or nature of the mailing list. You can use this field to enter a URL to an HTML page providing additional information about the mailing list. This is for informational purposes only; the URL is not used by Messaging Server or by Delegated Administrator.

   Primary Email Address. Enter the publicized address where mail for the mailing list can be sent. There can be only one primary address, which must be a valid, correctly formatted SMTP address conforming to RFC 821 specifications.

   Alternate Email Addresses. This field displays a list of alternate email addresses, or aliases to the primary email address. Click Add to modify the information in this field. Then, in the Set Mail Address window, provide the following:

   - Enter an alternate address. This is essentially an alias for the mailing list'ss primary address. For example, if a primary address is `humanresources@siore.com`, you can enter `hr@siroe.com` as an alternate address. This ensures that list members will receive messages that are mistakenly addressed to "hr."
   - You can specify any number of alternate addresses for a mail list, as long as each address is unique. Messages that arrive for any of these aliases are directed to the primary address.

   Owners. To add an existing user to the Owners list, click the corresponding Add button. Then use the Search for User window to locate and select the user.

Members. To add a user to the mail list, click the corresponding Add button. Then use the Add Member window to locate and select the user.

Person for Bounced Messages. Enter the email address of the person, possibly a list owner or system administrator, to whom error messages should be sent when mail sent to the list bounces. The address you enter in this field must be a correctly-formatted, valid SMTP address conforming to RFC 821 specifications.

Allow users to join. If you want to allow users to add themselves to the mail list, choose Yes. If you want to restrict users from adding themselves to the mail list, choose No.

Show Members of List To. If you want the owners and members of this list to be able to view the members' names, choose All. If you want no owners or members to be able to view members' names, choose None.

Hide Mail List. If you want to make a mailing list visible to all users for subscription purposes, choose No. To make the mailing list visible to only Top-level and Organization Administrators, choose Yes.

Authorized Senders to List. Enter information regarding users, groups of users or specific domains that are allowed to post messages to the mailing list:

> **Anyone.** Any user may contribute to the mailing list.
>
> **Anyone in the Mailing List.** Only users included in the mailing list may contribute to the mailing list.
>
> **Anyone in the following list**. If you want to allow specific individuals or groups of individuals to be able to post messages to the mailing list, click the associated radio button. Then specify the following:
>
> > **Users and Groups.** This fields displays the list of individual users and groups from which messages will be accepted for posting to this mailing list. To Add a user or group to the list, click the corresponding Add button. If no user or group is specified, there is no sender-user restriction.
> >
> > **DNS Domains.** This fields displays the list of domains from which messages will be accepted for posting to this mailing list. To Add a domain name to the list, click the corresponding Add button. If no domain is specified, there is no sender-domain restriction.

When Message to this List is rejected:

Send message to Moderator(s). If you want to automatically forward rejected messages to the mailing-list moderator or moderators for further action, select this option. If you select this option, you must add at least one entry in the List moderators field. To add a user to the moderator list, click the corresponding Add button. Then use the Add Moderator window to locate and select a user.

5. Click OK.

To Edit a Mailing List

1. Click My Accounts in the upper banner of your administration page.
2. In the My Account window, click Manage Mail Lists.
3. In the Manage Mail Lists window, click Owned Mail Lists.
4. Use the Search feature to generate a list of your mail lists.
5. In the Search results, locate the mail list you want to edit, and click its name.
6. In the Edit Mail List window, make changes as necessary, and then click OK.

To Subscribe to a Mailing List

1. Click My Account in the upper banner of your administration page.
2. In the My Account window, click Manage Mail Lists.
3. Use the Search feature to generate a list of mail lists in the organization.
   a. Select Subscribe to generate a list of mail lists that you currently subscribe to.
   b. Select Unsubscribe to generate a list of available mail lists that you can subscribe to.
4. In the Search results, locate the mailing list you want to subscribe to, and then click Subscribe.
5. In the Subscribe Mail List window, click Subscribe.
6. In the Status window, click Continue.

To Unsubscribe from a Mailing List

1. Click My Account in the upper banner of your administration page.
2. In the My Account window, click Manage Mail Lists.
3. Use the Search feature to generate a list of mail lists in the organization.
    a. Select Subscribe to generate a list of mail lists that you currently subscribe to.

    b. Select Unsubscribe to generate a list of available mail lists that you can subscribe to.
4. In the Search results, locate the mailing list you want to unsubscribe from, and then click Unsubscribe.
5. In the Unsubscribe Mail List window, click Unsubscribe.
6. In the Status window, click Continue.

To Delete a Mailing List

1. In your administration page, use the Search feature to generate a list of Mail Lists.
2. In the Search results, in the right pane, locate the mailing list you want to delete. In the drop-down list, choose Delete.
3. When you see a confirmation message, click Continue.

My Account

When an end user logs in using their his ID and password, an administration page for the individual’s user account is usually displayed. When you log in, however, because you belong to an administrator group, an administration page is displayed. The My Account icon allows you play the role of an end user and modify your own user account information.

To Modify Information in Your Own User Account

1. Click My Account in the upper banner of any administration page.
2. In the My Account window, click Account Information, and make changes as necessary:

   Login ID. Displays your system user ID as assigned by a network administrator.

   First name. Enter your given name as it appears on official company records.

   Last name. Enter your surname as it appears on official company records.

   Email addresses:

   > **Alternate Email Addresses.** This field displays a list of your alternate email addresses, or aliases to the primary email address. Click Add to modify the information in this field. Then, in the Set Mail Address window, provide the following:

   - Enter an alternate address. This is essentially an alias for your primary address. For example, if a your primary address is `smythe@siore.com`, you can enter `smith@siroe.com` as an alternate address. This ensures that you will receive messages that are mistakenly addressed to "smith."
   - You can specify any number of alternate addresses, as long as each address is unique. Messages that arrive for any of these aliases are directed to the primary address.

   Access domains: Lists the access domains from which you can retrieve mail.

NOTE If no access domains are specified in the Access domain field, you can retrieve mail from any domain.

   To add an access domain:

   a. Click Add (next to the Access domains field) to open the Set Domain window, and then enter either a regular domain name or an IP address. You must enter only one access domain each time you open the Access Domain name window. If you specify a domain that does not exist, or enter none, you effectively block email access.

   b. Click OK.

Quota. Enter a number to limit your own disk quotas. Disk quotas allow administrators to limit the amount of disk space allotted to each user. For detailed information, see Chapter 5, “Managing Messaging Store” in *Netscape Messaging Server Administrator’s Guide*.

3. If Class of Service is used, click it to modify its settings.

4. To change your password, click Change Password, and then enter the following:

   Current Password. Enter the password you currently use to log into your network.

   New Password. Enter a password that is different from the current password.

   Retype New Password. Type the new password again to confirm it.

5. To modify telephone and mail information, click Personal Information and then modify the following as necessary:

   Telephone number. Enter your phone number as it appears in company records. Example: 454-555-4444.

   Fax number. Enter your fax number as it appears in company records. Example: 454-555-4444.

   Mobile number. Enter your mobile or cell phone number as it appears in company records. Example: 454-555-4444.

   Pager number. Enter your pager number as it appears in company records. Example: 454-555-4444.

   Mailing address. Enter a street address where you can receive print mail or packages. Example: 1234 Main Street, Anytown, AnyState.

   Web Page URL. Enter the URL for a web page that contains more information about you. Example: http://www.siroe.com/sales/reps

   Description. Enter a description for the web page that contains more information about you.

   Preferred Language. Use the drop-down list to indicate your preferred language. Delegated Administrator will display the user interface localized for the preferred language. For example, the Siroe company has employees in Japan, and they have indicated they prefer to conduct business in Japanese. When the Siroe administrator sets this preference to Japanese for a user, Delegated Administrator displays the Japanese version of the user interface.

6. If Mail Delivery Options is displayed, click it and then modify the following information as necessary:

   Deliver incoming messages to:

   POP3/IMAP4 mailbox. To enable mail delivery to regular POP3 or IMAP4 mailboxes, select this option.

   Unix mailbox. To allow messages to be delivered to a designated Unix mailbox, select this option. Unix delivery is available only to users whose Messaging Server runs on a Unix host machine.

   Process incoming messages through one or more programs:

   By default, incoming messages are put in the inbox of the mail account the message is addressed to. Accounts can be configured to perform various operations with the messages it receives. Examples include putting incoming messages in particular mail folders, forwarding them somewhere else, or generating an automatic response. For detailed information, see Chapter 12, “Program Delivery” in *Netscape Messaging Server Administrator’s Guide.*

   Enable the following programs: If you want to specify a mechanism for forwarding messages to an external application for processing before delivery to you, select this option. Then enter the external application command(s) to be used for processing this user’s mail

   Forward a copy of each message to: Enter another address instead of or in addition to your primary address. This enables mail to automatically be forwarded to the specified address.

7. If Vacation Auto-Responder Rule is displayed, enter the following:

   Auto-responder mode. Use the drop-down list to select one of the following:

   ❍ **Off.** Disables auto-reply.

   ❍ **Echo.** An automatic reply is sent for each received message and the received message appended as a MIME attachment to the reply. If you select this mode, you can enter a reply message in the Message field.

   ❍ **Vacation.** The first message received by you from a given sender generates an automatic response; subsequent messages from that sender do not generate a response. If you select this mode, use the Vacation start/ end date options and enter a reply message in the Reply text field.

   ❍ **Auto-reply.** Every incoming message received by you generates the specified automatic response. (The received message is not attached to the reply.) If you select this mode, you can enter a reply message in the Message field.

If you selected vacation mode, supply dates and times to determine when the auto-reply message should start and end:

- **Vacation Start Date**. If your vacation begins immediately, choose Now. If you want to specify a date, choose Date and then use the drop-down lists to indicate the date.
- **Vacation Start Time**. Enter the start time using the 24-hour format.
- **Vacation End Date**. If you don’t have a specific end date, choose Never. If you want to specify a date, choose Date and then use the drop-down lists to indicate the date.
- **Vacation End Time. Enter the end time using the 24-hour format.**

Message text. If you selected echo, vacation, or auto-reply mode, type a reply message to be returned to the sender. When the Vacation Auto-Responder is activated, Delegated Administrator will send the following default messages unless a specific text message is created:

Echo mode:

“This account has been configured to echo all mail, with no added text”

Vacation:

This person is currently on vacation.

Auto-Reply:

This account has been configured to reply to all mail, with no text.

8. Click OK.

Modifying Configuration Information

As a Top-level administrator, you have access permissions to modify the Delegated Administrator configuration in the directory. The configuration parameters effect the way the Delegated Administrator user interface is displayed, the information it captures, and the way processes the information. Changing the configuration changes the way Delegated Administrator works for you. You’ll find detailed information about modifying Delegated Administrator configuration in Chapter 11 of the *Installation and Customization Guide*.

Chapter 8

Top-level Help Desk Administrators

This document provides step-by-step instructions that a Top-level administrator will need on a day-to-day basis. The topics included in this document are:

- The Top-level Help Desk Administration Page
- Using the Search Feature
- Changing a User’s Password
- My Account
- Mail Lists

Logging In

The user ID and password you use to log in determines your administrator role and determines which branches of the directory you have access to. There are two ways you can log in to Delegated Administrator.

- If you are using the default Delegated Administrator tree, and you are using the sample data that shipped with the product, you can use the Start Page to help you get started. See "The Start Page" on page 43 for more information. Once you're familiar with the product and with your administrator role, you can bypass the Start Page you go directly to the Login window to log in.
- If you have modified the Delegated Administrator tree, or you are not using the sample data that shipped with the product, you will not see the Start Page. You must log in using the Login window. See "Using the Login Window" on page 172 for more information.

Using the Start Page

The Start Page was designed to provide all the information you need to quickly begin using Delegated Administrator with sample data and the default organization `Siroe.com`.

NOTE	If you installed Delegated Administrator against an existing directory, this sample data was not automatically installed. Skip to the next section, "Using the Login Window" on page 172.

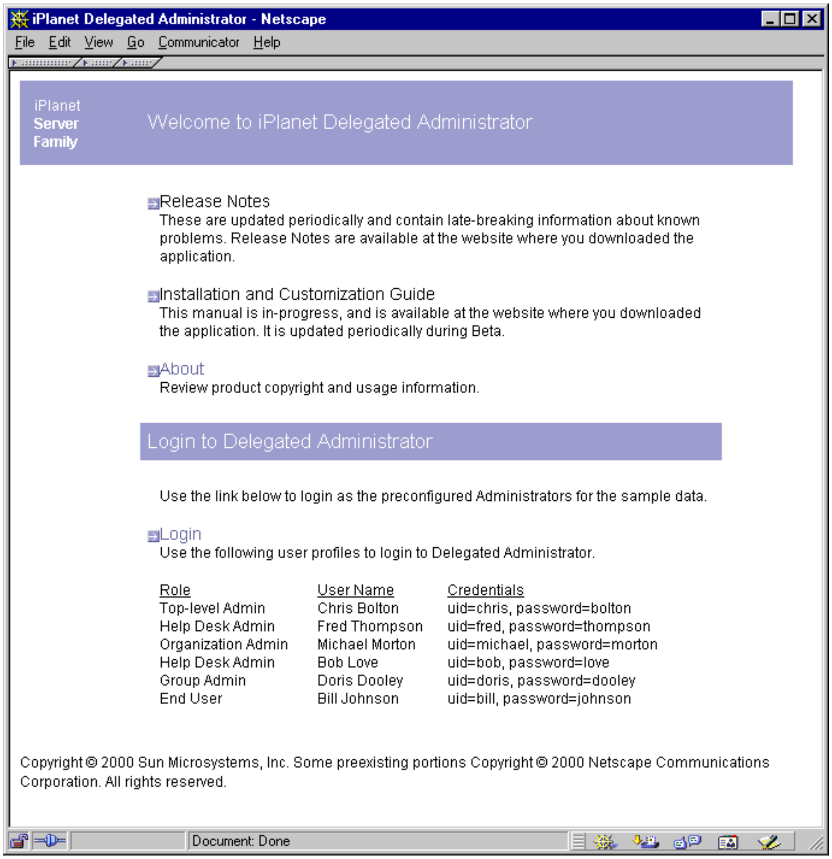
You can access the Start Page at any time by pointing a web browser to `http://<host_name>:<port>/nda/start.html`

You can use the Start Page to log in as any level of administrator named in the page. The user ID and password you use to log in determines your administrator role and determines which branches of the directory you have access to.

To start Delegated Administrator from the Start Page

1. Point a browser to the URL for the Delegated Administrator host using the form `http://<host:webserver_port>/nda/start.html`.

Figure 8-1 The Start Page



iPlanet Delegated Administrator - Netscape
File Edit View Go Communicator Help
iPlanet
Server
Family

Welcome to iPlanet Delegated Administrator

Release Notes
These are updated periodically and contain late-breaking information about known problems. Release Notes are available at the website where you downloaded the application.

Installation and Customization Guide
This manual is in-progress, and is available at the website where you downloaded the application. It is updated periodically during Beta.

About
Review product copyright and usage information.

Login to Delegated Administrator

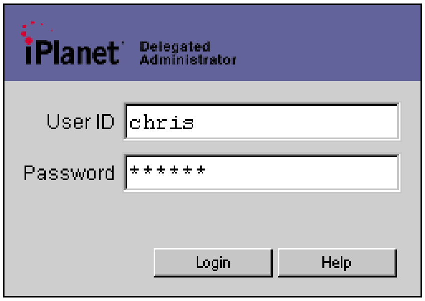
Use the link below to login as the preconfigured Administrators for the sample data.

Login
Use the following user profiles to login to Delegated Administrator.

Role	User Name	Credentials
Top-level Admin	Chris Bolton	uid=chris, password=bolton
Help Desk Admin	Fred Thompson	uid=fred, password=thompson
Organization Admin	Michael Morton	uid=michael, password=morton
Help Desk Admin	Bob Love	uid=bob, password=love
Group Admin	Doris Dooley	uid=doris, password=dooley
End User	Bill Johnson	uid=bill, password=johnson

Copyright © 2000 Sun Microsystems, Inc. Some preexisting portions Copyright © 2000 Netscape Communications Corporation. All rights reserved.

2. Click Login.



User ID chris

Password ******

In the Delegated Administrator Login window, using the information on the Start Page, enter an administrator's system user ID and password. For example, to log in as the Service Administrator, Chris Bolton, enter the following:

User ID. chris

Password. bolton

3. Click Login.

   Delegated Administrator displays the administration page that is appropriate for the User ID you entered. By default, your Delegated Administrator session will time out after thirty minutes of inactivity.

Using the Login Window

If you want to bypass the Start Page, or if the Start Page is not available to you, you can start Delegated Administrator and go directly to the Login window in one step.

To Start Delegated Administrator and Log In:

1. Point a browser to the URL for the Delegated Administrator host. Example:

   `http://<host_name>:<port>/nda/default/en/login.html`

2. In the Login window, enter your system user ID and password.

3. Click Login.

   Delegated Administrator displays the administration page that is appropriate for your administrator role. By default, your Delegated Administrator session will time out after thirty minutes of inactivity.

The Top-level Help Desk Administration Page

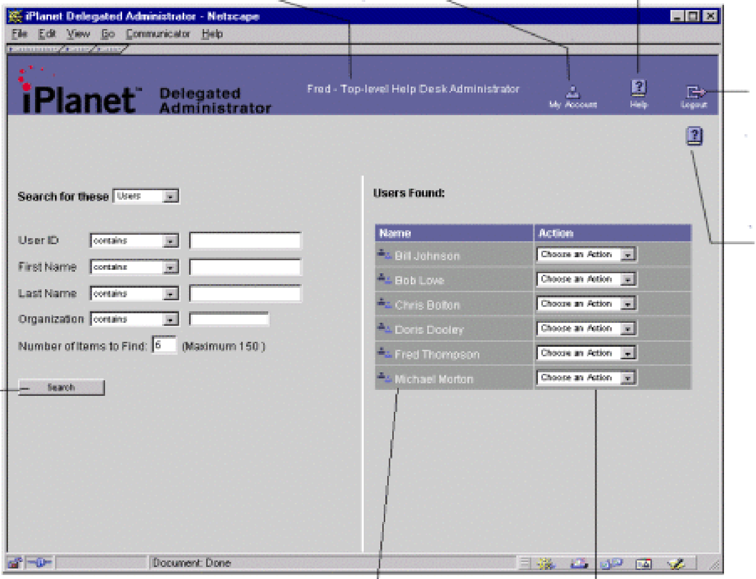
The Top-level administrator page provides access to all features and functions you're allowed to access. Figure 8-2 provides a quick tour of the page.

Figure 8-2 The Top-level Help Desk administration page.

Administrator Name. Displays the user ID and the administrator role of the person who logged in.

My Account. Click this icon when you want to modify your own user account information.

Help. Click this icon when you want information about all the tasks a Help Desk administrator can perform.



Fred - Top-level Help Desk Administrator

Search for these Users

User ID contains

First Name contains

Last Name contains

Organization contains

Number of Items to Find: 6 (Maximum 150)

Users Found:

Name	Action
Bill Johnson	Choose an Action
Bob Love	Choose an Action
Chris Bolton	Choose an Action
Doris Dooley	Choose an Action
Fred Thompson	Choose an Action
Michael Morton	Choose an Action

Logout. Click this icon when you want to end the current Delegated Administrator session.

Help. Click this icon when you want information about the data that's displayed, or the data to be entered in this window.

Search. Enter search criteria, and then click here to generate a list of users within the Top Level.

Search Results. Click a user's name to view his or her administration page.

Action. To edit a user's password, use the drop-down list to choose Edit.

Using the Search Feature

Use the Search feature to locate a user or mail list in the top level of the Delegated Administrator tree.

To Locate a User or Mail List

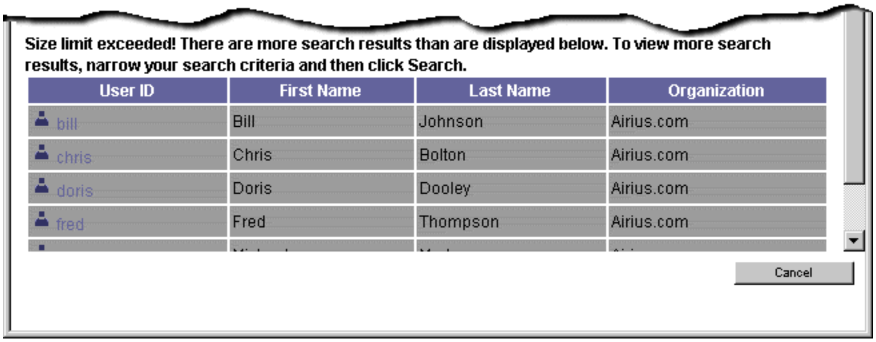
1. Use the Search for drop-down list to indicate whether you're searching for a user or mail list.
2. Use the remaining drop-down lists to indicate your search criteria.

   Number of Items to Find. Enter the number of search results you want to see displayed. The default is 5, but you can enter a number up to 150.
3. Click Search to generate a list of users or mail lists.
4. Once you locate a user or mail list:
   - Click the object's name to view and edit its settings or properties.
   - Choose an action from the corresponding Action drop-down list.

Exceeding the Search Results Size Limit

If you see the message regarding size limit (see Figure 8-3), the search operation found more results than the number you specified above, and cannot display all the results. When this happens, you can either enter a greater number in the **Display no more than....** field above, or you can enter more specific search criteria and begin the search again.

Figure 8-3 Size limit message.



Size limit exceeded! There are more search results than are displayed below. To view more search results, narrow your search criteria and then click Search.

User ID	First Name	Last Name	Organization
bill	Bill	Johnson	Airius.com
chris	Chris	Bolton	Airius.com
doris	Doris	Dooley	Airius.com
fred	Fred	Thompson	Airius.com

Changing a User's Password

You may need to change a user's password when the individual forgets it, or otherwise needs your help to reset it.

To Change a User's Password

1. Use the Search feature to generate a list of users within the Top-level.
2. In the Search results, locate the user, and then choose Edit from the drop-down list.
3. In the Basic Account Information window, click Change Password.
4. In the Change Password window, enter the following:

   Password. Enter the new password.

   Retype the password. Enter the password again to confirm it
5. Click OK.

In the Basic Account Information window, you can view, but you cannot edit, the following information:

Login ID. Displays the user's system user ID as assigned by a network administrator.

First name. Displays the user's given name as it appears on official company records.

Last name. Displays the user's surname as it appears in company records.

Organization. Displays the published name of the organization the user belongs to.

Title. Displays the user's job title as it appears on official company records.

Manager. Displays the distinguished name (DN) of the user's manager.

Email address. Displays the user's email address. .

Telephone number. Displays the user's phone number as it appears in company records.

Fax number. Displays the user's fax number as it appears in company records.

Mobile number. Displays the user's mobile or cell phone number as it appears in company records.

Pager number. Displays the user's pager number as it appears in company records.

Mailing address. Displays a street address where the user can receive print mail or packages.

Web Page URL. Displays the URL for a web page that contains more information about the user.

Description. Displays a word or phrase that describes the web page above.

Preferred Language. Displays the user's preferred language. Delegated Administrator will display the user interface localized for the preferred language. For example, the Siroe company has employees in Japan, and they have indicated they prefer to conduct business in Japanese. When the Siroe administrator sets this preference to Japanese for a user, Delegated Administrator displays the Japanese version of the user interface.

My Account

When an end user logs in using his or her ID and password, an administration page for the individual's user account is usually displayed. When you log in, however, because you belong to an administrator group, an administration page is displayed. The My Account icon allows you play the role of an end user and modify your own user account information.

To Modify Information in Your Own User Account

1. Click My Account in the upper banner of any administration page.
2. In the My Account window, click Account Information to view your account information:

   Login ID. Displays your system user ID as assigned by a network administrator.

   First name. Displays your given name as it appears on official company records.

   Last name. Displays your surname as it appears on official company records.

   Email addresses:

      Alternate Email Addresses. This field displays a list of your alternate email addresses, or aliases to the primary email address.

      Access domains: Lists the access domains from which you can retrieve mail.

NOTE If no access domains are specified in the Access domain field, you can retrieve mail from any domain.

   Quota. Displays your disk quota. Disk quotas allow administrators to limit the amount of disk space allotted to each user. If Class of Service is used, click it to modify its settings.

3. To change your password, click Change Password, and then enter the following:

   Current Password. Enter the password you currently use to log into your network.

New Password. Enter a password that is different from the current password.

Retype New Password. Type the new password again to confirm it.

4. To modify telephone and mail information, click Personal Information and then modify the following as necessary:

   Telephone number. Enter your phone number as it appears in company records. Example: 454-555-4444.

   Fax number. Enter your fax number as it appears in company records. Example: 454-555-4444.

   Mobile number. Enter your mobile or cell phone number as it appears in company records. Example: 454-555-4444.

   Pager number. Enter your pager number as it appears in company records. Example: 454-555-4444.

   Mailing address. Enter a street address where you can receive print mail or packages. Example: 1234 Main Street, Anytown, AnyState.

   Web Page URL. Enter the URL for a web page that contains more information about you. Example: http://www.siroe.com/sales/reps

   Description. Enter a description for the web page that contains more information about you.

   Preferred Language. Use the drop-down list to indicate your preferred language. Delegated Administrator will display the user interface localized for the preferred language. For example, the Siroe company has employees in Japan, and they have indicated they prefer to conduct business in Japanese. When the Siroe administrator sets this preference to Japanese for a user, Delegated Administrator displays the Japanese version of the user interface.

5. If Mail Delivery Options is displayed, click it and then modify the following information as necessary:

   Deliver incoming messages to:

   POP3/IMAP4 mailbox. To enable mail delivery to regular POP3 or IMAP4 mailboxes, select this option.

   Unix mailbox. To allow messages to be delivered to a designated Unix mailbox, select this option. Unix delivery is available only to users whose Messaging Server runs on a Unix host machine.

   Process incoming messages through one or more programs:

By default, incoming messages are put in the inbox of the mail account the message is addressed to. Accounts can be configured to perform various operations with the messages it receives. Examples include putting incoming messages in particular mail folders, forwarding them somewhere else, or generating an automatic response. For detailed information, contact your system administrator.

> **Enable the following programs:** If you want to specify a mechanism for forwarding messages to an external application for processing before delivery to you, select this option. Then enter the external application command(s) to be used for processing this user's mail.

Forward a copy of each message to: Enter another address instead of or in addition to your primary address. This enables mail to automatically be forwarded to the specified address.

6. If Vacation Auto-Responder Rule is displayed, enter the following:

   Auto-responder mode. Use the drop-down list to select one of the following:

   - **Off.** Disables auto-reply.
   - **Echo.** An automatic reply is sent for each received message and the received message appended as a MIME attachment to the reply. If you select this mode, you can enter a reply message in the Message field.
   - **Vacation.** The first message received by you from a given sender generates an automatic response; subsequent messages from that sender do not generate a response. If you select this mode, use the Vacation start/end date options and enter a reply message in the Reply text field.
   - **Auto-reply.** Every incoming message received by you generates the specified automatic response. (The received message is not attached to the reply.) If you select this mode, you can enter a reply message in the Message field.

   If you selected vacation mode, supply dates and times to determine when the auto-reply message should start and end:

   - **Vacation Start Date**. If your vacation begins immediately, choose Now. If you want to specify a date, choose Date and then use the drop-down lists to indicate the date.
   - **Vacation Start Time**. Enter the start time using the 24-hour format.
   - **Vacation End Date**. If you don't have a specific end date, choose Never. If you want to specify a date, choose Date and then use the drop-down lists to indicate the date.

- **Vacation End Time.** Enter the end time using the 24-hour format.

Message text. If you selected echo, vacation, or auto-reply mode, type a reply message to be returned to the sender. When the Vacation Auto-Responder is activated, Delegated Administrator will send the following default messages unless a specific text message is created:

Echo mode:

"This account has been configured to echo all mail, with no added text"

Vacation:

This person is currently on vacation.

Auto-Reply:

This account has been configured to reply to all mail, with no text.

7. If you want to create or manage mail lists, click Manage Mail Lists. Then skip to step 4 of To Create a New Mail List.
8. Click OK.

Mail Lists

Mail lists make it possible for a user to send the same message to a number of users at one time. A mail list specifies the email addresses (users) that receive all messages sent to a single email address. For example, in the Siroe company, if you send one email to the address `sales@Siroe.com`, each employee in the Sales Department will receive the email.

NOTE You cannot use Delegated Administrator to manage mail lists unless Netscape Messaging Server 4.x is installed and properly configured. The following mail list features and functionality will not be available to you until a higher-level administrator enables them for you.

As a Help Desk administrator, by default, you have access permissions to create and manage mail lists.

Mail List Owners

A mail list may have one or more owners assigned to it. The owner can edit the properties of the mail list that he or she owns. The owner can perform all operations on the mail list except for creating new mail lists and assigning owners. If the owner is a properly authorized administrator or user, he or she can create mail lists and assign owners to the lists.

Moderated Mail Lists

You can assign a moderator to filter messages sent to the mail list. This is useful in preventing unrelated messages from being distributed to members of the mail list. When you designate a moderator, the mail list is known as a *moderated lis*t. In a moderated mail list, all messages sent by members of the mail list are sent to the moderator. The moderator either approves or disapproves the messages, and then sends the only approved messages to all members of the mail list.

To Create a New Mail List

1. Click My Account in the upper banner of your administration page.
2. In the My Account window, click Manage Mail Lists.
3. In the My Account Mail window, click Create Mail List.
4. In the New Mail List window, provide the following mail list information:

   Mail List Name. Enter a name that describes the mail list. Example: Sales

   Description. Enter a description of the purpose or nature of the mail list. You can use this field to enter a URL to an HTML page providing additional information about the mail list. This is for informational purposes only; the URL is not used by Messaging Server or by Delegated Administrator.

   Primary Email Address. Enter the publicized address to which mail for the mail list can be sent. There can be only one primary address, which must be a valid, correctly formatted SMTP address conforming to RFC 821 specifications.

Alternate Email Addresses. This field displays a list of alternate email addresses or aliases to the primary email address. Click Add to modify the information in this field. Then, in the Set Mail Address window, provide the following information:

- Enter an alternate address. This is essentially an alias for the primary address. For example, if a user's primary address is `humanresources@siore.com`, you can enter `hr@siroe.com` as an alternate address. This ensures that recipients will receive messages that are mistakenly addressed to "hr."
- You can specify any number of alternate addresses as long as each address is unique. Messages that arrive for any of these aliases are directed to the primary address.

Owners. To add an existing user to the Owners list, click the corresponding Add button. Then use the Search for User window to locate and select the user.

Members. To add a user to the mail list, click the corresponding Add button. Then use the Add Member window to locate and select the user.

Person for Bounced Messages. Use the search feature to locate and select the person, possibly a list owner or system administrator, to whom error messages should be sent when mail sent to the list can not be delivered.

Allow users to join. If you want to allow users to add themselves to the mail list, choose Yes. If you want to restrict users from adding themselves to the mail list, choose No.

Show Members of List To. If you want the owners and members of this list to be able to view the members' names, choose All. If you want no owners or members to be able to view members' names, choose None.

Hide Mail List. If you want to make a mail list visible to all users for subscription purposes, choose No. To make the mail list visible to only Top-level and Organization Administrators, choose Yes.

Authorized Senders to List. Enter information regarding users, groups of users, or specific domains that are allowed to post messages to the mai list:

> **Anyone.** Any user may contribute to the mail list.
>
> **Anyone in the mail list.** Only users included in the mail list may contribute to the mail list.
>
> **Anyone in the following list**. If you want to allow specific individuals or groups of individuals to be able to post messages to the mail list, click the associated radio button. Then specify the following:

Users and Groups. This fields displays the list of individual users and groups from which messages will be accepted for posting to this mail list. To add a user or group to the list, click the corresponding Add button. If no user or group is specified, there is no sender-user restriction.

DNS Domains. This fields displays the list of domains from which messages will be accepted for posting to this mail list. To add a domain name to the list, click the corresponding Add button. If no domain is specified, there is no sender-domain restriction.

When Message to this List is rejected:

Send message to Moderator(s). If you want to automatically forward rejected messages to the mail-list moderator or moderators for further action, select this option. If you select this option, you must add at least one entry in the List moderators field. To add a user to the moderator list, click the corresponding Add button. Then use the Add Moderator window to locate and select a user.

5. Click OK.

To Edit a Mail List

1. Click My Accounts in the upper banner of your administration page.
2. In the My Account window, click Manage Mail Lists.
3. In the Manage Mail Lists window, click Owned Mail Lists.
4. Use the Search feature to generate a list of your mail lists.
5. In the Search results, locate the mail list you want to edit, and click its name.
6. In the Edit Mail List window, make changes as necessary, and then click OK.

To Subscribe to a Mail List

1. Click My Account in the upper banner of your administration page.
2. Use the Search feature to generate a list of mail lists in the organization.
   a. Select Subscribe to generate a list of mail lists that you currently subscribe to.
   b. Select Unsubscribe to generate a list of available mail lists that you can subscribe to.

3. In the Search results, locate the mail list you want to subscribe to, and then click Subscribe.
4. In the Subscribe Mail List window, click Subscribe.
5. In the Status window, click Continue.

To Unsubscribe from a Mail List

1. Click My Account in the upper banner of your administration page.
2. Use the Search feature to generate a list of mail lists in the organization.
    a. Select Subscribe to generate a list of mail lists that you currently subscribe to.
    b. Select Unsubscribe to generate a list of available mail lists that you can subscribe to.
3. In the Search results, locate the mail list you want to unsubscribe from, and then click Unsubscribe.
4. In the Unsubscribe Mail List window, click Unsubscribe.
5. In the Status window, click Continue.

To Delete a Mail List

1. In your administration page, use the Search feature to generate a list of Mail Lists.
2. In the Search results, in the right pane, locate the mail list you want to delete. In the drop-down list, choose Delete.
3. When you see a confirmation message, click Continue.

Chapter 9

Organization Administrators

This document provides step-by-step instructions that an Organization Administrator will need on a day-to-day basis. The topics included in this document are:

- Logging In
- The Organization Administration Page
- Managing Organizations
- Managing Groups
- Managing User Accounts
- My Account
- Modifying Configuration Information
- Mail Lists

Logging In

The user ID and password you use to log in determines your administrator role and determines which branches of the directory you have access to. There are two ways you can log in to Delegated Administrator.

- If you are using the default Delegated Administrator tree, and you are using the sample data that shipped with the product, you can use the Start Page to help you get started. See “The Start Page” on page 43 for more information. Once you’re familiar with the product and with your administrator role, you can bypass the Start Page you go directly to the Login window to log in.
- If you have modified the Delegated Administrator tree, or you are not using the sample data that shipped with the product, you will not see the Start Page. You must log in using the Login window. See “Using the Login Window” on page 188 for more information.

Using the Start Page

The Start Page was designed to provide all the information you need to quickly begin using Delegated Administrator with sample data and the default organization `Siroe.com`.

NOTE If you installed Delegated Administrator against an existing directory, this sample data was not automatically installed. Skip to the next section, “Using the Login Window” on page 188.

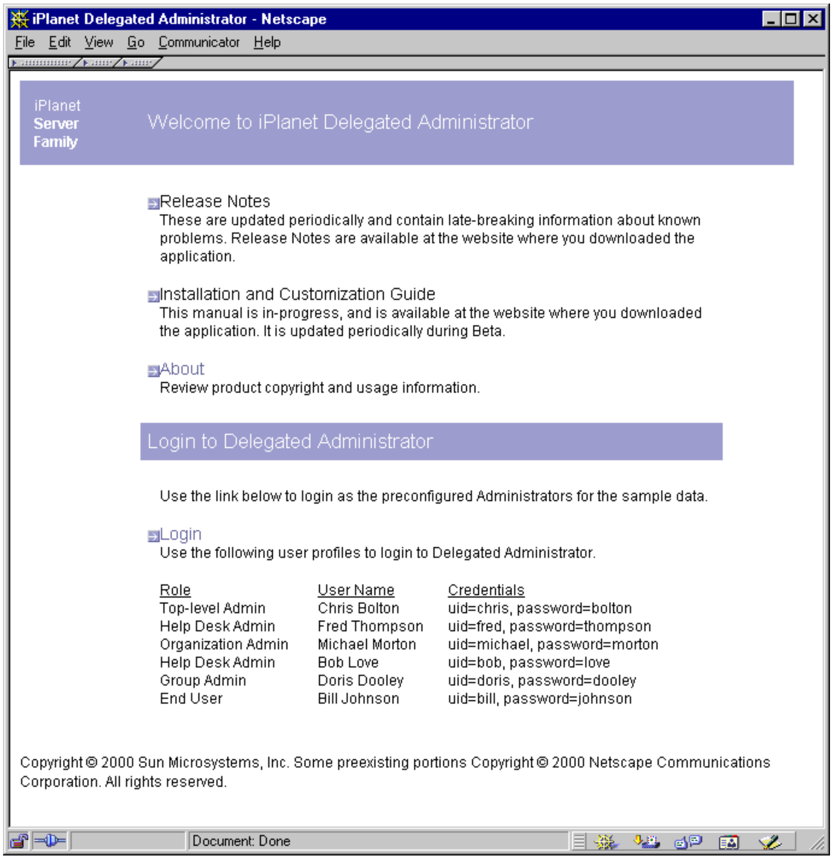
You can access the Start Page at any time by pointing a web browser to `http://<host_name>:<port>/nda/start.html`

You can use the Start Page to log in as any level of administrator named in the page. The user ID and password you use to log in determines your administrator role and determines which branches of the directory you have access to.

To start Delegated Administrator from the Start Page

1. Point a browser to the URL for the Delegated Administrator host using the form `http://<host:webserver_port>/nda/start.html`.

Figure 9-1 The Start Page


iPlanet Delegated Administrator - Netscape
File Edit View Go Communicator Help
iPlanet
Server
Family
Document: Done

Welcome to iPlanet Delegated Administrator

Release Notes
These are updated periodically and contain late-breaking information about known problems. Release Notes are available at the website where you downloaded the application.

Installation and Customization Guide
This manual is in-progress, and is available at the website where you downloaded the application. It is updated periodically during Beta.

About
Review product copyright and usage information.

Login to Delegated Administrator

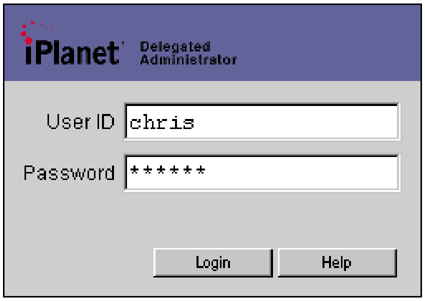
Use the link below to login as the preconfigured Administrators for the sample data.

Login
Use the following user profiles to login to Delegated Administrator.

Role	User Name	Credentials
Top-level Admin	Chris Bolton	uid=chris, password=bolton
Help Desk Admin	Fred Thompson	uid=fred, password=thompson
Organization Admin	Michael Morton	uid=michael, password=morton
Help Desk Admin	Bob Love	uid=bob, password=love
Group Admin	Doris Dooley	uid=doris, password=dooley
End User	Bill Johnson	uid=bill, password=johnson

Copyright © 2000 Sun Microsystems, Inc. Some preexisting portions Copyright © 2000 Netscape Communications Corporation. All rights reserved.

2. Click Login.



User ID chris

Password ******

In the Delegated Administrator Login window, using the information on the Start Page, enter an administrator's system user ID and password. For example, to log in as the Service Administrator, Chris Bolton, enter the following:

User ID. chris

Password. bolton

3. Click Login.

   Delegated Administrator displays the administration page that is appropriate for the User ID you entered. By default, your Delegated Administrator session will time out after thirty minutes of inactivity.

Using the Login Window

If you want to bypass the Start Page, or if the Start Page is not available to you, you can start Delegated Administrator and go directly to the Login window in one step.

To Start Delegated Administrator and Log In:

1. Point a browser to the URL for the Delegated Administrator host. Example:

   ```
   http://<host_name>:<port>/nda/default/en/login.html
   ```

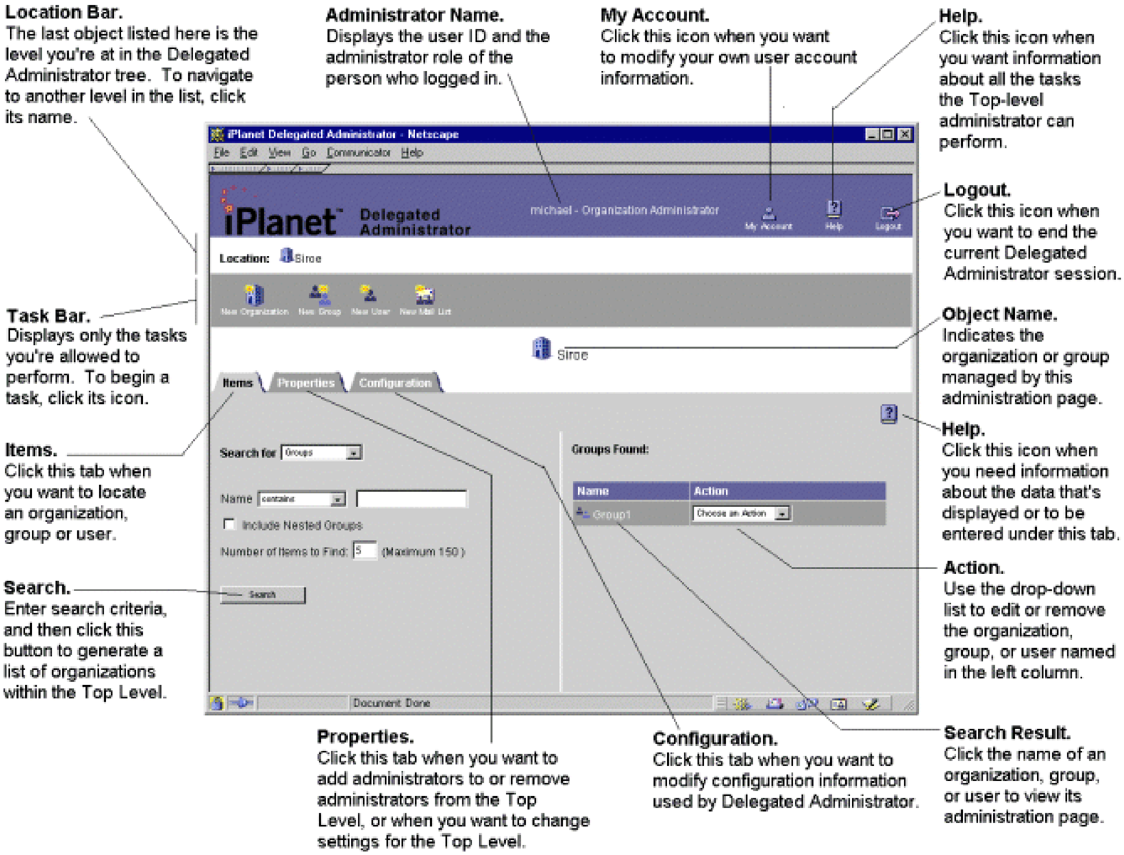
2. In the Login window, enter your system user ID and password.
3. Click Login.

   Delegated Administrator displays the administration page that is appropriate for your administrator role. By default, your Delegated Administrator session will time out after thirty minutes of inactivity.

The Organization Administration Page

The Organization administrator page provides access to all features and functions you're allowed to access. Figure 9-2 Figure 9-2 provides a quick tour of the page.

Figure 9-2 The Organization administration page.



Location Bar. The last object listed here is the level you're at in the Delegated Administrator tree. To navigate to another level in the list, click its name.

Administrator Name. Displays the user ID and the administrator role of the person who logged in.

My Account. Click this icon when you want to modify your own user account information.

Help. Click this icon when you want information about all the tasks the Top-level administrator can perform.

Logout. Click this icon when you want to end the current Delegated Administrator session.

Task Bar. Displays only the tasks you're allowed to perform. To begin a task, click its icon.

Object Name. Indicates the organization or group managed by this administration page.

Items. Click this tab when you want to locate an organization, group or user.

Help. Click this icon when you need information about the data that's displayed or to be entered under this tab.

Action. Use the drop-down list to edit or remove the organization, group, or user named in the left column.

Search. Enter search criteria, and then click this button to generate a list of organizations within the Top Level.

Properties. Click this tab when you want to add administrators to or remove administrators from the Top Level, or when you want to change settings for the Top Level.

Configuration. Click this tab when you want to modify configuration information used by Delegated Administrator.

Search Result. Click the name of an organization, group, or user to view its administration page.

Using the Location Bar

The Location Bar indicates you where you are in the directory tree. The last object listed indicates the object that is managed by the administration page. Objects are also represented by the following icons:

Base suffix. There is only one base suffix. This icon represents the top level of the Delegated Administrator tree.

Organization. This icon represents an organization or suborganization.

Group. This icon represents a group or subgroup.

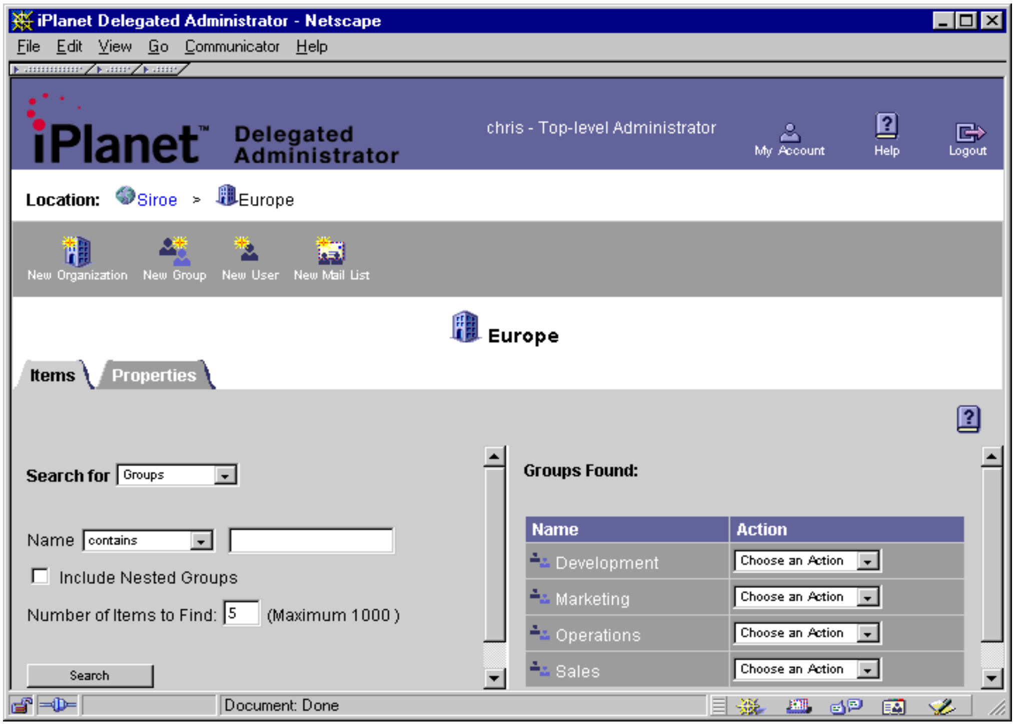
To navigate to the administration page for a different organization or group, click its name or icon in the Location Bar.

NOTE	Do not use the Back and Forward buttons in your browser to navigate to administration pages in Delegated Administrator. If you use the Back and Forward buttons in your browser, the Location Bar will not properly display your location in the Delegated Administrator tree.

Using the Search Feature

You'll see two forms of the Search feature, but they work similarly. Figure 9-3 illustrates the Search feature embedded in the Items tab. Use the Search feature in the Items tab when you want to navigate further down in the tree, or when you want to edit or delete a user, group, or organization. Figure 9-4 shows a discrete Search window invoked when performing a task such as adding a new administrator from within the Properties Tab.

Figure 9-3 The Search feature embedded in the Items tab.


iPlanet Delegated Administrator - Netscape
File Edit View Go Communicator Help
iPlanet™ Delegated Administrator
chris - Top-level Administrator
My Account
Help
Logout
New Organization
New Group
New User
New Mail List
Europe
Items
Properties
Search
Document: Done

Location: Siroe > Europe

Search for: Groups

Name: contains

☐ Include Nested Groups

Number of Items to Find: 5 (Maximum 1000)

Groups Found:

Name	Action
Development	Choose an Action
Marketing	Choose an Action
Operations	Choose an Action
Sales	Choose an Action

To Locate a Directory Object From the Items Tab

1. Enter the following search criteria:

   Search for. Use the drop-down list to indicate whether you’re searching for an organization, group, user, or mail list.

   Name. Enter the name of the directory object. Use the drop-down list to narrow your search criteria.

   Include Nested Organizations. If you want to search recursively through all suborganizations under the selected organization, select this option.

Number of Items to Find. Enter the number of search results you want to see displayed. The default is 5, but you can enter a number up to 150.

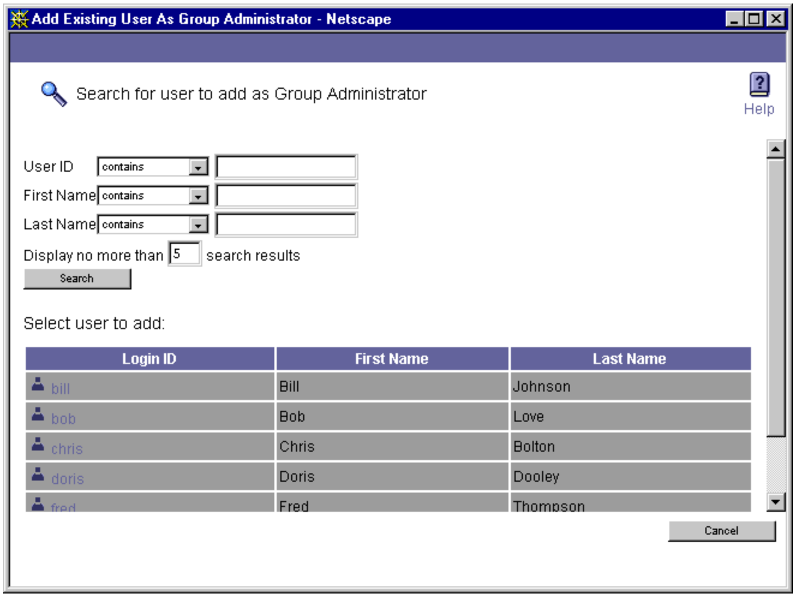
2. Once you locate a user, group, or organization in the results list, do one of the following:

   - Click the object's name to view and edit its settings or properties.
   - Choose an action from the corresponding Action drop-down list.

To Locate a User Using a Search Window

A Search window is automatically displayed when you want to add an existing user to a group.

Figure 9-4 A Search window is invoked when adding an administrator to a group.



Add Existing User As Group Administrator - Netscape

Search for user to add as Group Administrator

User ID: contains

First Name: contains

Last Name: contains

Display no more than 5 search results

Select user to add:

Login ID	First Name	Last Name
bill	Bill	Johnson
bob	Bob	Love
chris	Chris	Bolton
doris	Doris	Dooley
fred	Fred	Thompson

1. Enter one or more of the following, using the drop-down lists to narrow your search criteria.

   User ID. Enter the user's system user ID as assigned by a network administrator.

   First Name. Enter the user's given name as it appears in official records.

Last name. Enter the user's surname as it appears in official records.

NOTE	If you do not enter information in any of these fields, Delegated Administrator will generate a list of all user entries within the level, organization, or group you've selected. If there are more than 5000 users within this scope, the search could take a long time.

Display no more than. Enter the number of search results you want to see displayed. The default is 5, but you can enter a number up to 150.

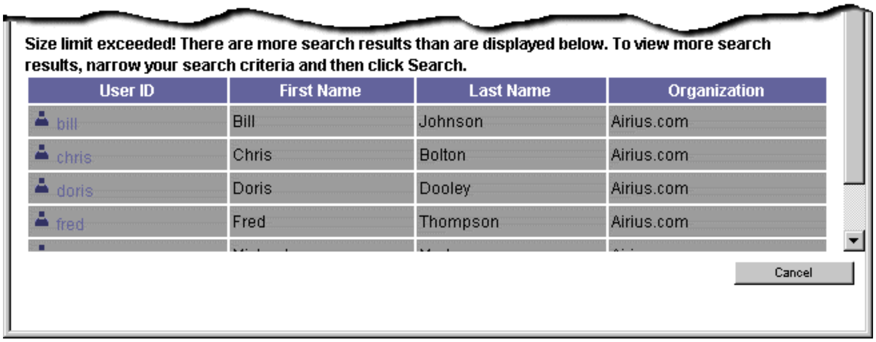
2. Click Search.

   Delegated Administrator generates a list of users within your scope of responsibility that match the criteria you've specified.

Exceeding the Search Results Size Limit

If you see the message regarding size limit (see Figure 9-5), the search operation found more results than the number you specified above, and cannot display all the results. When this happens, you can either enter a greater number in the **Display no more than....** field above, or you can enter more specific search criteria and begin the search again.

Figure 9-5 Size limit message.



Size limit exceeded! There are more search results than are displayed below. To view more search results, narrow your search criteria and then click Search.

User ID	First Name	Last Name	Organization
bill	Bill	Johnson	Airius.com
chris	Chris	Bolton	Airius.com
doris	Doris	Dooley	Airius.com
fred	Fred	Thompson	Airius.com

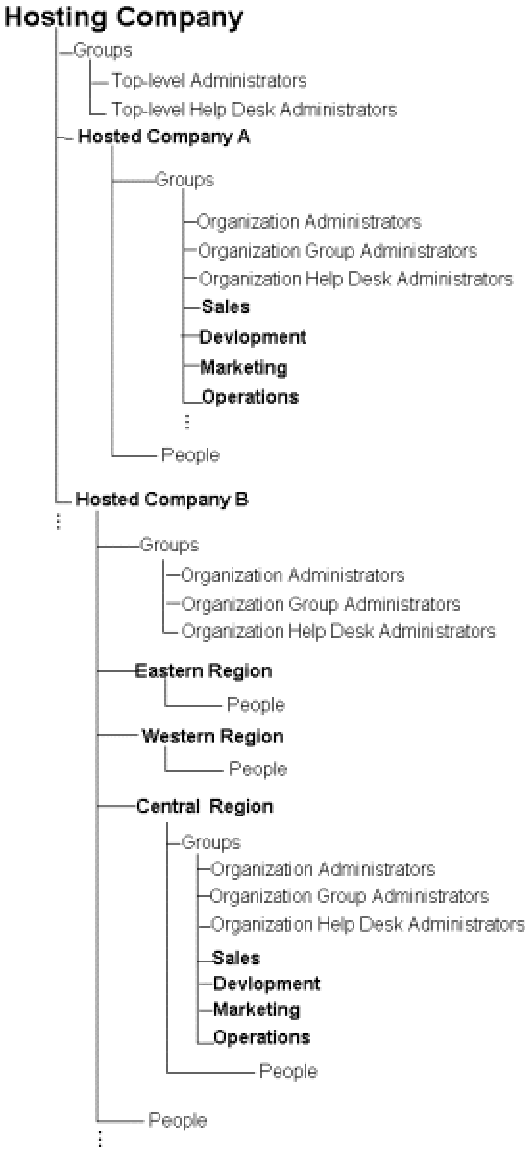
Managing Organizations

As an Organization Administrator, you can create and manage organizations, groups, user accounts, and mail lists. Use the Search feature to locate the organization you want to manage, and then navigate to its administration page.

Creating a New Organization

Create a new organization when you want to manage a large number of user accounts in one container in the directory. You can create an organization at the top level of the Delegated Administrator tree; you can create an organization within another organization. You cannot create an organization within a group. When you create a new organization, the new organization is located one level down in the directory. For example, see Figure 9-6 on page 195. A company creates two levels of organizations. At the top level, a Top-level administrator creates two organizations, Hosted Company A and Hosted Company B. These are *peer* organizations because they are created at the same level in the directory tree. Under Hosted Company B, an Organization Administrator creates three new organizations, one level down in the directory: Eastern Region, Western Region, and Central Region. Each contains a separate People container.

Figure 9-6 Peer organizations.


Hosting Company
Groups
Top-level Administrators
Top-level Help Desk Administrators
Hosted Company A
Groups
Organization Administrators
Organization Group Administrators
Organization Help Desk Administrators
Sales
Devlopment
Marketing
Operations
People
Hosted Company B
Groups
Organization Administrators
Organization Group Administrators
Organization Help Desk Administrators
Eastern Region
People
Western Region
People
Central Region
Groups
Organization Administrators
Organization Group Administrators
Organization Help Desk Administrators
Sales
Devlopment
Marketing
Operations
People
People

Limiting the Number of Objects in an Organization

You can limit the number of suborganizations, groups, or user accounts that may be included in the new organization. Limits are useful for two reasons. First, they optimize Delegated Administrator performance. Searches performed on organizations with fewer than 5000 users, or fewer than 50 suborganizations, take less time to process.

Secondly, limits can help you comply with parameters set by your company. For example, the Siroe company's fee structure is based on the number of users in an organization; organizations with more than 5000 users are charged more for service than organizations with fewer than 5000 users. When creating new organizations, the Siroe administrator limits the number of organizations to 5000.

To Create a New Organization

1. In the Organization administration page, in the task bar, click the New Organization icon.

2. In the Create Organization window, enter the following:

   Organization name. Enter a name as you want it to appear in your company's official records. The name can include spaces and numbers.

   Suborganization limit. Enter the maximum number of suborganizations allowed in the organization.

   Group limit. Enter the maximum number of groups allowed in the organization.

   Mail list. Enter the maximum number of mail lists allowed in the organization.

   User account limit. Enter the maximum number of user accounts allowed in the organization.

3. Click OK.

4. In the Status window, click Continue.

   The new organization is created one level down in the directory tree.

To Edit Organization Limits

1. Navigate to the top-level or organization administration page under which the organization was created.

2. Use the Search feature to generate a list of organizations.

3. In the Search results, in the right pane, click the name of the organization you want to edit.

4. In the Organization administration page, click Properties.

5. In the Properties tab, modify the following as necessary:

   Suborganizations. Indicates the number of suborganizations that currently exist under the organization.

   Suborganization limit. Enter the maximum number of suborganizations allowed in the organization.

   Groups. Indicates the number of groups that currently exist under the organization.

   Group limit. Enter the maximum number of groups allowed in the organization.

   User accounts. Indicates the number of user accounts that currently exist under the organization.

   User account limit. Enter the maximum number of user accounts allowed in the organization.

   Mail lists. Indicates the number of mail lists that currently exist under the organization.

   Mail list limit. Enter the maximum number of mail lists allowed in the organization.

6. Click Save.

Creating a Suborganization

When you create an organization within another organization, the new object is called a *suborganization*.

To Create a Suborganization

1. Navigate to the administration page of the organization under which the suborganization will be created.
2. In the organization administration page, in the task bar, click the New Organization icon.
3. In the Create Organization window, enter the following:

   Organization name. Enter a name as you want it to appear in your company's official records. The name can include spaces and numbers.

   Suborganization limit. Enter the maximum number of suborganizations allowed in the organization.

   Group limit. Enter the maximum number of groups allowed in the organization.

   User account limit. Enter the maximum number of user accounts allowed in the organization.
4. Click OK.
5. In the Status window, click Continue.

Adding Organization Administrators

Add an existing user to the Organization Administrators group if you want the user to share the administration duties at the organization level. When you add a user to the Organization Administrators group, you extend to that user all the access privileges accorded the group.

To Add an Organization Administrator

1. Navigate to the organization under which the Organization Administrators group is located.
2. In the Organization administration page, click the Properties tab.
3. In the Properties tab, click the Add button beside the list of Organization Administrators.
4. In the Add Existing User window, use the Search feature to locate and select the user you want to add to the Organization Administrator's group.
5. In the UserID column, click the user you want to add to the Organization Administrators group.
6. In the Status window, click Continue.

The user is added to the Organization Administrators group, and now has all access privileges accorded this group. The administrator's user ID is displayed in the Organization Administrators list.

Removing Organization Administrators

When you remove a member of the Organization Administrators group, that user no longer has access privileges accorded to the group. The user's account is not deleted from the user directory.

To Remove a Organization Administrator

1. Navigate to the organization under which the Organization Administrators group is located.

1. In the organization administrator page, click the Properties tab.
2. In the Properties tab, in the Organization Administrators list, click the user ID of the administrator you want to remove.
3. Click the Remove button beside the Organization Administrators list.
4. In the Status window, click Continue.

The user is removed from the Organization Administrators list, and no longer has the access privileges accorded this group.

Adding Organization Help Desk Administrators

Add an existing user to the Organization Help Desk Administrators group if you want the user to be able to modify the passwords of other users in the organization. When you add a user to the Organization Help Desk Administrators group, you extend to that user all the access privileges accorded the group. Help Desk Administrators, by default, can modify only user passwords within their scope of access.

To Add a Organization Help Desk Administrator

1. In the Organization administration page, click the Properties tab.
2. In the Properties tab, click the Add button beside the list of Organization Help Desk Administrators.
3. In the Add Existing User window, use the Search feature to locate and select the user you want to add to the Organization Help Desk Administrator's group.
4. In the UserID column, click the user you want to add to the Organization Help Desk Administrators group.
5. In the Status window, click Continue.

The user is added to the Organization Help Desk Administrators group, and now has all access privileges accorded this group. The administrator's user ID is displayed in the Organization Help Desk Administrators list.

Removing Organization Help Desk Administrators

When you remove a member of the Organization Help Desk Administrators group, that user no longer has access privileges accorded to the group. The user's account is not deleted from the user directory.

To Remove a Organization Help Desk Administrator

1. Navigate to the organization under which the user is located.
2. In the organization administration page, click the Properties tab.
3. In the Properties tab, in the Organization Help Desk Administrators list, click the user ID of the administrator you want to remove.

4. Click the Remove button beside the Organization Help Desk Administrators list.

5. In the Status window, click Continue.

The user is removed from the Organization Help Desk Administrators list, and no longer has the access privileges accorded this group.

Deleting an Organization

When you delete an organization, its entry is deleted from the directory.

To Delete an Organization

1. Navigate to the organization administration page that manages the organization you want to delete.

2. Use the Search feature to locate the organization you want to delete.

3. In the Search results list, in the right pane, find the organization you want to edit, and then from its drop-down list, choose Delete.

4. When you see the confirmation message, click OK.

Managing Groups

As a Organization administrator, you can also perform any task that a Group administrator can perform.

Creating a New Group

Create a new group when you want to associate a number of users under one name. For example, in the Siroe company, all Sales employees are considered members of the Sales Department even though their user accounts might be stored in other parts of the organization. You can create a group within an organization; you can create a group within another group. You cannot create a new group at the top level of the Delegated Administrator tree.

Limiting the Number of Objects in an Group

You can limit the number of groups, or user accounts that may be included in the new groups. Limits are useful for two reasons. First, they optimize Delegated Administrator performance. Searches performed on groups with fewer users take less time to process.

Secondly, limits can help you comply with parameters set by your company. For example, the Siroe company's fee structure is based on the number of users in an group; groups with more than 5000 users are charged more for service than groups with fewer than 5000 users. When creating new groups, the Siroe administrator limits the number of users to 5000.

To Create a New Group

1. Navigate to the administration page for the organization in which the group will be created.
2. In the organization administration page, in the task bar, click New Group.
3. In the Create Group window, enter the following:

   Group name. Enter a name as you want it to appear in your company's official records. The name can include spaces and numbers.

   Nested group limit. Enter the maximum number of subgroups allowed in the group.

   User account limit. Enter the maximum number of user accounts allowed in the group.

4. Click OK.
5. In the Status window, click Continue.

To Edit Group Limits

1. Navigate to the organization administration page that manages the group you want to edit.
2. In the organization administration page, use the Search feature to generate a list of groups within the organization.
3. In the Search results, in the right pane, locate the group you want to edit, and then use its drop-down list to choose Edit.
4. Modify the following as necessary:

   Nested groups. Indicates the number of subgroups that currently exist under the group.

   Nested group limit. Enter the maximum number of subgroups allowed in the group.

   User accounts. Indicates the number of user accounts that currently exist under the group.

   User account limit. Enter the maximum number of user accounts allowed in the group.
5. Click Save.

Creating a Subgroup

When you create a group within another group, the new object is called a *subgroup*. Create a subgroup when you want to associate a number of users under one name.

1. Navigate to the administration page for the group in which the subgroup will be created.
2. In the group administration page, in the task bar, click New Group.
3. In the Create Group window, enter the following:

   Group name. Enter a name as you want it to appear in your company’s official records. The name can include spaces and numbers.

   Nested group limit. Enter the maximum number of subgroups allowed within the subgroup.

   User account limit. Enter the maximum number of user accounts allowed in the subgroup.
4. Click OK.

5. In the Status window, click Continue.

Adding a User to a Group

Group administrators add users to groups in one of two ways: by adding a new user to the group, or by adding an existing user to a group.

To Add an Existing User to a Group

1. Navigate to the administration page for the organization under which the group was created.
2. Use the Search feature to locate and select the group to which the user will belong.
3. In the group administration page, in the task bar, click Add Existing User.
4. In the "Search for user to add as Group Member" window, locate and click the User ID of the user you want to add to the group.
5. Click OK.

To add a New User to a Group

1. Navigate to the administration page for the organization under which the group was created.
2. Use the Search feature to locate and select the group to which the new user will belong.
3. In the group administration page, in the task bar, click New User.
4. In the New User window, click Basic Account Information. Skip to step 3 of To Create a New User Account in the section "Managing User Accounts."

Adding Group Administrators

Add an existing user to the Group Administrators list if you want the user to be able to create new groups or modify the user accounts within a group. When you add a user to the Group Administrators list, you extend to that user all the access privileges accorded the group. Group Administrators, by default, can modify most information in the User Account Information window.

To Add a Group Administrator

1. In the organization administration page, under the Items tab, search for the group to which the new Group Administrator will belong.
2. In the Properties tab, click the Add button beside the list of Group Administrators.
3. In the Add Existing User window, use the Search feature to locate and select the user you want to add to the Group Administrators list.
4. In the UserID column, click the user you want to add to the Group Administrators list.
5. In the Status window, click Continue.

The user is added to the Group Administrators list, and now has all access privileges accorded this group. The administrator’s User ID is displayed in the Organization Administrators list.

Removing Group Administrators

When you remove a member of the Group Administrators group, that user no longer has access privileges accorded to the group. The user’s account is not deleted from the user directory.

To Remove a Group Administrator

1. In the Organization administration page, under the Items tab, search for the group to which the Group Administrator belongs.
2. In the Properties tab, in the Group Administrators list, click the UserID of the administrator you want to remove.
3. Click the Remove button beside the Group Administrators list.
4. In the Status window, click Continue.

The user is removed from the Group Administrators list, and no longer has the access privileges accorded this group.

Removing a User from a Group

When you remove a user from a group, the individual's user ID is no longer associated with the group; the user entry remains in the directory. This is not the same as *deleting* a user account. When you delete a user account, the individual's entry is deleted from the user directory. (See Deleting a User Account.)

To Remove a User from a Group

1. Navigate to the administration page for the organization under which the group was created.
2. Use the Search feature to generate a list of groups within the organization.
3. In the Search results, in the right pane, locate the name of the user you want to remove, and then use its drop-down list to choose Remove.
4. When you see the confirmation message, click OK.

Deleting a Group

When you delete a group, its entry is deleted from the user directory.

To Delete a Group

1. Navigate to the organization or group administration page that manages the group.
2. Use the Search feature to generate a list of groups within the organization or group.
3. In the Search results, in the left pane, locate the group you want to delete, and then use its drop-down list to choose Delete.

Managing User Accounts

As an Organization administrator, you can create user accounts at the organization or the group level.

Creating a New User Account

Create a new account when you want to add a user to the directory.

To Create a New User Account

1. Navigate to administration page for the organization or group to which the user will belong.
2. In organization or group administration page task bar, click New User.
3. In the New User window, in the Basic Account Information pane, enter the following required information:

   Login ID. Enter the user's system user ID as assigned by a network administrator.

   First name. Enter the user's given name as it appears on official company records.

   Last name. Enter the user's surname as it appears in company records.

   Password. Enter the user's password.

   Confirm password. Enter the user's password again to confirm it.

   Organization. Enter the published name of the organization the user belongs to. Example: Sales Department.

   Title. Enter the user's job title as it appears on official company records. Example: Sales Associate.

   Manager. Enter the distinguished name (DN) of the user's manager. Example: `uid=doris, ou=People, o=Siroe, o=ISP`.

   Email address. Enter the user's email address. Example: ginac@siroe.com.

   Telephone number. Enter the user's phone number as it appears in company records. Example: 454-555-4444.

   Fax number. Enter the user's fax number as it appears in company records. Example: 454-555-4444.

Mobile number. Enter the user’s mobile or cell phone number as it appears in company records. Example: 454-555-4444.

Pager number. Enter the user’s pager number as it appears in company records. Example: 454-555-4444.

Mailing address. Enter a street address where the user can receive print mail or packages. Example: 1234 Main Street, Anytown, AnyState.

Web Page URL. Enter the URL for a web page that contains more information about the user. Example: http://www.siroe.com/sales/reps

Description. Enter a word or phrase that describes the web page above. Example: Sales Reps.

Preferred Language. Use the drop-down list to indicate the user’s preferred language. Delegated Administrator will display the user interface localized for the preferred language. For example, the Siroe company has employees in Japan, and they have indicated they prefer to conduct business in Japanese. When the Siroe administrator sets this preference to Japanese for a user, Delegated Administrator displays the Japanese version of the user interface.

4. If Class of Service is used, click it and enter the appropriate information.

5. If Basic Mail Information is displayed, click it and then enter the following information:

   Mail host: Enter the Messaging Server host name. This is the machine hosting the Messaging Server that will process this user's mail. This must be the fully-qualified domain name (FQDN) known to the Messaging Server on that machine.

Alternative email addresses: An alternate address is essentially an alias for the user's primary address. You can use this feature to:

- Ensure proper delivery of frequently misspelled addresses (such as "Smith" as an alias for "Smithy").
- Enable host name hiding in outgoing mail headers. To do so, supply an alternate address that includes the host name and do not include the host name in the primary email address (see step 3).
- You can specify any number of alternate addresses for a particular user, as long as each address is unique. Messages that arrive for any of these aliases are directed to the primary address.

Access domains: Lists the access domains from which the user can retrieve mail.

NOTE If no access domains are specified in the Access domain field, the user can retrieve mail from any domain.

To add an access domain:

a. Click Add (next to the Access domains field) to open the Set Domain window, and then enter either a regular domain name or an IP address. You must enter only one access domain each time you open the Access Domain name window. If you specify a domain that does not exist, or enter none, you effectively block access for the user.

b. Click OK.

Allow following service(s): To enable mail services for a specific type of server, select one or more of the available options: IMAP, POP, and HTTP. Netscape Messaging Server supports the Post Office Protocol 3 (POP3), the Internet Mail Access Protocol 4 (IMAP4), and the HyperText Transfer Protocol (HTTP) for client access to mailboxes. IMAP and POP are both Internet-standard mailbox protocols. Messenger Express, a web-enabled electronic mail program, lets end users access their mailboxes using a browser running on an Internet-connected computer system using HTTP.

Can Create E-mail Lists? This option applies only to Group administrators and individual users. All higher-level administrators, by default, have full mail list privileges regardless of whether this option is selected for them. When you select this option for a Group administrator or individual user, the Manage Mail Lists option is displayed when the individual edits his own account information.

6. If Mail Delivery Options is displayed, click it and then enter the following information:

Deliver incoming messages to:

POP3/IMAP4 mailbox. Select this option if you want to configure delivery and access to an individual user's POP or IMAP mailboxes.

Message store name. Enter the name (nickname, not pathname) of the message store partition to which the user's incoming mail should be delivered, if other than the current default primary partition. The name must represent an existing partition. For information on the message store and instructions for creating partition nicknames, see the *Messaging Server Administrator's Guide.*

Mailbox disk quota. Specify an allocated storage limit for this user. Enter a number in the field and select the appropriate unit (KB or MB). The disk quota or allocated storage limit you specify applies to this user alone.

Unix mailbox. Select this option if you want messages to be delivered to the user's designated Unix mailbox. Unix delivery is available only to users whose Messaging Server runs on a Unix host machine.

Process incoming messages through one or more programs:

By default, incoming messages are put in the inbox of the mail account the message is addressed to. Accounts can be configured to perform various operations with the messages it receives. Examples include putting incoming messages in particular mail folders, forwarding them somewhere else, or generating an automatic response. For detailed information, see Chapter 12, "Program Delivery" in *Netscape Messaging Server Administrator's Guide.*

Enable the following programs: If you want to specify a mechanism for forwarding messages to an external application for processing before delivery to the user, select this option. Then enter the external application command(s) to be used for processing this user's mail.

Forward a copy of each message to: Enter another address instead of or in addition to the primary address for the user. This enables mail to automatically be forwarded to the specified address.

7. Click OK.

To Edit a User Account

1. Navigate to the administration page of the organization or group under which the user account was created.
2. Use the Search feature to generate a list of user accounts within the organization or group.
3. In the Search results, in the right pane, locate the user ID of the account you want to modify, and then use the drop-down list to choose Edit.
4. Modify the user account information as necessary. See Creating a New User Account for detailed information about each of the fields in this window.
5. Click OK.

Deleting a User Account

Before you can delete a user account, you must navigate to the administration page for the organization or group under which the user account was created. When you delete a user account, the individual's entry is deleted from the user directory.

To Delete a User Account

1. Navigate to the administration page for the organization or group under which the user account was created.
2. Use the Search feature to generate a list of users within the organization or group.
3. In the Search results, in the right pane, locate the name of the user name for the account you want to delete, and then use its drop-down list to choose Delete.
4. When you see the confirmation message, click OK.

My Account

When an end user logs in using their his ID and password, an administration page for the individual's user account is usually displayed. When you log in, however, because you belong to an administrator group, an administration page is displayed. The My Account icon allows you play the role of an end user and modify your own user account information.

To Modify Information in Your Own User Account

1. Click My Account in the upper banner of any administration page.
2. In the My Account window, click Account Information, and make changes as necessary:

   Login ID. Displays your system user ID as assigned by a network administrator.

   First name. Enter your given name as it appears on official company records.

   Last name. Enter your surname as it appears on official company records.

   Email addresses:

   Alternate Email Addresses. This field displays a list of your alternate email addresses, or aliases to the primary email address. Click Add to modify the information in this field. Then, in the Set Mail Address window, provide the following:

   - Enter an alternate address. This is essentially an alias for your primary address. For example, if a user's primary address is `smythe@siore.com`, he enters `smith@siroe.com` as an alternate address. This ensures that he will receive messages that are mistakenly addressed to "smith."
   - You can specify any number of alternate addresses, as long as each address is unique. Messages that arrive for any of these aliases are directed to the primary address.

   Access domains: Lists the access domains from which you can retrieve mail.

NOTE If no access domains are specified in the Access domain field, the user can retrieve mail from any domain.

To add an access domain:

a. Click Add (next to the Access domains field) to open the Set Domain window, and then enter either a regular domain name or an IP address. You must enter only one access domain each time you open the Access Domain name window. If you specify a domain that does not exist, or enter none, you effectively block email access.

b. Click OK.

Quota. Enter a number to limit your own disk quotas. Disk quotas allow administrators to limit the amount of disk space allotted to each user. For detailed information, see Chapter 5, “Managing Messaging Store” in *Netscape Messaging Server Administrator’s Guide*.

3. If Class of Service is used, click it to modify its settings.

4. To change your password, click Change Password, and then enter the following:

   Current Password. Enter the password you currently use to log into your network.

   New Password. Enter a password that is different from the current password.

   Retype New Password. Type the new password again to confirm it.

5. To modify telephone and mail information, click Personal Information and then modify the following as necessary:

   Telephone number. Enter your phone number as it appears in company records. Example: 454-555-4444.

   Fax number. Enter your fax number as it appears in company records. Example: 454-555-4444.

   Mobile number. Enter your mobile or cell phone number as it appears in company records. Example: 454-555-4444.

   Pager number. Enter your pager number as it appears in company records. Example: 454-555-4444.

   Mailing address. Enter a street address where you can receive print mail or packages. Example: 1234 Main Street, Anytown, AnyState.

   Web Page URL. Enter the URL for a web page that contains more information about you. Example: http://www.siroe.com/sales/reps

   Description. Enter a description for the web page that contains more information about you.

Preferred Language. Use the drop-down list to indicate your preferred language. Delegated Administrator will display the user interface localized for the preferred language. For example, the Siroe company has employees in Japan, and they have indicated they prefer to conduct business in Japanese. When the Siroe administrator sets this preference to Japanese for a user, Delegated Administrator displays the Japanese version of the user interface.

6. If Mail Delivery Options is displayed, click it and then modify the following information as necessary:

   Deliver incoming messages to:

   POP3/IMAP4 mailbox. To enable mail delivery to regular POP3 or IMAP4 mailboxes, select this option.

   Unix mailbox. To allow messages to be delivered to a designated Unix mailbox, select this option. Unix delivery is available only to users whose Messaging Server runs on a Unix host machine.

   Process incoming messages through one or more programs:

   By default, incoming messages are put in the inbox of the mail account the message is addressed to. Accounts can be configured to perform various operations with the messages it receives. Examples include putting incoming messages in particular mail folders, forwarding them somewhere else, or generating an automatic response. For detailed information, see Chapter 12, “Program Delivery” in *Netscape Messaging Server Administrator’s Guide.*

   Enable the following programs: If you want to specify a mechanism for forwarding messages to an external application for processing before delivery to you, select this option. Then enter the external application command(s) to be used for processing this user’s mail

   Forward a copy of each message to: Enter another address instead of or in addition to your primary address. This enables mail to automatically be forwarded to the specified address.

7. If Vacation Auto-Responder Rule is displayed, enter the following:

   Auto-responder mode. Use the drop-down list to select one of the following:

   ❍ **Off.** Disables auto-reply.

   ❍ **Echo.** An automatic reply is sent for each received message and the received message appended as a MIME attachment to the reply. If you select this mode, you can enter a reply message in the Message field.

- **Vacation.** The first message received by you from a given sender generates an automatic response; subsequent messages from that sender do not generate a response. If you select this mode, use the Vacation start/ end date options and enter a reply message in the Reply text field.
- **Auto-reply.** Every incoming message received by you generates the specified automatic response. (The received message is not attached to the reply.) If you select this mode, you can enter a reply message in the Message field.

If you selected vacation mode, supply dates and times to determine when the auto-reply message should start and end:

- **Vacation Start Date**. If your vacation begins immediately, choose Now. If you want to specify a date, choose Date and then use the drop-down lists to indicate the date.
- **Vacation Start Time**. Enter the start time using the 24-hour format.
- **Vacation End Date**. If you don't have a specific end date, choose Never. If you want to specify a date, choose Date and then use the drop-down lists to indicate the date.
- **Vacation End Time.** Enter the end time using the 24-hour format.

Message text. If you selected echo, vacation, or auto-reply mode, type a reply message to be returned to the sender. When the Vacation Auto-Responder is activated, Delegated Administrator will send the following default messages unless a specific text message is created:

Echo mode:

"This account has been configured to echo all mail, with no added text"

Vacation:

This person is currently on vacation.

Auto-Reply:

This account has been configured to reply to all mail, with no text.

8. Click OK.

Modifying Configuration Information

As an Organization administrator, you have access permissions to modify the Delegated Administrator configuration in the directory. The configuration parameters effect the way the Delegated Administrator user interface is displayed, the information it captures, and the way it processes the information. Changing the configuration changes the way Delegated Administrator works for you. You'll find detailed information about modifying Delegated Administrator configuration in Chapter 11 of the *Installation and Customization Guide.*

Mail Lists

Mail lists make it possible for a user to send the same message to a number of users at one time. A mail list specifies the email addresses (users) that receive all messages sent to a single email address. For example, in the Siroe company, if you send one email to the address `sales@Siroe.com`, each employee in the Sales Department will receive the email.

NOTE You cannot use Delegated Administrator to manage mail lists unless Netscape Messaging Server 4.x is installed and properly configured. The following mail list features and functionality will not be available to you until a higher-level administrator enables them for you.

Mail List Owners

A mail list may have one or more owners assigned to it. The owner can perform all operations on the mail list including creating new mail lists and assigning owners. The owner can edit the properties of any mail list that he or she owns. If the owner is a properly authorized administrator or user, he or she can create mail lists and assign owners to the lists.

Moderated Mail Lists

You can assign a moderator to filter messages sent to the mail list. This is useful in preventing unrelated messages from being distributed to members of the mail list. When you designate a moderator, the mail list is known as a *moderated lis*t. In a moderated mail list, all messages sent by members of the mail list are sent to the moderator. The moderator either approves or rejects the messages, and then sends only approved messages to all members of the mail list.

Managing Mail Lists

By default, the following administrators have access privileges for managing mail lists:

- Organization
- Top-level Help Desk
- Organization Help Desk

Their access privileges allow them to create and delete mail lists, subscribe to mail lists, or unsubscribe from them. In contrast, Group administrators and individual users cannot create or manage mail lists until they are granted sufficient privileges by a Top-level or Organization administrator. There are three different paths to managing your mail lists. Your role as administrator or as an individual user determines which path you should use. Table 9-1 provides a summary of administrator mail management privileges and the paths they must take to manage mail lists.

Table 9-1 Accessing Mail List Management Options

Administrator	Default Mail List Privileges	Go To
Organization	Can create, edit, delete lists; subscribe to or unsubscribe from lists.	Organization administration page
Help Desk	Can create, edit, delete lists; subscribe to or unsubscribe from lists.	My Account page
Group	Can subscribe to or unsubscribe from mail lists. Cannot create or edit mail lists until granted privileges by Organization administrator.	My Account page
User Account	Can subscribe to or unsubscribe from mail lists. Cannot create or edit mail lists until granted privileges by Organization administrator.	User Account administration page

Organization Administrators’ Mail Lists

Organization administrates use organization administration pages to manage their mail lists.

To Create a New Mail List

1. Navigate to the administration page of the organization in which the mail list will be created.
2. In the task bar, click New Mail List.
3. In the New Mail List window, enter Mail List information. Skip to step 4 of To Create a New Mail List in the section “Managing Mail Lists.”

To Edit a Mail List

1. Navigate to the administration page for the organization in which the mail list was created.
2. Use the Search feature to generate a list of mail lists in the organization.
3. In the Search results, in the right pane, locate the mail list you want to edit. In the drop-down list, choose Edit.
4. In the Edit Mail List window, make changes as necessary. For detailed information about each field, see step 4 of To Create a New Mail List in the section “Managing Mail Lists.”
5. Click OK.

To Subscribe to a Mail List

1. Navigate to the administration page for the organization in which the mail list was created.
2. Use the Search feature to generate a list of mail lists in the organization.
3. In the Search results, in the right pane, locate the mail list you want to subscribe to. Use the drop-down list to choose Edit.
4. In the Edit Mail List window, click the Add button beside the Members list.
5. In the Add Members window, use the Search feature to locate your own user ID, and then click it. Your user ID is added to the Members list.
6. In the Edit Mail List window, click OK.

To Unsubscribe from a mail list

1. Navigate to the administration page for the organization in which the mail list was created.
2. Use the Search feature to generate a list of mail lists in the organization.

3. In the Search results, in the right pane, locate the mail list you want to unsubscribe from. Use the drop-down list to choose Edit.
4. In the Edit Mail List window, locate your user ID in the Members list, and then click it to select it.
5. Click the Remove button beside the Members list. Your user ID is deleted from the Members list.
6. In the Edit Mail List window, click OK.

To Delete a mail list

1. Navigate to the administration page for the organization in which the mail list was created.
2. Use the Search feature to generate a list of mail lists in the organization.
3. In the Search results, in the right pane, locate the mail list you want to delete. In the drop-down list, choose Delete.
4. When you see a confirmation message, click OK.

Help Desk Administrators' Mail Lists

Organization Help Desk Administrators manage mail lists through the My Account page.

To Create a New Mail List

1. Click My Account in the upper banner of your administration page.
2. In the My Account window, click Manage Mail Lists.
3. In the My Account Mail window, click Create Mail List.
4. In the New Mail List window, provide the following mail list information:

   Mail List Name. Enter a name that describes the mail list. Example: Sales

   Description. Enter a description of the purpose or nature of the mail list. You can use this field to enter a URL to an HTML page providing additional information about the mail list. This is for informational purposes only; the URL is not used by Messaging Server or by Delegated Administrator.

   Primary Email Address. Enter the publicized address to which mail for the mail list can be. There can be only one primary address, which must be a valid, correctly formatted SMTP address conforming to RFC 821 specifications.

Alternate Email Addresses. This field displays a list of alternate email addresses, or aliases to the primary email address. Click Add to modify the information in this field. Then, in the Set Mail Address window, provide the following information:

- Enter an alternate addres. This is essentially an alias for the user's primary address. For example, if a user's primary address is `smythe@siore.com`, he enters `smith@siroe.com` as an alternate address. This ensures that he will receive messages that are mistakenly addressed to "smith."
- You can specify any number of alternate addresses as long as each address is unique. Messages that arrive for any of these aliases are directed to the primary address.

Owners. To add an existing user to the Owners list, click the corresponding Add button. Then use the Search for User window to locate and select the user.

Members. To add a user to the mail list, click the corresponding Add button. Then use the Add Member window to locate and select the user.

Person for Bounced Messages. Use the search feature to locate and select the person, possibly a list owner or system administrator, to whom error messages should be sent when mail sent to the list can not be delivered.

Allow users to join. If you want to allow users to add themselves to the mail list, choose Yes. If you want to restrict users from adding themselves to the mail list, choose No.

Show Members of List To. If you want the owners and members of this list to be able to view the members' names, choose All. If you want no owners or members to be able to view members' names, choose None.

Hide Mail List. If you want to make a mail list visible to all users for subscription purposes, choose No. To make the mail list visible to only Organization Administrators, choose Yes.

Authorized Senders to List. Enter information regarding users, groups of users or specific domains that are allowed to post messages to the mail list:

> **Anyone.** Any user may contribute to the mail list.
>
> **Anyone in the mail list.** Only users included in the mail list may contribute to the mail list.
>
> **Anyone in the following list**. If you want to allow specific individuals or groups of individuals to be able to post messages to the mail list, click the associated radio button. Then specify the following:

Users and Groups. This fields displays the list of individual users and groups from which messages will be accepted for posting to this mail list. To Add a user or group to the list, click the corresponding Add button. If no user or group is specified, there is no sender-user restriction.

DNS Domains. This fields displays the list of domains from which messages will be accepted for posting to this mail list. To Add a domain name to the list, click the corresponding Add button. If no domain is specified, there is no sender-domain restriction.

When Message to this List is rejected:

Send message to Moderator(s). If you want to automatically forward rejected messages to the mailing-list moderator or moderators for further action, select this option. If you select this option, you must add at least one entry in the List moderators field. To add a user to the moderator list, click the corresponding Add button. Then use the Add Moderator window to locate and select a user.

5. Click OK.

To Edit a mail list

1. Click My Accounts in the upper banner of your administration page.
2. In the My Account window, click Manage Mail Lists.
3. In the Manage Mail Lists window, click Owned Mail Lists.
4. Use the Search feature to generate a list of your mail lists.
5. In the Search results, locate the mail list you want to edit, and click its name.
6. In the Edit Mail List window, make changes as necessary, and then click OK.

To Subscribe to a mail list

1. Click My Account in the upper banner of your administration page.
2. Use the Search feature to generate a list of mail lists in the organization.
   a. Select Subscribe to generate a list of mail lists that you currently subscribe to.
   b. Select Unsubscribe to generate a list of available mail lists that you can subscribe to.

3. In the Search results, locate the mail list you want to subscribe to, and then click Subscribe.
4. In the Subscribe Mail List window, click Subscribe.
5. In the Status window, click Continue.

To Unsubscribe from a mail list

1. Click My Account in the upper banner of your administration page.
2. Use the Search feature to generate a list of mail lists in the organization.
   a. Select Subscribe to generate a list of mail lists that you currently subscribe to.
   b. Select Unsubscribe to generate a list of available mail lists that you can subscribe to.
3. In the Search results, locate the mail list you want to unsubscribe from, and then click Unsubscribe.
4. In the Unsubscribe Mail List window, click Unsubscribe.
5. In the Status window, click Continue.

To Delete a mail list

1. In your administration page, use the Search feature to generate a list of Mail Lists.
2. In the Search results, in the right pane, locate the mail list you want to delete. In the drop-down list, choose Delete.
3. When you see a confirmation message, click Continue.

Group and User Account Administrators

Group administrators and individual users can create and manage mail lists only if they are granted mail list privileges from an Organization Administrator. Once a user is granted mail list privileges, the Manage Mail Lists option is displayed in their account information window.

To Create a New Mail List

1. In the top of Help Desk administration page, click My Account.
2. In the My Account window, click Manage Mail Lists.

3. In the My Account Mail window, click Create Mail List.

4. In the New Mail List window, provide the following mail list information:

   Mail List Name. Enter a name that describes the mail list. Example: Sales

   Description. Enter a description of the purpose or nature of the mail list. You can use this field to enter a URL to an HTML page providing additional information about the mail list. This is for informational purposes only; the URL is not used by Messaging Server or by Delegated Administrator.

   Primary Email Address. Enter the publicized address to which mail for the mail list can be sent. There can be only one primary address, which must be a valid, correctly formatted SMTP address conforming to RFC 821 specifications.

   Alternate Email Addresses. This field displays a list of alternate email addresses, or aliases to the primary email address. Click Add to modify the information in this field. Then, in the Set Mail Address window, the following the following:

   - Enter an alternate address. This is essentially an alias for the primary address. For example, if a primary address is `humanresources@siore.com`, you can enters `hr@siroe.com` as an alternate address. This ensures that he will receive messages that are mistakenly addressed to “hr.”

   - You can specify any number of alternate addresses for a particular user, as long as each address is unique. Messages that arrive for any of these aliases are directed to the primary address.

   Owners. To add an existing user to the Owners list, click the corresponding Add button. Then use the Search for User window to locate and select the user.

   Members. To add a user to the mail list, click the corresponding Add button. Then use the Add Member window to locate and select the user.

   Person for Bounced Messages. Enter the email address of the person, possibly a list owner or system administrator, to whom error messages should be sent when mail sent to the list bounces. The address you enter in this field must be a correctly-formatted, valid SMTP address conforming to RFC 821 specifications.

   Allow users to join. If you want to allow users to add themselves to the mail list, choose Yes. If you want to restrict users from adding themselves to the mail list, choose No.

   Show Members of List To. If you want the owners and members of this list to be able to view the members’ names, choose All. If you want no owners or members to be able to view members’ names, choose None.

Hide Mail List. If you want to make a mail list visible to all users for subscription purposes, choose No. To make the mail list visible to only Organization Administrators, choose Yes.

Authorized Senders to List. Enter information regarding users, groups of users or specific domains that are allowed to post messages to the mail list:

Anyone. Any user may contribute to the mail list.

Anyone in the mail list. Only users included in the mail list may contribute to the mail list.

Anyone in the following list. If you want to allow specific individuals or groups of individuals to be able to post messages to the mail list, click the associated radio button. Then specify the following:

Users and Groups. This fields displays the list of individual users and groups from which messages will be accepted for posting to this mail list. To Add a user or group to the list, click the corresponding Add button. If no user or group is specified, there is no sender-user restriction.

DNS Domains. This fields displays the list of domains from which messages will be accepted for posting to this mail list. To Add a domain name to the list, click the corresponding Add button. If no domain is specified, there is no sender-domain restriction.

When Message to this List is rejected:

Send message to Moderator(s). If you want to automatically forward rejected messages to the mailing-list moderator or moderators for further action, select this option. If you select this option, you must add at least one entry in the List moderators field. To add a user to the moderator list, click the corresponding Add button. Then use the Add Moderator window to locate and select a user.

5. Click OK.

To Edit a Mail List

1. Click My Accounts in the upper banner of your administration page.
2. In the My Account window, click Manage Mail Lists.
3. In the Manage Mail Lists window, click Owned Mail Lists.
4. Use the Search feature to generate a list of your mail lists.
5. In the Search results, locate the mail list you want to edit, and click its name.
6. In the Edit Mail List window, make changes as necessary, and then click OK.

To Subscribe to a Mail List

1. Click My Account in the upper banner of your administration page.
2. Use the Search feature to generate a list of mail lists in the organization.
    a. Select Subscribe to generate a list of mail lists that you currently subscribe to.
    b. Select Unsubscribe to generate a list of available mail lists that you can subscribe to.
3. In the Search results, locate the mail list you want to subscribe to, and then click Subscribe.
4. In the Subscribe Mail List window, click Subscribe.
5. In the Status window, click Continue.

To Unsubscribe from a Mail List

1. Click My Account in the upper banner of your administration page.
2. In the My Account window, click Manage Mail Lists.
3. Use the Search feature to generate a list of mail lists in the organization.
    a. Select Subscribe to generate a list of mail lists that you currently subscribe to.
    b. Select Unsubscribe to generate a list of available mail lists that you can subscribe to.
4. In the Search results, locate the mail list you want to unsubscribe from, and then click Unsubscribe.
5. In the Unsubscribe Mail List window, click Unsubscribe.
6. In the Status window, click Continue.

To Delete a Mail List

1. In your administration page, use the Search feature to generate a list of Mail Lists.
2. In the Search results, in the right pane, locate the mail list you want to delete. In the drop-down list, choose Delete.
3. When you see a confirmation message, click Continue.

Chapter 10

Organization Help Desk Administrators

This document provides step-by-step instructions that an Organization Help Desk Administrator will need on a day-to-day basis. The topics included in this document are:

- Logging In
- The Organization Help Desk Administration Page
- Using the Search Feature
- Changing a User's Password
- My Account
- Mail Lists

Logging In

The user ID and password you use to log in determines your administrator role and determines which branches of the directory you have access to. There are two ways you can log in to Delegated Administrator.

- If you are using the default Delegated Administrator tree, and you are using the sample data that shipped with the product, you can use the Start Page to help you get started. See "The Start Page" on page 43 for more information. Once you're familiar with the product and with your administrator role, you can bypass the Start Page you go directly to the Login window to log in.
- If you have modified the Delegated Administrator tree, or you are not using the sample data that shipped with the product, you will not see the Start Page. You must log in using the Login window. See "Using the Login Window" on page 232 for more information.

Using the Start Page

The Start Page was designed to provide all the information you need to quickly begin using Delegated Administrator with sample data and the default organization `Siroe.com`.

NOTE If you installed Delegated Administrator against an existing directory, this sample data was not automatically installed. Skip to the next section, "Using the Login Window" on page 232.

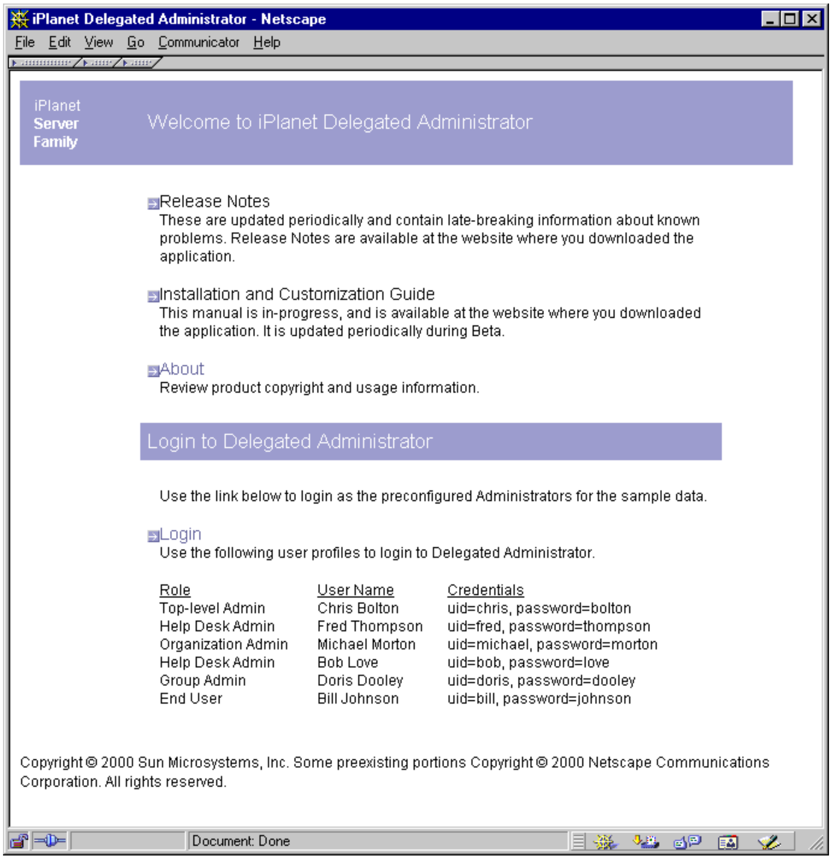
You can access the Start Page at any time by pointing a web browser to `http://<host_name>:<port>/nda/start.html`

You can use the Start Page to log in as any level of administrator named in the page. The user ID and password you use to log in determines your administrator role and determines which branches of the directory you have access to.

To start Delegated Administrator from the Start Page

1. Point a browser to the URL for the Delegated Administrator host using the form `http://<host:webserver_port>/nda/start.html`.

Figure 10-1 The Start Page



Welcome to iPlanet Delegated Administrator

Release Notes
These are updated periodically and contain late-breaking information about known problems. Release Notes are available at the website where you downloaded the application.

Installation and Customization Guide
This manual is in-progress, and is available at the website where you downloaded the application. It is updated periodically during Beta.

About
Review product copyright and usage information.

Login to Delegated Administrator

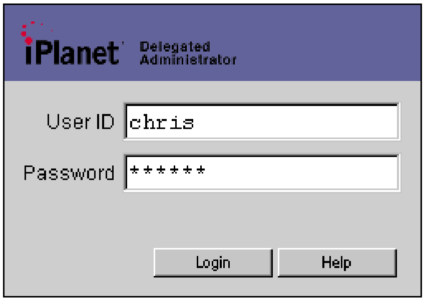
Use the link below to login as the preconfigured Administrators for the sample data.

Login
Use the following user profiles to login to Delegated Administrator.

Role	User Name	Credentials
Top-level Admin	Chris Bolton	uid=chris, password=bolton
Help Desk Admin	Fred Thompson	uid=fred, password=thompson
Organization Admin	Michael Morton	uid=michael, password=morton
Help Desk Admin	Bob Love	uid=bob, password=love
Group Admin	Doris Dooley	uid=doris, password=dooley
End User	Bill Johnson	uid=bill, password=johnson

Copyright © 2000 Sun Microsystems, Inc. Some preexisting portions Copyright © 2000 Netscape Communications Corporation. All rights reserved.

2. Click Login.



User ID chris

Password ******

In the Delegated Administrator Login window, using the information on the Start Page, enter an administrator's system user ID and password. For example, to log in as the Service Administrator, Chris Bolton, enter the following:

User ID. chris

Password. bolton

3. Click Login.

Delegated Administrator displays the administration page that is appropriate for the User ID you entered. By default, your Delegated Administrator session will time out after thirty minutes of inactivity.

Using the Login Window

If you want to bypass the Start Page, or if the Start Page is not available to you, you can start Delegated Administrator and go directly to the Login window in one step.

To Start Delegated Administrator and Log In:

1. Point a browser to the URL for the Delegated Administrator host. Example:

   `http://<host_name>:<port>/nda/default/en/login.html`

2. In the Login window, enter your system user ID and password.

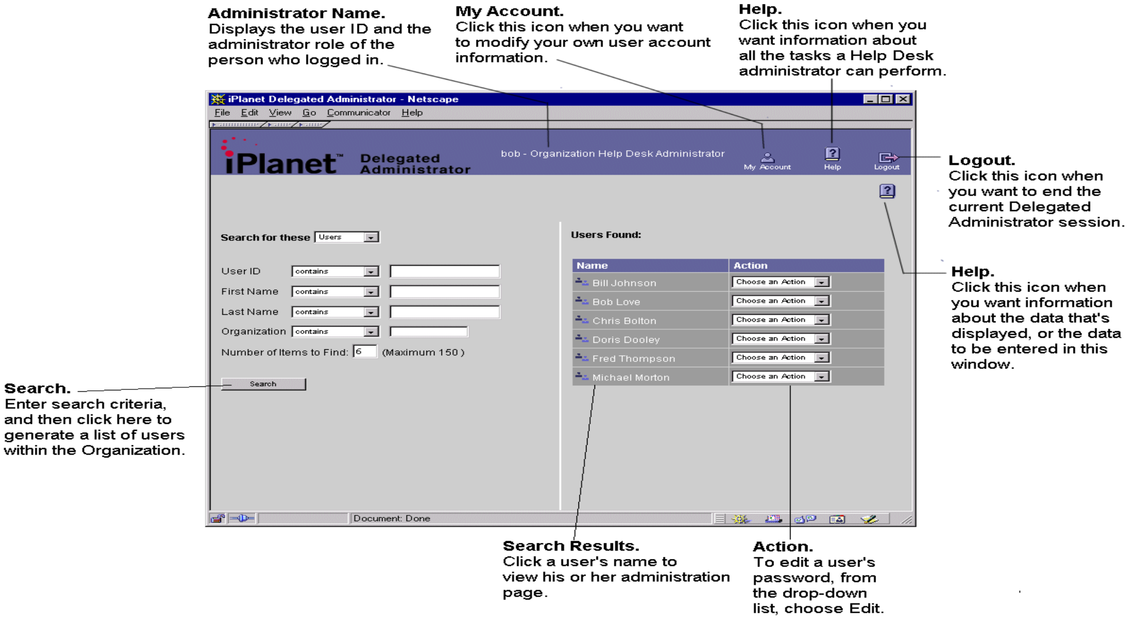
3. Click Login.

   Delegated Administrator displays the administration page that is appropriate for your administrator role. By default, your Delegated Administrator session will time out after thirty minutes of inactivity.

The Organization Help Desk Administration Page

The Organization administrator page provides access to all features and functions you're allowed to access. Figure 10-2 provides a quick tour of the page.

Figure 10-2 The Organization Help Desk administration page.



iPlanet Delegated Administrator - Netscape

bob - Organization Help Desk Administrator

Search for these: Users

User ID: contains

First Name: contains

Last Name: contains

Organization: contains

Number of Items to Find: 6 (Maximum 150)

Users Found:

Name	Action
Bill Johnson	Choose an Action
Bob Love	Choose an Action
Chris Bolton	Choose an Action
Doris Dooley	Choose an Action
Fred Thompson	Choose an Action
Michael Morton	Choose an Action

Document: Done

File Edit View Go Communicator Help
iPlanet™ Delegated Administrator
My Account
Help
Logout
Search

Administrator Name. Displays the user ID and the administrator role of the person who logged in.

My Account. Click this icon when you want to modify your own user account information.

Help. Click this icon when you want information about all the tasks a Help Desk administrator can perform.

Logout. Click this icon when you want to end the current Delegated Administrator session.

Help. Click this icon when you want information about the data that's displayed, or the data to be entered in this window.

Search. Enter search criteria, and then click here to generate a list of users within the Organization.

Search Results. Click a user's name to view his or her administration page.

Action. To edit a user's password, from the drop-down list, choose Edit.

Using the Search Feature

Use the Search feature to locate a user or mail list in the top level of the Delegated Administrator tree.

To Locate a User or Mail List

1. Use the Search for drop-down list to indicate whether you're searching for a user or mail list.

2. Use the remaining drop-down lists to indicate your search criteria.

   Number of Items to Find. Enter the number of search results you want to see displayed. The default is 5, but you can enter a number up to 150.

3. Click Search to generate a list of users or mail lists.

4. Once you locate a user or mail list:

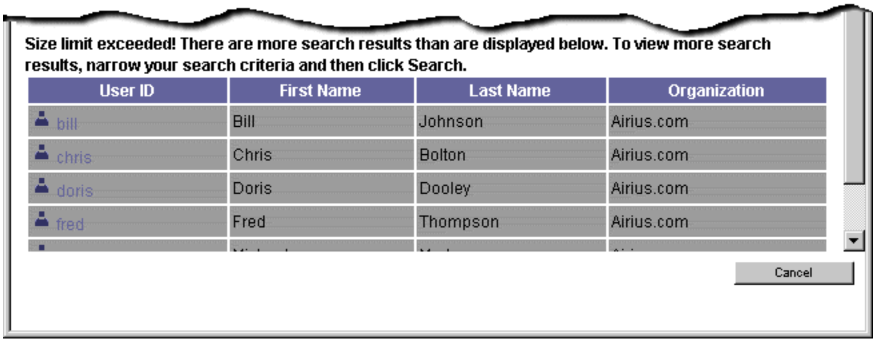
   - Click the object's name to view and edit its settings or properties.

   Choose an action from the corresponding Action drop-down list.

Exceeding the Search Results Size Limit

If you see the message regarding size limit (see Figure 10-3), the search operation found more results than the number you specified above, and cannot display all the results. When this happens, you can either enter a greater number in the **Display no more than....** field above, or you can enter more specific search criteria and begin the search again

Figure 10-3 Size limit message.



Size limit exceeded! There are more search results than are displayed below. To view more search results, narrow your search criteria and then click Search.

User ID	First Name	Last Name	Organization
bill	Bill	Johnson	Airius.com
chris	Chris	Bolton	Airius.com
doris	Doris	Dooley	Airius.com
fred	Fred	Thompson	Airius.com

Changing a User’s Password

You may need to change a user’s password when the individual forgets it, or otherwise needs your help to reset it.

To Change a User’s Password

1. Use the Search feature to generate a list of users within the Organization.
2. In the Search results, locate the user, and then choose Edit from the drop-down list.
3. In the Basic Account Information window, click Change Password.
4. In the Change Password window, enter the following:

   Password. Enter the new password.

   Retype the password. Enter the password again to confirm it
5. Click OK.

In the Basic Account Information window, you can view, but you cannot edit, the following information:

Login ID. Displays the user’s system user ID as assigned by a network administrator.

First name. Displays the user’s given name as it appears on official company records.

Last name. Displays the user’s surname as it appears in company records.

Organization. Displays the published name of the organization the user belongs to.

Title. Displays the user’s job title as it appears on official company records.

Manager. Displays the distinguished name (DN) of the user's manager.

Email address. Displays the user’s email address. .

Telephone number. Displays the user’s phone number as it appears in company records.

Fax number. Displays the user’s fax number as it appears in company records.

Mobile number. Displays the user’s mobile or cell phone number as it appears in company records.

Pager number. Displays the user's pager number as it appears in company records.

Mailing address. Displays a street address where the user can receive print mail or packages.

Web Page URL. Displays the URL for a web page that contains more information about the user.

Description. Displays a word or phrase that describes the web page above.

Preferred Language. Displays the user's preferred language. The Delegated Administrator will use the user interface localized for the preferred language. For example, the Siroe company has employees in Japan, and they have indicated they prefer to conduct business in Japanese. When the Siroe administrator sets this preference to Japanese for a user, Delegated Administrator displays the Japanese version of the user interface.

My Account

When an end user logs in using their his ID and password, an administration page for the individual's user account is usually displayed. When you log in, however, because you belong to an administrator group, an administration page is displayed. The My Account icon allows you play the role of an end user and modify your own user account information.

To Modify Information in Your Own User Account

1. Click My Account in the upper banner of any administration page.
2. In the My Account window, click Account Information to view your account information:

   Login ID. Displays your system user ID as assigned by a network administrator.

   First name. Displays your given name as it appears on official company records.

   Last name. Displays your surname as it appears on official company records.

   Email addresses:

Alternate Email Addresses. This field displays a list of your alternate email addresses, or aliases to the primary email address.

Access domains: Lists the access domains from which you can retrieve mail.

NOTE If no access domains are specified in the Access domain field, the you can retrieve mail from any domain.

Quota. Dispalys your own disk quotas. Disk quotas allow administrators to limit the amount of disk space allotted to each user.

3. If Class of Service is used, click it to modify its settings.

4. To change your password, click Change Password, and then enter the following:

   Current Password. Enter the password you currently use to log into your network.

   New Password. Enter a password that is different from the current password.

   Retype New Password. Type the new password again to confirm it.

5. To modify telephone and mail information, click Personal Information and then modify the following as necessary:

   Telephone number. Enter your phone number as it appears in company records. Example: 454-555-4444.

   Fax number. Enter your fax number as it appears in company records. Example: 454-555-4444.

   Mobile number. Enter your mobile or cell phone number as it appears in company records. Example: 454-555-4444.

   Pager number. Enter your pager number as it appears in company records. Example: 454-555-4444.

   Mailing address. Enter a street address where the you can receive print mail or packages. Example: 1234 Main Street, Anytown, AnyState.

   Web Page URL. Enter the URL for a web page that contains more information about the you. Example: http://www.siroe.com/sales/reps

   Description. Enter a description for the web page that contains more information about you.

Preferred Language. Use the drop-down list to indicate your preferred language. Delegated Administrator will display the user interface localized for the preferred language. For example, the Siroe company has employees in Japan, and they have indicated they prefer to conduct business in Japanese. When the Siroe administrator sets this preference to Japanese for a user, Delegated Administrator displays the Japanese version of the user interface.

6. If Mail Delivery Options is displayed, click it and then modify the following information as necessary:

Deliver incoming messages to:

POP3/IMAP4 mailbox. To enable mail delivery to regular POP3 or IMAP4 mailboxes, select this option.

Unix mailbox. To allow messages to be delivered to a designated Unix mailbox, select this option. Unix delivery is available only to users whose Messaging Server runs on a Unix host machine.

Process incoming messages through one or more programs:

By default, incoming messages are put in the inbox of the mail account the message is addressed to. Accounts can be configured to perform various operations with the messages it receives. Examples include putting incoming messages in particular mail folders, forwarding them somewhere else, or generating an automatic response. For detailed information, contact your system administrator.

Enable the following programs: If you want to specify a mechanism for forwarding messages to an external application for processing before delivery to you, select this option. Then enter the external application command(s) to be used for processing this user's mail

Forward a copy of each message to: Enter another address instead of or in addition to your primary address. This enables mail to automatically be forwarded to the specified address.

7. If Vacation Auto-Responder Rule is displayed, enter the following:

Auto-responder mode. Use the drop-down list to select one of the following:

- **Off.** Disables auto-reply.
- **Echo.** An automatic reply is sent for each received message and the received message appended as a MIME attachment to the reply. If you select this mode, you can enter a reply message in the Message field.

- **Vacation.** The first message received by you from a given sender generates an automatic response; subsequent messages from that sender do not generate a response. If you select this mode, use the Vacation start/ end date options and enter a reply message in the Reply text field.
- **Auto-reply.** Every incoming message received by you generates the specified automatic response. (The received message is not attached to the reply.) If you select this mode, you can enter a reply message in the Message field.

If you selected vacation mode, supply dates and times to determine when the auto-reply message should start and end:

- **Vacation Start Date**. If your vacation begins immediately, choose Now. If you want to specify a date, choose Date and then use the drop-down lists to indicate the date.
- **Vacation Start Time**. Enter the start time using the 24-hour format.
- **Vacation End Date**. If you don’t have a specific end date, choose Never. If you want to specify a date, choose Date and then use the drop-down lists to indicate the date.
- **Vacation End Time.** Enter the end time using the 24-hour format.

Message text. If you selected echo, vacation, or auto-reply mode, type a reply message to be returned to the sender. When the Vacation Auto-Responder is activated, Delegated Administrator will send the following default messages unless a specific text message is created:

Echo mode:

“This account has been configured to echo all mail, with no added text”

Vacation:

This person is currently on vacation.

Auto-Reply:

This account has been configured to reply to all mail, with no text.

8. If you want to create or manage mail lists, click Manage Mail Lists. Then skip to step 4 of To Create a New Mail List.
9. Click OK.

Mail Lists

Mail lists make it possible for a user to send the same message to a number of users at one time. A mail list specifies the email addresses (users) that receive all messages sent to a single email address. For example, in the Siroe company, if you send one email to the address `sales@Siroe.com`, each employee in the Sales Department will receive the email.

NOTE You cannot use Delegated Administrator to manage mail lists unless Netscape Messaging Server 4.x is installed and properly configured. The following mail list features and functionality will not be available to you until a higher-level administrator enables them for you.

As a Help Desk administrator, by default, you have access permissions to create and manage mail lists.

Mail List Owners

A mail list may have one or more owners assigned to it. The owner can edit the properties of the mail list that he or she owns. The owner can perform all operations on the mail list except for creating new mail lists and assigning owners. If the owner is a properly authorized administrator or user, he or she can create mail lists and assign owners to the lists.

Moderated Mail Lists

You can assign a moderator to filter messages sent to the mail list. This is useful in preventing unrelated messages from being distributed to members of the mail list. When you designate a moderator, the mail list is known as a *moderated lis*t. In a moderated mail list, all messages sent by members of the mail list are sent to the moderator. The moderator either approves or disapproves the messages, and then sends the only approved messages to all members of the mail list.

To Create a New Mail List

1. Click My Account in the upper banner of your administration page.
2. In the My Account window, click Manage Mail Lists.
3. In the My Account Mail window, click Create Mail List.

4. In the New Mail List window, provide the following mail list information:

   Mail List Name. Enter a name that describes the mail list. Example: Sales

   Description. Enter a description of the purpose or nature of the mail list. You can use this field to enter a URL to an HTML page providing additional information about the mail list. This is for informational purposes only; the URL is not used by Messaging Server or by Delegated Administrator.

   Primary Email Address. Enter the publicized address to which mail for the mail list can be sent. There can be only one primary address, which must be a valid, correctly formatted SMTP address conforming to RFC 821 specifications.

   Alternate Email Addresses. This field displays a list of alternate email addresses, or aliases to the primary email address. Click Add to modify the information in this field. Then, in the Set Mail Address window, provide the following information:

   ❍ Enter an alternate address. This is essentially an alias for the primary address. For example, if a primary address is `humanresources@siore.com`, you can enter `hr@siroe.com` as an alternate address. This ensures that recipients will receive messages that are mistakenly addressed to “hr.”

   ❍ You can specify any number of alternate addresses as long as each address is unique. Messages that arrive for any of these aliases are directed to the primary address.

   Owners. To add an existing user to the Owners list, click the corresponding Add button. Then use the Search for User window to locate and select the user.

   Members. To add a user to the mail list, click the corresponding Add button. Then use the Add Member window to locate and select the user.

   Person for Bounced Messages. Use the search feature to locate and select the person, possibly a list owner or system administrator, to whom error messages should be sent when mail sent to the list can not be delivered.

   Allow users to join. If you want to allow users to add themselves to the mail list, choose Yes. If you want to restrict users from adding themselves to the mail list, choose No.

   Show Members of List To. If you want the owners and members of this list to be able to view the members’ names, choose All. If you want no owners or members to be able to view members’ names, choose None.

Hide Mail List. If you want to make a mail list visible to all users for subscription purposes, choose No. To make the mail list visible to only Top-level and Organization Administrators, choose Yes.

Authorized Senders to List. Enter information regarding users, groups of users or specific domains that are allowed to post messages to the mail list:

Anyone. Any user may contribute to the mail list.

Anyone in the mail list. Only users included in the mail list may contribute to the mail list.

Anyone in the following list. If you want to allow specific individuals or groups of individuals to be able to post messages to the mail list, click the associated radio button. Then specify the following:

Users and Groups. This fields displays the list of individual users and groups from which messages will be accepted for posting to this mail list. To Add a user or group to the list, click the corresponding Add button. If no user or group is specified, there is no sender-user restriction.

DNS Domains. This fields displays the list of domains from which messages will be accepted for posting to this mail list. To Add a domain name to the list, click the corresponding Add button. If no domain is specified, there is no sender-domain restriction.

When Message to this List is rejected:

Send message to Moderator(s). If you want to automatically forward rejected messages to the mailing-list moderator or moderators for further action, select this option. If you select this option, you must add at least one entry in the List moderators field. To add a user to the moderator list, click the corresponding Add button. Then use the Add Moderator window to locate and select a user.

5. Click OK.

To Edit a Mail List

1. Click My Accounts in the upper banner of your administration page.
2. In the My Account window, click Manage Mail Lists.
3. In the Manage Male Lists window, click Owned Mail Lists.
4. Use the Search feature to generate a list of your mail lists.
5. In the Search results, locate the mail list you want to edit, and click its name.
6. In the Edit Mail List window, make changes as necessary, and then click OK.

To Subscribe to a Mail List

1. Click My Account in the upper banner of your administration page.
2. Use the Search feature to generate a list of mail lists in the organization.
   a. Select Subscribe to generate a list of mail lists that you currently subscribe to.
   b. Select Unsubscribe to generate a list of available mail lists that you can subscribe to.
3. In the Search results, locate the mail list you want to subscribe to, and then click Subscribe.
4. In the Subscribe Mail List window, click Subscribe.
5. In the Status window, click Continue.

To Unsubscribe from a Mail List

1. Click My Account in the upper banner of your administration page.
2. Use the Search feature to generate a list of mail lists in the organization.
   a. Select Subscribe to generate a list of mail lists that you currently subscribe to.
   b. Select Unsubscribe to generate a list of available mail lists that you can subscribe to.
3. In the Search results, locate the mail list you want to unsubscribe from, and then click Unsubscribe.
4. In the Unsubscribe Mail List window, click Unsubscribe.
5. In the Status window, click Continue.

To Delete a Mail List

1. In your administration page, use the Search feature to generate a list of Mail Lists.
2. In the Search results, in the right pane, locate the mail list you want to delete. In the drop-down list, choose Delete.
3. When you see a confirmation message, click Continue.

Chapter 11

Group Administrators

This document provides step-by-step instructions that a Group administrator will need on a day-to-day basis. The topics included in this document are:

- Logging In
- My Groups and The Group Administration Page
- Managing Groups
- Managing User Accounts
- My Account
- Mail Lists

Logging In

The user ID and password you use to log in determines your administrator role and determines which branches of the directory you have access to. There are two ways you can log in to Delegated Administrator.

- If you are using the default Delegated Administrator tree, and you are using the sample data that shipped with the product, you can use the Start Page to help you get started. See "The Start Page" on page 43 for more information. Once you're familiar with the product and with your administrator role, you can bypass the Start Page you go directly to the Login window to log in.
- If you have modified the Delegated Administrator tree, or you are not using the sample data that shipped with the product, you will not see the Start Page. You must log in using the Login window. See "Using the Login Window" on page 248 for more information.

Using the Start Page

The Start Page was designed to provide all the information you need to quickly begin using Delegated Administrator with sample data and the default organization `Siroe.com`.

NOTE If you installed Delegated Administrator against an existing directory, this sample data was not automatically installed. Skip to the next section, "Using the Login Window" on page 248.

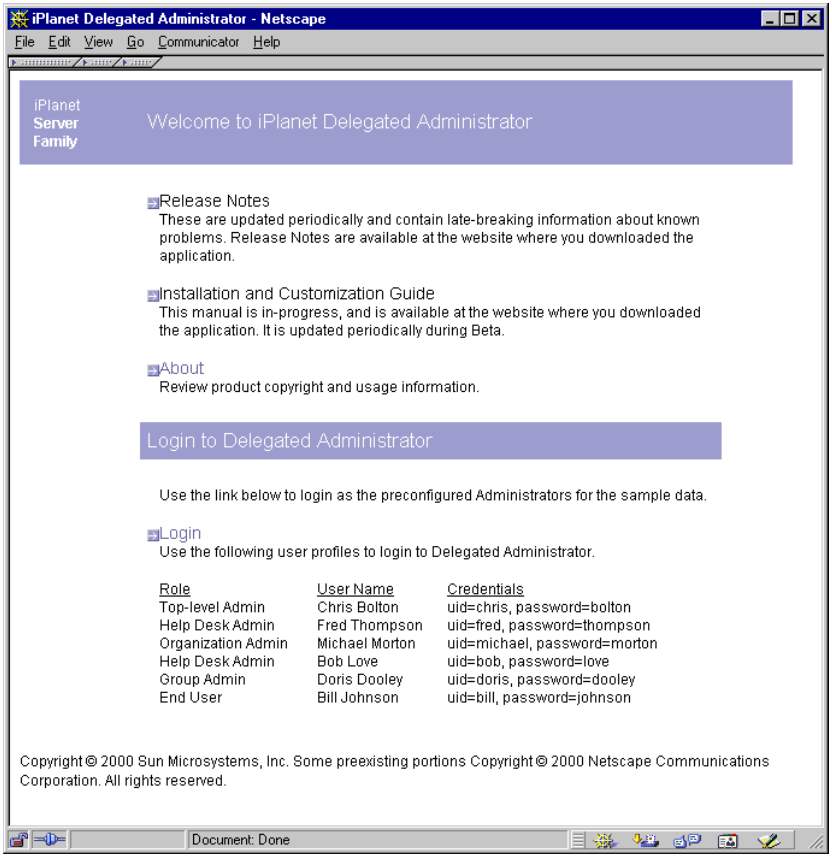
You can access the Start Page at any time by pointing a web browser to `http://<host_name>:<port>/nda/start.html`

You can use the Start Page to log in as any level of administrator named in the page. The user ID and password you use to log in determines your administrator role and determines which branches of the directory you have access to.

To start Delegated Administrator from the Start Page

1. Point a browser to the URL for the Delegated Administrator host using the form `http://<host:webserver_port>/nda/start.html`.

Figure 11-1 The Start Page



iPlanet Delegated Administrator - Netscape
File Edit View Go Communicator Help
iPlanet
Server
Family

Welcome to iPlanet Delegated Administrator

Release Notes
These are updated periodically and contain late-breaking information about known problems. Release Notes are available at the website where you downloaded the application.

Installation and Customization Guide
This manual is in-progress, and is available at the website where you downloaded the application. It is updated periodically during Beta.

About
Review product copyright and usage information.

Login to Delegated Administrator

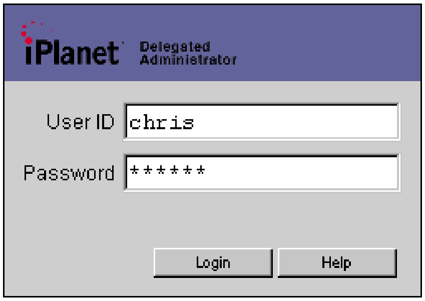
Use the link below to login as the preconfigured Administrators for the sample data.

Login
Use the following user profiles to login to Delegated Administrator.

Role	User Name	Credentials
Top-level Admin	Chris Bolton	uid=chris, password=bolton
Help Desk Admin	Fred Thompson	uid=fred, password=thompson
Organization Admin	Michael Morton	uid=michael, password=morton
Help Desk Admin	Bob Love	uid=bob, password=love
Group Admin	Doris Dooley	uid=doris, password=dooley
End User	Bill Johnson	uid=bill, password=johnson

Copyright © 2000 Sun Microsystems, Inc. Some preexisting portions Copyright © 2000 Netscape Communications Corporation. All rights reserved.

2. Click Login.



User ID chris

Password ******

In the Delegated Administrator Login window, using the information on the Start Page, enter an administrator's system user ID and password. For example, to log in as the Service Administrator, Chris Bolton, enter the following:

User ID. chris

Password. bolton

3. Click Login.

Delegated Administrator displays the administration page that is appropriate for the User ID you entered. By default, your Delegated Administrator session will time out after thirty minutes of inactivity.

Using the Login Window

If you want to bypass the Start Page, or if the Start Page is not available to you, you can start Delegated Administrator and go directly to the Login window in one step.

To Start Delegated Administrator and Log In:

1. Point a browser to the URL for the Delegated Administrator host. Example:

```
http://<host_name>:<port>/nda/default/en/login.html
```

2. In the Login window, enter your system user ID and password.

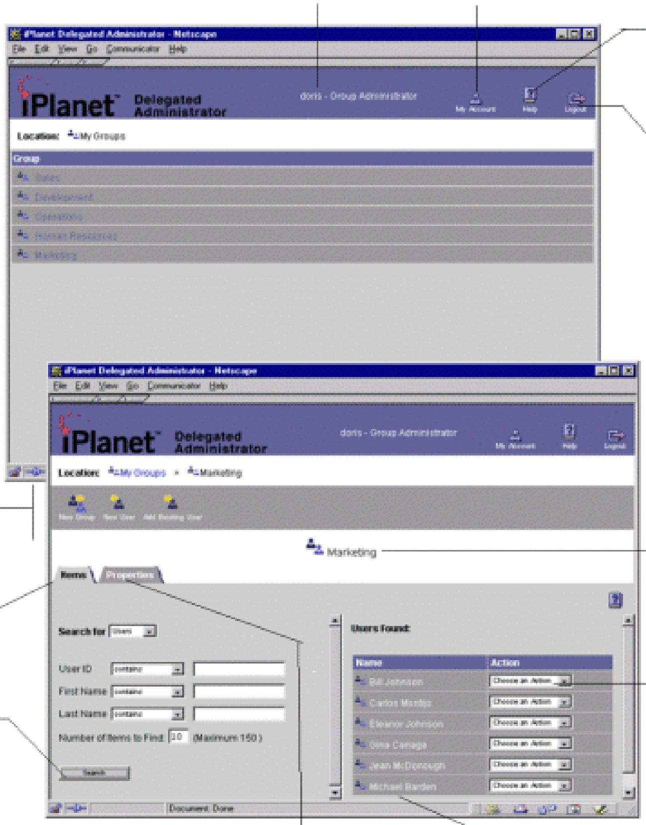
3. Click Login.

Delegated Administrator displays the administration page that is appropriate for your administrator role. By default, your Delegated Administrator session will time out after thirty minutes of inactivity.

My Groups and The Group Administration Page

The My Groups page and the Group administrator page provide access to all features and functions you're allowed to access. Figure 11-2 provides a quick tour of the page.

Figure 11-2 The My Groups page and the Group administration page.



Users Found:

Name	Action
Bill Johnson	Choose an Action
Carlos Mordijo	Choose an Action
Eleanor Johnson	Choose an Action
Gina Camaga	Choose an Action
Jean McDonough	Choose an Action
Michael Barden	Choose an Action

Location Bar. The last object in this list indicates where you are in the Delegated Administrator tree.

Administrator. Indicates the user ID and administrator role of the person who logged in.

My Account. Click this icon when you want modify your own user account information.

Help. Click this icon when you want information about all the tasks a Group administrator can perform.

Logout. Click this icon when you want to end the Delegated Administrator session.

Groups. Lists the groups you're allowed to manage. **Click a group name to open its administration page.**

Task Bar. Displays only the tasks you're allowed to perform.

Group Name. Indicates the group that is managed by this page.

Items. Click this tab when you want to locate a user or subgroup within this group.

Action. Use the drop-down list when you want to modify a user's account data, remove the user from the group, or delete the user from the Delegated Administrator tree.

Search. Enter search criteria, and then click this button to generate a list of groups or users within your scope of responsibility.

Properties. Click this tab when you want to add administrators to or remove them from group.

Search Result. Click a user's name when you want to view or edit his or her user account information.

Using the Location Bar

The Location Bar indicates you where you are in the directory tree. The last group listed indicates the group that is managed by the administration page. To navigate to the administration page for a different group, click its name or icon in the Location Bar.

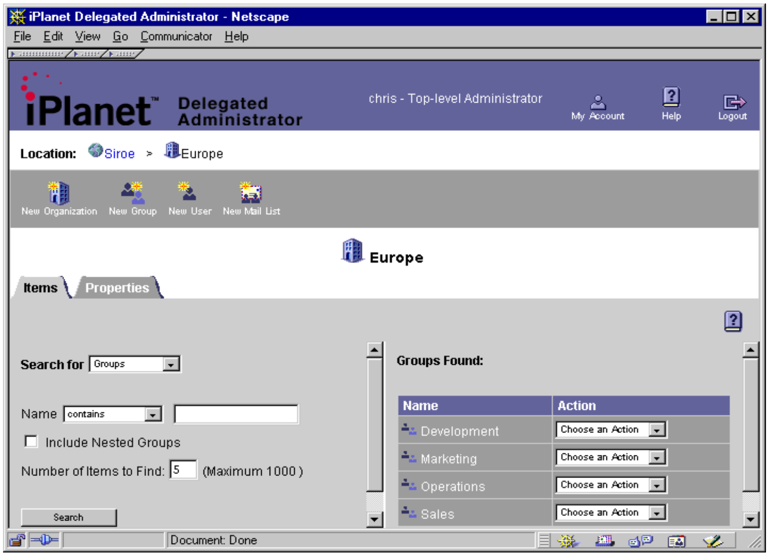
-

NOTE Do not use the Back and Forward buttons in your browser to navigate to administration pages in Delegated Administrator. If you use the Back and Forward buttons in your browser, the Location Bar will not properly display your location in the Delegated Administrator tree.

Using the Search Feature

You'll see two forms of the Search feature, but they work similarly. Figure 11-3 illustrates the Search feature embedded in the Items tab. Use the Search feature in the Items tab when you want to navigate further down in the tree, or when you want to edit or delete a user, group, or organization. Figure 11-4 shows a discrete Search window invoked when performing a task such as adding a new administrator from within the Properties Tab.

Figure 11-3 The Search feature embedded in the Items tab.



chris - Top-level Administrator

Location: Siroe > Europe

Europe

Search for Groups

Name contains

☐ Include Nested Groups

Number of Items to Find: 5 (Maximum 1000)

Groups Found:

Name	Action
Development	Choose an Action
Marketing	Choose an Action
Operations	Choose an Action
Sales	Choose an Action

Document: Done

To Locate a Directory Object From the Items Tab

1. Enter the following search criteria:

   Search for. Use the drop-down list to indicate whether you’re searching for an organization, group, user, or mail list.

   Name. Enter the name of the directory object. Use the drop-down list to narrow your search criteria.

   Include Nested Organizations. If you want to search recursively through all suborganizations under the selected organization, select this option.

   Number of Items to Find. Enter the number of search results you want to see displayed. The default is 5, but you can enter a number up to 150.

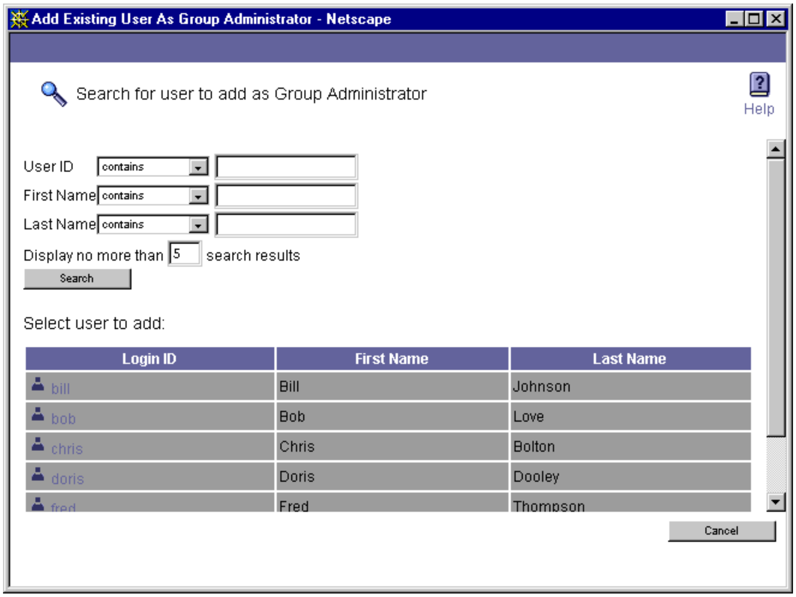
2. Once you locate a user, group, or organization in the results list, do one of the following:

   - Click the object’s name to view and edit its settings or properties.
   - Choose an action from the corresponding Action drop-down list.

To Locate a User Using a Search Window

A Search window is automatically displayed when you want to add an existing user to a group.

Figure 11-4 A Search window is invoked when adding an administrator to a group.



Search for user to add as Group Administrator

User ID contains

First Name contains

Last Name contains

Display no more than 5 search results

Select user to add:

Login ID	First Name	Last Name
bill	Bill	Johnson
bob	Bob	Love
chris	Chris	Bolton
doris	Doris	Dooley
fred	Fred	Thompson

1. Enter one or more of the following, using the drop-down lists to narrow your search criteria.

User ID. Enter the user's system user ID as assigned by a network administrator.

First Name. Enter the user's given name as it appears in official records.

Last name. Enter the user's surname as it appears in official records.

NOTE If you do not enter information in any of these fields, Delegated Administrator will generate a list of all user entries within the level, organization, or group you've selected. If there are more than 5000 users within this scope, the search could take a long time.

Display no more than. Enter the number of search results you want to see displayed. The default is 5, but you can enter a number up to 150.

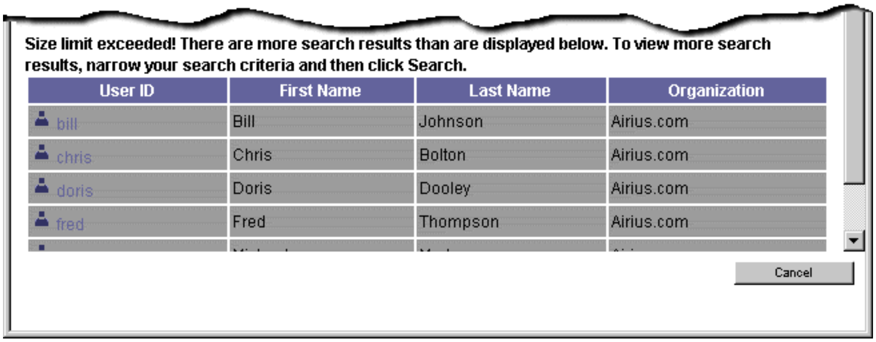
2. Click Search.

Delegated Administrator generates a list of users within your scope of responsibility that match the criteria you've specified.

Exceeding the Search Results Size Limit

If you see the message regarding size limit (see Figure 11-5), the search operation found more results than the number you specified above, and cannot display all the results. When this happens, you can either enter a greater number in the **Display no more than....** field above, or you can enter more specific search criteria and begin the search again

Figure 11-5 Size limit message.



Size limit exceeded! There are more search results than are displayed below. To view more search results, narrow your search criteria and then click Search.

User ID	First Name	Last Name	Organization
bill	Bill	Johnson	Airius.com
chris	Chris	Bolton	Airius.com
doris	Doris	Dooley	Airius.com
fred	Fred	Thompson	Airius.com

Managing Groups

As a Group administrator, you can create groups, subgroups, and user accounts.

Creating a New Group

Create a new group when you want to associate a number of users under one name. For example, in the Siroe company, all Sales employees are considered members of the Sales Department even though their user accounts might be stored in other parts of the organization. You can create a group within an organization; you can create a group within another group. You cannot create a new group at the top level of the Delegated Administrator tree.

Limiting the Number of Objects in an Group

You can limit the number of groups, or user accounts that may be included in the new groups. Limits are useful for two reasons. First, they optimize Delegated Administrator performance. Searches performed on groups with fewer users take less time to process.

Secondly, limits can help you comply with parameters set by your company. For example, the Siroe company's fee structure is based on the number of users in an group; groups with more than 5000 users are charged more for service than groups with fewer than 5000 users. When creating new groups, the Siroe administrator limits the number of users to 5000.

To Create a New Group

1. In the My Groups page, locate the group under which you'll create the new group, then click its name.
2. In the Group administration page, in the task bar, click New Group.
3. In the Create Group window, enter the following:

   Group name. Enter a name as you want it to appear in your company's official records. The name can include spaces and numbers.

   Nested group limit. Enter the maximum number of subgroups allowed in the group.

   User account limit. Enter the maximum number of user accounts allowed in the group.
4. Click OK.
5. In the Status window, click Continue.

To Edit Group Limits

1. In the My Groups page, locate the group you want to edit, and then click its name.
2. In the Group administration page, use the Search feature to generate a list of groups.
3. In the Search results, in the right pane, locate the group you want to edit, and then use its drop-down list to choose Edit.
4. Modify the following as necessary:

   Nested groups. Indicates the number of subgroups that currently exist under the group.

   Nested group limit. Enter the maximum number of subgroups allowed in the group.

   User accounts. Indicates the number of user accounts that currently exist under the group.

   User account limit. Enter the maximum number of user accounts allowed in the group.
5. Click Save.

Creating a Subgroup

When you create a group within another group, the new object is called a *subgroup*. Create a subgroup when you want to associate a number of users under one name.

1. Navigate to the administration page for the group in which the subgroup will be created.
2. In the Group administration page, in the task bar, click New Group.
3. In the Create Group window, enter the following:

   Group name. Enter a name as you want it to appear in your company's official records. The name can include spaces and numbers.

   Nested group limit. Enter the maximum number of subgroups allowed within the subgroup.

User account limit. Enter the maximum number of user accounts allowed in the subgroup.

4. Click OK.
5. In the Status window, click Continue.

Adding a User to a Group

Group administrators add users to groups in one of two ways: by adding a new user to the group, or by adding an existing user to a group. In addition to Group administrators, Top-level and Organization may add users to groups and it is possible for individual users to belong to more than one group.

To Add an Existing User to a Group

1. Navigate to Group administration page under which the group was created.
2. Use the Search feature to locate and select the group to which the user will belong.
3. In the Group administration page, in the task bar, click Add Existing User.
4. In the “Search for user to add as Group Member” window, locate and click the User ID of the user you want to add to the group.
5. Click OK.

To add a New User to a Group

1. Navigate to the Groupadministration page under which the group was created.
2. Use the Search feature to locate and select the group to which the new user will belong.
3. In the Group administration page, in the task bar, click New User.
4. In the New User window, click Basic Account Information. Skip to step 4 of To Create a New User Account in the section “Managing User Accounts.”

Adding Group Administrators

Add an existing user to the Group Administrators list if you want the user to be able to create new groups or modify the user accounts within a group. When you add a user to the Group Administrators list, you extend to that user all the access privileges accorded the group. Group Administrators, by default, can modify most information in the User Account Information window.

To Add a Group Administrator

1. In the Group administration page, under the Items tab, search for the group to which the new Group Administrator will belong.
2. In the Properties tab, click the Add button beside the list of Group Administrators.
3. In the Add Existing User window, use the Search feature to locate and select the user you want to add to the Group Administrators list.
4. In the UserID column, click the user you want to add to the Group Administrators list.
5. In the Status window, click Continue.

The user is added to the Group Administrators list, and now has all access privileges accorded this group. The administrator's User ID is displayed in the Organization Administrators list.

Removing Group Administrators

When you remove a member of the Group Administrators group, that user no longer has access privileges accorded to the group. The user's account is not deleted from the user directory.

To Remove a Group Administrator

1. In the Group administration page, under the Items tab, search for the group to which the Group Administrator belongs.
2. In the Properties tab, in the Group Administrators list, click the UserID of the administrator you want to remove.
3. Click the Remove button beside the Group Administrators list.
4. In the Status window, click Continue.

The user is removed from the Group Administrators list, and no longer has the access privileges accorded this group.

Removing a User from a Group

When you remove a user from a group, the individual's user ID is no longer associated with the group; the user entry remains in the directory. This is not the same as *deleting* a user account. When you delete a user account, the individual's entry is deleted from the user directory. (See Deleting a User Account.)

To Remove a User from a Group

1. Navigate to the Group administration page under which the group was created.
2. Use the Search feature to generate a list of groups within the organization.
3. In the Search results, in the right pane, locate the name of the user you want to remove, and then use its drop-down list to choose Remove.
4. When you see the confirmation message, click OK.

Deleting a Group

When you delete a group, its entry is deleted from the user directory.

To Delete a Group

1. Navigate to the Group administration page that manages the group.
2. Use the Search feature to generate a list of groups.
3. In the Search results, in the left pane, locate the group you want to delete, and then use its drop-down list to choose Delete.
4. When you see a confirmation message, click OK.

Managing User Accounts

As a Group administrator, you can create user accounts or add existing ones to the user directory.

Limited Access to Higher-level Administrators

Group administrators have limited access privileges to administrator entries that exist above them in the directory tree. For example, by default, the following administrators exist in the Delegated Administrator tree above Group administrators:

- Top-level Administrators
- Top-level Help Desk Administrators
- Organizational Administrators
- Organizational Help Desk Administrators.

Group administrators cannot modify attribute values in the entries for these users. Group administrators also cannot add these users to, or remove them from, their administrator groups.

Creating a New User Account

Create a new account when you want to add a user to the directory.

To Create a New User Account

1. Navigate to administration page for the group to which the user will belong.

2. In Group administration page task bar, click New User.

3. In the New User window, in the Basic Account Information pane, enter the following required information:

   Login ID. Enter the user's system user ID as assigned by a network administrator.

   First name. Enter the user's given name as it appears on official company records.

   Last name. Enter the user's surname as it appears in company records.

   Password. Enter the user's password.

   Confirm password. Enter the user's password again to confirm it.

   Organization. Enter the published name of the organization the user belongs to. Example: Sales Department.

   Title. Enter the user's job title as it appears on official company records. Example: Sales Associate.

   Manager. Enter the distinguished name (DN) of the user's manager. Example: `uid=doris, ou=People, o=Siroe, o=ISP`.

   Email address. Enter the user's email address. Example: ginac@siroe.com.

   Telephone number. Enter the user's phone number as it appears in company records. Example: 454-555-4444.

   Fax number. Enter the user's fax number as it appears in company records. Example: 454-555-4444.

   Mobile number. Enter the user's mobile or cell phone number as it appears in company records. Example: 454-555-4444.

   Pager number. Enter the user's pager number as it appears in company records. Example: 454-555-4444.

   Mailing address. Enter a street address where the user can receive print mail or packages. Example: 1234 Main Street, Anytown, AnyState.

   Web Page URL. Enter the URL for a web page that contains more information about the user. Example: http://www.siroe.com/sales/reps

Description. Enter a word or phrase that describes the web page above. Example: Sales Reps.

Preferred Language. Use the drop-down list to indicate the user’s preferred language. Delegated Administrator will display the user interface localized for the preferred language. For example, the Siroe company has employees in Japan, and they have indicated they prefer to conduct business in Japanese. When the Siroe administrator sets this preference to Japanese for a user, Delegated Administrator displays the Japanese version of the user interface.

4. If Class of Service is used, click it and enter the appropriate information.
5. If Basic Mail Information is displayed, click it and then enter the following information:

Mail host: Enter the Messaging Server host name. This is the machine hosting the Messaging Server that will process this user's mail. This must be the fully-qualified domain name (FQDN) known to the Messaging Server on that machine.

Alternative email addresses: An alternate address is essentially an alias for the user's primary address. You can use this feature to:

- Ensure proper delivery of frequently misspelled addresses (such as “Smith” as an alias for “Smithy”).
- Enable host name hiding in outgoing mail headers. To do so, supply an alternate address that includes the host name and do not include the host name in the primary email address (see step 3).
- You can specify any number of alternate addresses for a particular user, as long as each address is unique. Messages that arrive for any of these aliases are directed to the primary address.

Access domains: Lists the access domains from which the user can retrieve mail.

NOTE If no access domains are specified in the Access domain field, the user can retrieve mail from any domain.

To add an access domain:

a. Click Add (next to the Access domains field) to open the Set Domain window, and then enter either a regular domain name or an IP address. You must enter only one access domain each time you open the Access Domain name window. If you specify a domain that does not exist, or enter none, you effectively block access for the user.

b. Click OK.

Allow following service(s): To enable mail services for a specific type of server, select one or more of the available options: IMAP, POP, and HTTP. Netscape Messaging Server supports the Post Office Protocol 3 (POP3), the Internet Mail Access Protocol 4 (IMAP4), and the HyperText Transfer Protocol (HTTP) for client access to mailboxes. IMAP and POP are both Internet-standard mailbox protocols. Messenger Express, a web-enabled electronic mail program, lets end users access their mailboxes using a browser running on an Internet-connected computer system using HTTP.

Can Create E-mail Lists? This option applies only to Group administrators and individual users. All higher-level administrators, by default, have full mail list privileges regardless of whether this option is selected for them. When you select this option for a Group administrator or individual user, the Manage Mail Lists option is displayed when the individual edits his own account information.

6. If Mail Delivery Options is displayed, click it and then enter the following information:

Deliver incoming messages to:

POP3/IMAP4 mailbox. Select this option if you want to configure delivery and access to an individual user's POP or IMAP mailboxes.

Message store name. Enter the name (nickname, not pathname) of the message store partition to which the user's incoming mail should be delivered, if other than the current default primary partition. The name must represent an existing partition. For information on the message store and instructions for creating partition nicknames, see the *Messaging Server Administrator's Guide*.

Mailbox disk quota. Specify an allocated storage limit for this user. Enter a number in the field and select the appropriate unit (KB or MB). The disk quota or allocated storage limit you specify applies to this user alone.

Unix mailbox. Select this option if you want messages to be delivered to the user's designated Unix mailbox. Unix delivery is available only to users whose Messaging Server runs on a Unix host machine.

Process incoming messages through one or more programs:

By default, incoming messages are put in the inbox of the mail account the message is addressed to. Accounts can be configured to perform various operations with the messages it receives. Examples include putting incoming messages in particular mail folders, forwarding them somewhere else, or generating an automatic response. For detailed information, see Chapter 12, “Program Delivery” in *Netscape Messaging Server Administrator’s Guide*.

Enable the following programs: If you want to specify a mechanism for forwarding messages to an external application for processing before delivery to the user, select this option. Then enter the external application command(s) to be used for processing this user’s mail.

Forward a copy of each message to: Enter another address instead of or in addition to the primary address for the user. This enables mail to automatically be forwarded to the specified address.

7. Click OK.

To Edit a User Account

1. Navigate to the administration page of the group under which the user account was created.
2. Use the Search feature to generate a list of user accounts within the group.
3. In the Search results, in the right pane, locate the user ID of the account you want to modify, and then use the drop-down list to choose Edit.
4. Modify the user account information as necessary. See Creating a New User Account for detailed information about each of the fields in this window.
5. Click OK.

Deleting a User Account

Before you can delete a user account, you must navigate to the administration page for the group under which the user account was created. When you delete a user account, the individual’s entry is deleted from the user directory.

To Delete a User Account

1. Navigate to the administration page for the group under which the user account was created.

2. Use the Search feature to generate a list of users within the group.
3. In the Search results, in the right pane, locate the name of the user name for the account you want to delete, and then use its drop-down list to choose Delete.
4. When you see the confirmation message, click OK.

My Account

When an end user logs in using their his ID and password, an administration page for the individual's user account is usually displayed. When you log in, however, because you belong to an administrator group, an administration page is displayed. The My Account icon allows you play the role of an end user and modify your own user account information.

To Modify Information in Your Own User Account

1. Click My Account in the upper banner of the My Groups page or the Group administration page.
2. In the My Account window, click Account Information, and make changes as necessary:

   Login ID. Displays your system user ID as assigned by a network administrator.

   First name. Enter your given name as it appears on official company records.

   Last name. Enter your surname as it appears on official company records.

   Email addresses:

      Alternate Email Addresses. This field displays a list of your alternate email addresses, or aliases to the primary email address. Click Add to modify the information in this field. Then, in the Set Mail Address window, provide the following:

   - Enter an alternate address. This is essentially an alias for your primary address. For example, if a your primary address is `smythe@siore.com`, you can enter `smith@siroe.com` as an alternate address. This ensures that you will receive messages that are mistakenly addressed to "smith."

- You can specify any number of alternate addresses, as long as each address is unique. Messages that arrive for any of these aliases are directed to the primary address.

Access domains: Lists the access domains from which you can retrieve mail.

NOTE If no access domains are specified in the Access domain field, you can retrieve mail from any domain.

To add an access domain:

a. Click Add (next to the Access domains field) to open the Set Domain window, and then enter either a regular domain name or an IP address. You must enter only one access domain each time you open the Access Domain name window. If you specify a domain that does not exist, or enter none, you effectively block email access.

b. Click OK.

Quota. Enter a number to limit your own disk quotas. Disk quotas allow administrators to limit the amount of disk space allotted to each user. For detailed information, see Chapter 5, "Managing Messaging Store" in *Netscape Messaging Server Administrator's Guide*.

3. If Class of Service is used, click it to modify its settings.

4. To change your password, click Change Password, and then enter the following:

   Current Password. Enter the password you currently use to log into your network.

   New Password. Enter a password that is different from the current password.

   Retype New Password. Type the new password again to confirm it.

5. To modify telephone and mail information, click Personal Information and then modify the following as necessary:

   Telephone number. Enter your phone number as it appears in company records. Example: 454-555-4444.

   Fax number. Enter your fax number as it appears in company records. Example: 454-555-4444.

   Mobile number. Enter your mobile or cell phone number as it appears in company records. Example: 454-555-4444.

Pager number. Enter your pager number as it appears in company records. Example: 454-555-4444.

Mailing address. Enter a street address where you can receive print mail or packages. Example: 1234 Main Street, Anytown, AnyState.

Web Page URL. Enter the URL for a web page that contains more information about you. Example: http://www.siroe.com/sales/reps

Description. Enter a description for the web page that contains more information about you.

Preferred Language. Use the drop-down list to indicate your preferred language. Delegated Administrator will display the user interface localized for the preferred language. For example, the Siroe company has employees in Japan, and they have indicated they prefer to conduct business in Japanese. When the Siroe administrator sets this preference to Japanese for a user, Delegated Administrator displays the Japanese version of the user interface.

6. If Mail Delivery Options is displayed, click it and then modify the following information as necessary:

Deliver incoming messages to:

POP3/IMAP4 mailbox. To enable mail delivery to regular POP3 or IMAP4 mailboxes, select this option.

Unix mailbox. To allow messages to be delivered to a designated Unix mailbox, select this option. Unix delivery is available only to users whose Messaging Server runs on a Unix host machine.

Process incoming messages through one or more programs:

By default, incoming messages are put in the inbox of the mail account the message is addressed to. Accounts can be configured to perform various operations with the messages it receives. Examples include putting incoming messages in particular mail folders, forwarding them somewhere else, or generating an automatic response. For detailed information, see Chapter 12, “Program Delivery” in *Netscape Messaging Server Administrator’s Guide.*

Enable the following programs: If you want to specify a mechanism for forwarding messages to an external application for processing before delivery to you, select this option. Then enter the external application command(s) to be used for processing this user’s mail

Forward a copy of each message to: Enter another address instead of or in addition to your primary address. This enables mail to automatically be forwarded to the specified address.

7. If Vacation Auto-Responder Rule is displayed, enter the following:

   Auto-responder mode. Use the drop-down list to select one of the following:

   - **Off.** Disables auto-reply.
   - **Echo.** An automatic reply is sent for each received message and the received message appended as a MIME attachment to the reply. If you select this mode, you can enter a reply message in the Message field.
   - **Vacation.** The first message received by you from a given sender generates an automatic response; subsequent messages from that sender do not generate a response. If you select this mode, use the Vacation start/ end date options and enter a reply message in the Reply text field.
   - **Auto-reply.** Every incoming message received by you generates the specified automatic response. (The received message is not attached to the reply.) If you select this mode, you can enter a reply message in the Message field.

   If you selected vacation mode, supply dates and times to determine when the auto-reply message should start and end:

   - **Vacation Start Date**. If your vacation begins immediately, choose Now. If you want to specify a date, choose Date and then use the drop-down lists to indicate the date.
   - **Vacation Start Time**. Enter the start time using the 24-hour format.
   - **Vacation End Date**. If you don’t have a specific end date, choose Never. If you want to specify a date, choose Date and then use the drop-down lists to indicate the date.
   - **Vacation End Time.** Enter the end time using the 24-hour format.

   Message text. If you selected echo, vacation, or auto-reply mode, type a reply message to be returned to the sender. When the Vacation Auto-Responder is activated, Delegated Administrator will send the following default messages unless a specific text message is created:

   Echo mode:

   “This account has been configured to echo all mail, with no added text”

   Vacation:

   This person is currently on vacation.

   Auto-Reply:

This account has been configured to reply to all mail, with no text.

8. If Manage Mail Lists is not displayed, then skip to step 9. If Manage Mail Lists is displayed, skip to step 4 of To Create a New Mail List.

9. Click OK.

Mail Lists

Mail lists make it possible for a user to send the same message to a number of other users at one time. A mail list specifies the email addresses (users) that receive all messages sent to a single email address. For example, in the Siroe company, if you send one email to the address `sales@Siroe.com`, each employee in the Sales Department will receive the email.

NOTE You cannot use Delegated Administrator to manage mail lists unless Netscape Messaging Server 4.x is installed and properly configured. The following mail list features and functionality will not be available to you until a higher-level administrator enables them for you.

As a Group administrator, by default, you do not have sufficient privileges to create or manage mail lists. Those privileges must be granted to you by an Organization administrator.

Mail List Owners

A mail list may have one or more owners assigned to it. The owner can perform all operations on the mail list including creating new mail lists and assigning owners. The owner can edit the properties of any mail list that he or she owns. If the owner is a properly authorized administrator or user, he or she can create mail lists and assign owners to the lists.

Moderated Mail Lists

You can assign a moderator to filter messages sent to the mail list. This is useful in preventing unrelated messages from being distributed to members of the mail list. When you designate a moderator, the mail list is known as a *moderated lis*t. In a moderated mail list, all messages sent by members of the mail list are sent to the moderator. The moderator either approves or rejects the messages, and then sends only approved messages to all members of the mail list.

Managing Mail Lists

Group administrators and individual users can create and manage mail lists only if they are granted mail list privileges from an Organization administrator. Once a user is granted mail list privileges, the Manage Mail Lists option is displayed in their account information window.

To Create a New Mail List

1. In the top of the My Groups or Group administration page, click My Account.
2. In the My Account window, click Manage Mail Lists.
3. In the My Account Mail window, click Create Mail List.
4. In the New Mail List window, provide the following mail list information:

   Mail List Name. Enter a name that describes the mail list. Example: Sales

   Description. Enter a description of the purpose or nature of the mail list. You can use this field to enter a URL to an HTML page providing additional information about the mail list. This is for informational purposes only; the URL is not used by Messaging Server or by Delegated Administrator.

   Primary Email Address. Enter the publicized address to which mail for the mail list is sent. There can be only one primary address, which must be a valid, correctly formatted SMTP address conforming to RFC 821 specifications.

Alternate Email Addresses. This field displays a list of alternate email addresses, or aliases to the primary email address. Click Add to modify the information in this field. Then, in the Set Mail Address window, provide the following:

- Enter an alternate address. This is essentially an alias for the primary address. For example, if a primary address is `human resources@siore.com`, you can enter `hr@siroe.com` as an alternate address. This ensures that recipients will receive messages that are mistakenly addressed to "hr."
- You can specify any number of alternate addresses as long as each address is unique. Messages that arrive for any of these aliases are directed to the primary address.

Owners. To add an existing user to the Owners list, click the corresponding Add button. Then use the Search for User window to locate and select the user.

Members. To add a user to the mail list, click the corresponding Add button. Then use the Add Member window to locate and select the user.

Person for Bounced Messages. Use the search feature to locate and select the person, possibly a list owner or system administrator, to whom error messages should be sent when mail sent to the list can not be delivered.

Allow users to join. If you want to allow users to add themselves to the mail list, choose Yes. If you want to restrict users from adding themselves to the mail list, choose No.

Show Members of List To. If you want the owners and members of this list to be able to view the members' names, choose All. If you want no owners or members to be able to view members' names, choose None.

Hide Mail List. If you want to make a mail list visible to all users for subscription purposes, choose No. To make the mail list visible to only Organization Administrators, choose Yes.

Authorized Senders to List. Enter information regarding users, groups of users or specific domains that are allowed to post messages to the mail list:

> **Anyone.** Any user may contribute to the mail list.
>
> **Anyone in the mail list.** Only users included in the mail list may contribute to the mail list.
>
> **Anyone in the following list**. If you want to allow specific individuals or groups of individuals to be able to post messages to the mail list, click the associated radio button. Then specify the following:

Users and Groups. This fields displays the list of individual users and groups from which messages will be accepted for posting to this mail list. To Add a user or group to the list, click the corresponding Add button. If no user or group is specified, there is no sender-user restriction.

DNS Domains. This fields displays the list of domains from which messages will be accepted for posting to this mail list. To Add a domain name to the list, click the corresponding Add button. If no domain is specified, there is no sender-domain restriction.

When Message to this List is rejected:

Send message to Moderator(s). If you want to automatically forward rejected messages to the mailing-list moderator or moderators for further action, select this option. If you select this option, you must add at least one entry in the List moderators field. To add a user to the moderator list, click the corresponding Add button. Then use the Add Moderator window to locate and select a user.

5. Click OK.

To Edit a Mail List

1. Click My Account in the upper banner of your administration page.
2. In the My Account window, click Manage Mail Lists.
3. In the Manage Mail Lists window, click Owned Mail Lists.
4. Use the Search feature to generate a list of your mail lists.
5. In the Search results, locate the mail list you want to edit, and click its name.
6. In the Edit Mail List window, make changes as necessary, and then click OK.

To Subscribe to a Mail List

1. Click My Account in the upper banner of your administration page.
2. Use the Search feature to generate a list of mail lists in the organization.
   a. Select Subscribe to generate a list of mail lists that you currently subscribe to.
   b. Select Unsubscribe to generate a list of available mail lists that you can subscribe to.

3. In the Search results, locate the mail list you want to subscribe to, and then click Subscribe.
4. In the Subscribe Mail List window, click Subscribe.
5. In the Status window, click Continue.

To Unsubscribe from a Mail List

1. Click My Account in the upper banner of your administration page.
2. Use the Search feature to generate a list of mail lists in the organization.
    a. Select Subscribe to generate a list of mail lists that you currently subscribe to.

    b. Select Unsubscribe to generate a list of available mail lists that you can subscribe to.
3. In the Search results, locate the mail list you want to unsubscribe from, and then click Unsubscribe.
4. In the Unsubscribe Mail List window, click Unsubscribe.
5. In the Status window, click Continue.

To Delete a Mail List

1. In your administration page, use the Search feature to generate a list of Mail Lists.
2. In the Search results, in the right pane, locate the mail list you want to delete. In the drop-down list, choose Delete.
3. When you see a confirmation message, click Continue.

Chapter 12

End Users as Administrators

This document provides step-by-step instructions that an End User will need to modify his or her own account information. The topics included in this document are:

- Logging In
- Modifying User Account Information
- Mail Lists

Logging In

To Start Delegated Administrator and Log In:

1. Point a browser to the URL for the Delegated Administrator host. Example:

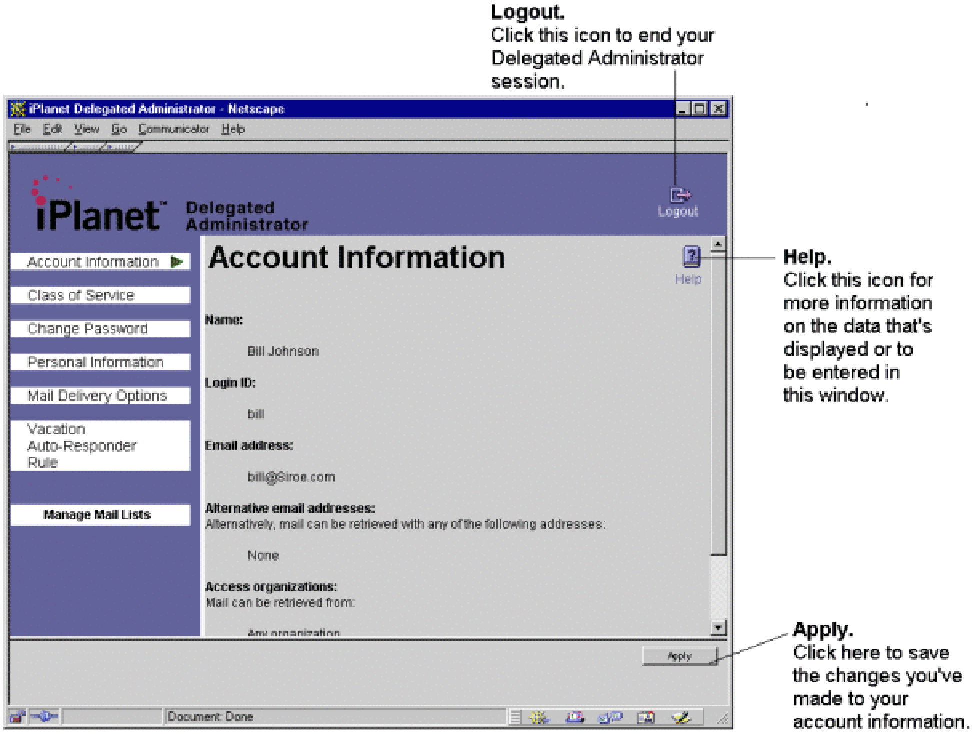
   `http://<host_name>:<port>/nda/default/en/login.html`

2. In the Login window, enter your system user ID and password.

3. Click Login.

   Delegated Administrator displays the your user account administration page. Figure 12-1 provides a quick tour of the page. By default, your Delegated Administrator session will time out after thirty minutes of inactivity.

Figure 12-1 The End-User Administration Page.



iPlanet Delegated Administrator - Netscape
File Edit View Go Communicator Help
iPlanet™ Delegated Administrator
Logout
Account Information
Class of Service
Change Password
Personal Information
Mail Delivery Options
Vacation Auto-Responder Rule
Manage Mail Lists
Help
Apply
Document: Done

Account Information

Name:

Bill Johnson

Login ID:

bill

Email address:

bill@Siroe.com

Alternative email addresses:
Alternatively, mail can be retrieved with any of the following addresses:

None

Access organizations:
Mail can be retrieved from:

Any organization

Logout. Click this icon to end your Delegated Administrator session.

Help. Click this icon for more information on the data that's displayed or to be entered in this window.

Apply. Click here to save the changes you've made to your account information.

To View Basic Information

Your basic user account information is entered by a system administrator, and you cannot modify it. Click Basic Information to view the following:

Login ID. Displays your system user ID as assigned by a network administrator.

First name. Enter your given name as it appears on official company records.

Last name. Enter your surname as it appears on official company records.

Email address: Displays your primary email address.

Mail host: Displays the name of the computer system from which receive email.

Alternate Email Addresses. Displays a list of your alternate email addresses, or aliases to the primary email address.

Access domains: Lists the access domains from which you can retrieve mail.

NOTE If no access domains are specified in the Access domain field, you can retrieve mail from any domain.

Quota. Displays your mail disk quota. Disk quotas allow administrators to limit the amount of disk space allotted to each user.

To View Class of Services

Class of Services determines which services are available to you. Your class of services is assigned by a system administrator, and you cannot modify it. Click Class of Service to view the services available to you.

Modifying User Account Information

You can modify your password, language preference, and mail delivery options. Depending upon the way your system administrator has set up your network, you may be able to modify other information about yourself such as your work phone numbers, mailing address, and individual web page URL.

To Change Your Password

1. Click Change Password, and then enter the following:

   Current Password. Enter the password you currently use to log into your network.

   New Password. Enter a password that is different from the current password.

   Retype New Password. Type the new password again to confirm it.

2. Click Apply.

To Modify Personal Information

1. Click Personal Information and then modify the following as necessary:

   Telephone number. Enter your phone number as it appears in company records. Example: 454-555-4444.

   Fax number. Enter your fax number as it appears in company records. Example: 454-555-4444.

   Mobile number. Enter your mobile or cell phone number as it appears in company records. Example: 454-555-4444.

   Pager number. Enter your pager number as it appears in company records. Example: 454-555-4444.

   Mailing address. Enter a street address where you can receive print mail or packages. Example: 1234 Main Street, Anytown, AnyState.

   Web Page URL. Enter the URL for a web page that contains more information about you. Example: http://www.siroe.com/sales/reps

   Description. Enter a description for the web page that contains more information about you.

   Preferred Language. Use the drop-down list to indicate your preferred language. Delegated Administrator will display the user interface localized for the preferred language. For example, the Siroe company has employees in Japan, and they have indicated they prefer to conduct business in Japanese. When the Siroe administrator sets this preference to Japanese for a user, Delegated Administrator displays the Japanese version of the user interface.

2. Click Apply.

NOTE If the following features are not displayed in your adminstration page, they may not be enabled or available to you. If you have questions regarding these features, contact your system administrator.

Mail Delivery Options

3. If Mail Delivery Options is displayed, click it and then modify the following information as necessary:

Deliver incoming messages to:

POP3/IMAP4 mailbox. To enable mail delivery to regular POP3 or IMAP4 mailboxes, select this option.

Unix mailbox. To allow messages to be delivered to a designated Unix mailbox, select this option. Unix delivery is available only to users whose Messaging Server runs on a Unix host machine.

Process incoming messages through one or more programs:

By default, incoming messages are put in the inbox of the mail account the message is addressed to. Accounts can be configured to perform various operations with the messages it receives. Examples include putting incoming messages in particular mail folders, forwarding them somewhere else, or generating an automatic response. For detailed information, contact your system administrator.

Enable the following programs: If you want to specify a mechanism for forwarding messages to an external application for processing before delivery to you, select this option. Then enter the external application command(s) to be used for processing this user's mail

Forward a copy of each message to: Enter another address instead of or in addition to your primary address. This enables mail to automatically be forwarded to the specified address.

Setting Vacation Auto-Responder Rules

Vacation Auto-Responder Rules make it possible for you to set up an automatic reply to messages you receive when you are not at work.

1. If Vacation Auto-Responder Rule is displayed, enter the following:

   Auto-responder mode. Use the drop-down list to select one of the following:

   ❍ **Off.** Disables auto-reply.

   ❍ **Echo.** An automatic reply is sent for each received message and the received message appended as a MIME attachment to the reply. If you select this mode, you can enter a reply message in the Message field.

   ❍ **Vacation.** The first message received by you from a given sender generates an automatic response; subsequent messages from that sender do not generate a response. If you select this mode, use the Vacation start/ end date options and enter a reply message in the Reply text field.

   ❍ **Auto-reply.** Every incoming message received by you generates the specified automatic response. (The received message is not attached to the reply.) If you select this mode, you can enter a reply message in the Message field.

   If you selected vacation mode, supply dates and times to determine when the auto-reply message should start and end:

   ❍ **Vacation Start Date**. If your vacation begins immediately, choose Now. If you want to specify a date, choose Date and then use the drop-down lists to indicate the date.

   ❍ **Vacation Start Time**. Enter the start time using the 24-hour format.

   ❍ **Vacation End Date**. If you don't have a specific end date, choose Never. If you want to specify a date, choose Date and then use the drop-down lists to indicate the date.

   ❍ **Vacation End Time.** Enter the end time using the 24-hour format.

   Message text. If you selected echo, vacation, or auto-reply mode, type a reply message to be returned to the sender. When the Vacation Auto-Responder is activated, Delegated Administrator will send the following default messages unless a specific text message is created:

   ```
   Echo mode:
   ```

   ```
   "This account has been configured to echo all mail, with no added
   text"
   ```

```
Vacation:

This person is currently on vacation.

Auto-Reply:

This account has been configured to reply to all mail, with no
text.
```

2. Click OK.

Mail Lists

Mail lists make it possible for you to send the same message to a number of other users at one time. A mail list specifies the email addresses (users) that receive all messages sent to a single email address. For example, in the Siroe company, if you send one email to the address `sales@Siroe.com`, each employee in the Sales Department will receive the email.

NOTE You cannot use Delegated Administrator to manage mail lists unless Netscape Messaging Server 4.x is installed and properly configured. The following mail list features and functionality will not be available to you until a higher-level administrator enables them for you.

Mail List Owners

A mail list may have one or more owners assigned to it. The owner can perform all operations on the mail list including creating new mail lists and assigning owners. The owner can edit the properties of any mail list that he or she owns. If the owner is a properly authorized administrator or user, he or she can create mail lists and assign owners to the lists.

Moderated Mail Lists

You can assign a moderator to filter messages sent to the mail list. This is useful in preventing unrelated messages from being distributed to members of the mail list. When you designate a moderator, the mail list is known as a *moderated lis*t. In a moderated mail list, all messages sent by members of the mail list are sent to the moderator. The moderator either approves or rejects the messages, and then sends only approved messages to all members of the mail list.

Managing Mail Lists

You can create and manage mail lists only if you are granted mail list privileges from a system dministrator. Once a user is granted mail list privileges, the Manage Mail Lists option is displayed in your account information window.

To Create a New Mail List

1. Click Manage Mail Lists.
2. In the My Account Mail window, click Create Mail List.
3. In the New Mail List window, provide the following mail list information:

   Mail List Name. Enter a name that describes the mail list. Example: Sales

   Description. Enter a description of the purpose or nature of the mail list. You can use this field to enter a URL to an HTML page providing additional information about the mail list. This is for informational purposes only; the URL is not used by Messaging Server or by Delegated Administrator.

   Primary Email Address. Enter the publicized address to which mail for the mail list is sent. There can be only one primary address, which must be a valid, correctly formatted SMTP address conforming to RFC 821 specifications.

   Alternate Email Addresses. This field displays a list of alternate email addresses, or aliases to the primary email address. Click Add to modify the information in this field. Then, in the Set Mail Address window, provide the following:

   - Enter an alternate address. This is essentially an alias for the primary address. For example, if a primary address is `human resources@siore.com`, you can enter `hr@siroe.com` as an alternate address. This ensures that recipients will receive messages that are mistakenly addressed to “hr.”
   - You can specify any number of alternate addresses as long as each address is unique. Messages that arrive for any of these aliases are directed to the primary address.

   Owners. To add an existing user to the Owners list, click the corresponding Add button. Then use the Search for User window to locate and select the user.

   Members. To add a user to the mail list, click the corresponding Add button. Then use the Add Member window to locate and select the user.

   Person for Bounced Messages. Use the search feature to locate and select the person, possibly a list owner or system administrator, to whom error messages should be sent when mail sent to the list can not be delivered.

Allow users to join. If you want to allow users to add themselves to the mail list, choose Yes. If you want to restrict users from adding themselves to the mail list, choose No.

Show Members of List To. If you want the owners and members of this list to be able to view the members' names, choose All. If you want no owners or members to be able to view members' names, choose None.

Hide Mail List. If you want to make a mail list visible to all users for subscription purposes, choose No. To make the mail list visible to only Organization Administrators, choose Yes.

Authorized Senders to List. Enter information regarding users, groups of users or specific domains that are allowed to post messages to the mail list:

> **Anyone.** Any user may contribute to the mail list.
>
> **Anyone in the Mail List.** Only users included in the mail list may contribute to the mail list.
>
> **Anyone in the following list**. If you want to allow specific individuals or groups of individuals to be able to post messages to the mail list, click the associated radio button. Then specify the following:
>
> > **Users and Groups.** This fields displays the list of individual users and groups from which messages will be accepted for posting to this mail list. To Add a user or group to the list, click the corresponding Add button. If no user or group is specified, there is no sender-user restriction.
> >
> > **DNS Domains.** This fields displays the list of domains from which messages will be accepted for posting to this mail list. To Add a domain name to the list, click the corresponding Add button. If no domain is specified, there is no sender-domain restriction.

When Message to this List is rejected:

> **Send message to Moderator(s).** If you want to automatically forward rejected messages to the mailing-list moderator or moderators for further action, select this option. If you select this option, you must add at least one entry in the List moderators field. To add a user to the moderator list, click the corresponding Add button. Then use the Add Moderator window to locate and select a user.

4. Click OK.

To Edit a Mail List

1. Click Manage Mail Lists.
2. In the Manage Mail Lists window, click Owned Mail Lists.
3. Use the Search feature to generate a list of your mail lists.
4. In the Search results, locate the mail list you want to edit, and click its name.
5. In the Edit Mail List window, make changes as necessary, and then click OK.

To Subscribe to a Mail List

1. Click Manage Mail Lists.
2. Click Subscriptions to Mail Lists.
3. Use the Search feature to generate a list of mail lists in the organization.
   a. Select Subscribe to generate a list of mail lists that you currently subscribe to.
   b. Select Unsubscribe to generate a list of available mail lists that you can subscribe to.
4. In the Search results, locate the mail list you want to subscribe to, and then click Subscribe.
5. In the Subscribe Mail List window, click Subscribe.
6. In the Status window, click Continue.

To Unsubscribe from a Mail List

1. Click Manage Mail Lists.
2. Click Subscriptions to Mail Lists.
3. Use the Search feature to generate a list of mail lists in the organization.
   a. Select Subscribe to generate a list of mail lists that you currently subscribe to.
   b. Select Unsubscribe to generate a list of available mail lists that you can subscribe to.
4. In the Search results, locate the mail list you want to unsubscribe from, and then click Unsubscribe.
5. In the Unsubscribe Mail List window, click Unsubscribe.

6. In the Status window, click Continue.

To Delete a Mail List

1. Click Manage Mail Lists.
2. Click Owned Mail Lists.
3. In the Search results, in the right pane, locate the mail list you want to delete. In the drop-down list, choose Delete.
4. When you see a confirmation message, click Continue.

Part 4

Customizing Delegated Administrator

Chapter 13

Customizing the User Interface

This chapter provides instructions for modifying the HTML pages that make up the Delegated Administrator user interface.

This chapter contains the following sections:

- HTML Templates
- Configuration Data
- NDAGetPage Servlet
- Customizing the Display of Search Results
- Customizing HTML Templates

HTML Templates

Delegated Administrator provides preconfigured *templates* from which its HTML user interface is generated. These templates are simply text files containing HTML with embedded *directives*. Each directive provides instructions about what HTML text or values to display, and how to display them.

The templates are stored in the following directory:

```
<delegatedadmin_root>/nda/nda/default/en/templates
```

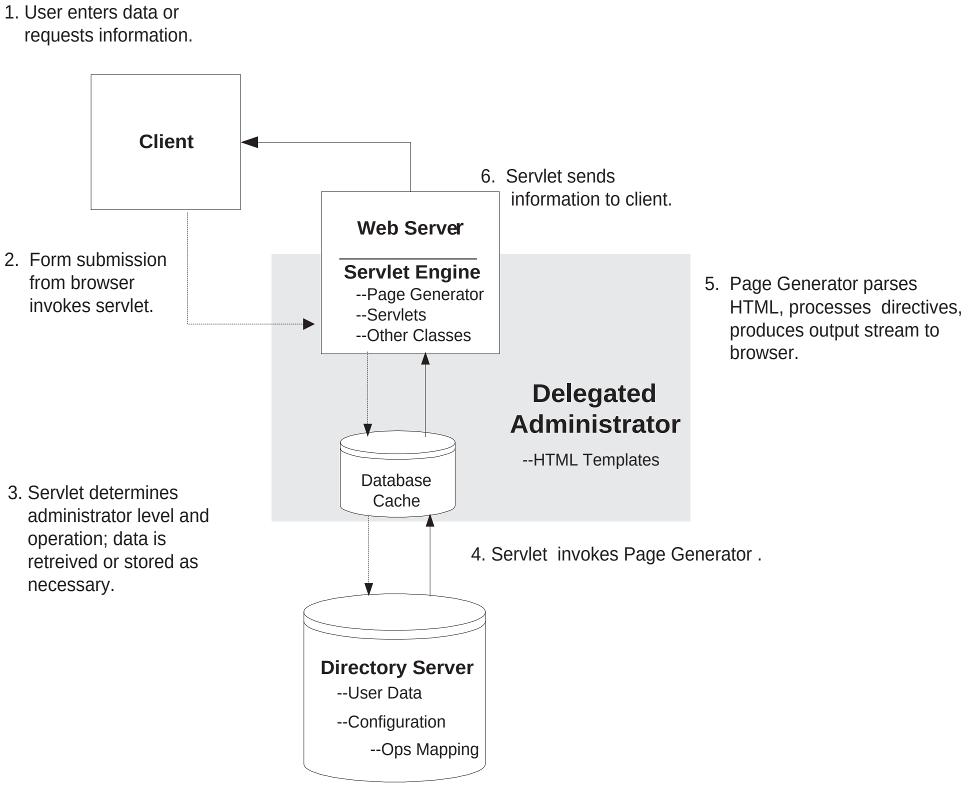
You can modify these templates to make changes in the Administrator Pages and their related dialogs. These are examples of page elements you can modify:

- Colors, images, and banners
- Onscreen text including field and control labels
- Data generated as a result of LDAP lookups

How the Templates Work

Delegated Administrator includes a Page Generator, a component that dynamically generates the HTML user interface based upon user-entered data and corresponding data in the Directory Server database. Each time an administrator invokes an operation from an HTML page, Page Generator parses directives embedded in a corresponding HTML template. The directives, along with data from the Directory Server, then dynamically generate the next appropriate HTML page.

Figure 13-1 Page Generator parses HTML with embedded directives.


1. User enters data or requests information.
Client
6. Servlet sends information to client.
Web Server
Servlet Engine
--Page Generator
--Servlets
--Other Classes
2. Form submission from browser invokes servlet.
5. Page Generator parses HTML, processes directives, produces output stream to browser.
Delegated Administrator
--HTML Templates
Database Cache
3. Servlet determines administrator level and operation; data is retreived or stored as necessary.
4. Servlet invokes Page Generator .
Directory Server
--User Data
--Configuration
--Ops Mapping

For example, when a Top-level Administrator logs in, he enters his user ID and password into the Login page, which invokes the `postLogin` operation. Page Generator parses the User ID and password together with directives embedded in the Login page, and maps the following:

```
[ postLogin + serviceadm ] -> templates/isp/index.html
```

Page Generator then displays the file `index.html` which is the Top-level Administrator page.

When an end user logs in, Page Generator maps the following:

```
[ postLogin + enduser ] -> templates/enduser/My-acct/index.html
```

In this case, Page Generator displays the file `enduser/My-acct/index.html`, which is the User Account page.

There is an HTML page associated with each Delegated Administrator operation. For each operation, there are mappings for each of the defined user types. You can customize Delegate Administrator by modifying its operations, directives, or HTML pages.

To change the user directory content, modify directives and organization configuration as explained in the rest of this chapter. To change the look and feel of the user interface, use standard HTML to modify the template files in the new organization directory. The new user interface will be displayed when a user logs in against the new organization.

Creating Templates for a New Organization

When you create a new organization, if you want to customize its templates (HTML pages), you must create a new directory for the templates. You must also create a new Start page and a new Login page for the organization.

By default, the Page Generator uses templates from the following directory:

```
<delegatedadmin_root >/nda/nda/default
```

Create a directory for the new organization under the Delegated Administrator root. You can give the directory any name. Page Generator will use the configuration and templates in this new organization directory.

To create a templates directory for a new organization:

1. Create a new directory at this location:

   `<delegatedadmin_root >/nda/nda`

2. Recursively copy the contents of the directory `<delegatedadmin_root >/nda/nda/default` to the new organization directory.

To create new Start and Login Pages

1. Copy these files to the directory where your organization files are stored:

   `<delegatedadmin_root>/nda/nda/start.htm`

   `<delegatedadmin_root>/nda/nda/login.htm`

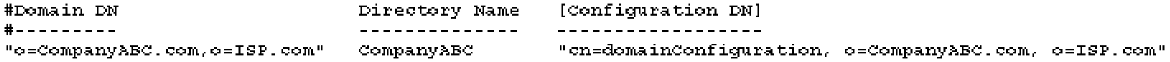
2. In the file `start.htm`, set the value of the form element `organization to` the dn component for the new organization. For example:

   ```
   var domain = "o=Airius.com";
   ```

3. In the file `login.htm`, modify the following line, replacing `o=Airius.com` with the base DN for the new organization:

   ```
   var domain = "o=Airius.com";
   ```

4. 4. In the file <delegatedadmin_root>/nda/nda/domain.map, create a new entry for the organization. For example, if the new organization is CompanyABC.com, and the templates are stored under <delegatedadmin_root>/nda/nda/ComapnyABC, then add the following entry:



```
#Domain DN                     Directory Name    [Configuration DN]
#---------                     --------------    ------------------
"o=CompanyABC.com,o=ISP.com"   CompanyABC        "cn=domainConfiguration, o=CompanyABC.com, o=ISP.com"
```

Configuration Data

The default configuration for a Delegated Administrator organization is stored in the Directory Server under the following DN:

```
cn=domainconfig, ou=configuration, o=<base suffix>
```

It includes information specific to the organization including: permissible users types; user type options; and search locations, filters, and scope.

The opconf area of the Directory Server stores information for mapping operations to template files. (For more information, see “Determining the Appropriate Template” on page 302.) The mainconf area of the Directory Server contains datatype identifiers and matchtype identifiers. The macrosconf area of the Directory Server contains Delegated Administrator macros.

Datatype Identifiers

The datatype identifier provides information about the supported types of data obtainable from the directory under the following DN:

cn=domainconfig, ou=configuration, o=<base suffix>

A datatype identifier is a category of one or more entries that are returned from the database as a result of a search that qualifies that datatype. For example, the datatype isp refers to the entry returned as a result of a search done on the directory tree with the basedn o=ISP, using a BASE scope with a filter objectclass=nsManagedISP.

```
dn: cn=isp, cn=datatypes, cn=mainconf, cn=en,
cn=domainConfiguration, ou=config, o=ISP
objectclass: top
objectclass: extensibleObject
cn: isp
iDAhandle: isp
iDAdisplayText: ISP
iDAbaseDN: $ISPDN$
iDAscope: BASE
iDAfilter: objectclass=nsManagedISP
```

Similarly, the datatype domainlist refers to the list of entries returned as a result of a search done on the directory tree with the base dn of o=ISP, with a SUBTREE scope and a filter objectclass=nsManagedDomain.

```
dn: cn=alldomains, cn=datatypes, cn=mainconf, cn=en,
cn=domainConfiguration, ou=config, o=ISP
objectclass: top
objectclass: extensibleObject
cn: alldomains
iDAhandle: alldomains
iDAdisplayText: All Domains
iDAbaseDN: $ISPDN$
iDAscope: SUBTREE
iDAfilter: objectclass=nsManagedDomain
```

Defining New Datatypes

You can define new datatypes that the templates can refer to. You can also allow the backend to automatically obtain information for extracting data from the directory. To do this, you must completely define the new datatype by providing values for the basedn, scope, and filter. The attribute list may be left out if you don't need it. This allows you to define new types of searches that can be invoked from the templates without any change to the servlets.

Internal Datatypes

You need internal datatypes only when you write your own servlets and need to preserve or list one or more entries across form submissions. If data is not committed into your database, while you are doing some preprocessing or composite operation on it across form invocations, you may need to define internal datatypes. This involves creating a new datatype in the `mainconf` area of the Directory Server. You must also provide the data for the internal datatype by registering it with the datatype name in the hash table of the `HttpSession` object. The Page Generator extracts the data from the HttpSession object and populates it into the HTML being generated from the template.

Matchtype Identifiers

Identifiers of matchtype associate the list-box text that the user selects in the List interface with a specified pattern.

Syntax

```
matchtype "<text>" "(<pattern>))"
```

Examples

```
matchtype "is" "(%a=%v))"

matchtype "is not" "(!(%a=%v)))"

matchtype "sounds like" "(%a~=%v))"

matchtype "starts with" "(%a=%v*))"

matchtype "ends with" "(%a=*%v))"

matchtype "contains" "(%a=*%v*))"
```

Macros

Macros define generic datatypes whose definitions do not need to specify organization or department names.

Macros are strings that occur in datatype definitions as literals enclosed within $ characters. A macro has the format `$<identifier>$`. The following macros are defined in the file `<delegatedadmin_root>/nda/nda/config/macro.ldif`:

Table 13-1 Delegated Administrator macros.

Macro	Description
`$AncestorDomainDNs$`	Keeps track of all ancestor domain DN values.
`$AncestorDeptDNs$`	Keeps track of all ancestor department DN values.
`$DomainDN$`	Keeps track of the current domain DN value.
`$DomainContainerDN$`	Keeps track of the current domain container DN value.
`$DeptDN$`	Keeps track of the current department DN value.
`$FamilyGroupDN$`	Keeps track of the current family group DN value.
`$MailListDN$`	Keeps track of the current mail list DN value.
`$AdmDeptDN$`	Keeps track of the current administrator group DN value.
`$UserDN$`	Keeps track of the current user DN value.
`$AuthDomainDN$`	Keeps track of the authenticated user’s domain DN value.
`$SelfDN$`	Keeps track of the authenticated user’s DN value.
`$SelfPasswd$`	Keeps track of the authenticated user’s password value.
`$ISPDN$`	Keeps track of the root node for the NDA installation.

Macros allow you to substitute context-related information into the generic datatype definitions. This makes the definition independent of the context. For example, if a user logs in as an organization administrator for AnyCompany.com, and the Delegated Administrator base suffix is o=ISP, the macro $ISPDN$ is set to o=ISP and $DOMAINDN$ to o=AnyCompany.com,o=ISP. For the Organization Administrator for AnyCompany.com, the datatype deptlist refers to the entries returned as a result of a search on the BaseDN $DOMAINDN$ which evaluates to a baseDN of o=AnyCompany.com,o=ISP.

Delegated Administrator sets the appropriate macros defined by each administrator role at login. Table 13-2 summarizes the macros that are defined when a user logs in.

Table 13-2 Macros used with each administrator role

Role	$ISPDN$	$DOMAINDN$	$DEPTDN$	$USERDN$	$SELFDN$
Top-level Administrator	✓				✓
Organization Administrator	✓	✓			✓
Group Administrator	✓	✓			✓
Top-level Help Desk Administrator	✓				✓
Organization Help Desk Administrator	✓	✓			✓
End User	✓	✓		✓	✓

If the corresponding macro name-value pair is passed as a parameter when a form is submitted to the servlet, then after the initial login, the NDAGetPage servlet sets further macros. The out-of-the-box forms pass these name-value pairs to the servlet as the context gets defined further. For example, upon logging in, a Top-level Administrator sees a list of organizations she has access to. Navigating to the organization level, the Top-level Administrator's context is specifically defined to the selected organization. Therefore, the form passes the name-value pair `DOMAINDN=o=AnyCompany.com,o=ISP` to the NDAGetPage servlet. The servlet then sets the value of the DOMAINDN macro for future reference.

NOTE The form should never pass a new value for a macro that had been defined at login. This would overwrite the original value and may lead to an inconsistent state.

Supported Directives

Directives are instructions written as Server Side Include commands that are interpreted by the Page Generator. Each directive begins on a new line and exists as a single independent line of HTML in the template file. A directive may have zero or more arguments.

Delegated Administrator 4.5 supports the following directives:

- S_ENTRYBEGIN
- S_ENTRYEND
- S_ATTRBEGIN
- S_ATTREND
- S_ATTRIBUTE
- S_ATTRIBUTE_MULTIVALUED
- S_SEARCH_PARAMS
- S_PROGRAM
- S_SESSION

Syntax

Each directive instructs the Page Generator about what replacement HTML text and values to display and how to display them. Each directive begins on a new line and exists as a single independent line of HTML in the template file. The directives have syntax similar to Server Side Includes, and they may have zero or more quoted arguments:

```
<!-- <directive>  "<arg1>=<value1>" "<arg2>=<value2>" ... -->
```

S_ENTRYBEGIN

This directive marks the start of a data group. A data group refers to the set of data (defined by a datatype) from which values will be retrieved and displayed. A data group can be a single LDAP entry or multiple LDAP entries in a search result. A data group is defined as a data type in Directory Server. For example, for the default configuration, you can find the datatype definitions for the Top-level suffix under the following entry:

```
dn: cn=isp, cn=datatypes, cn=mainconf, cn=en,
 cn=domainConfiguration, ou=config, o=ISP
```

The S_ENTRYBEGIN directive must always be paired with an S_ENTRYEND directive. There can be multiple S_ENTRYBEGIN and S_ENTRYEND blocks in a given HTML template. However, these S_ENTRYBEGIN and S_ENTRYEND blocks may not be nested.

In the case where this directive marks the start of a data group with multiple LDAP entries in a search result, the section within the S_ENTRYBEGIN and S_ENTRYEND block are iterated for each search result. This means that any text within the S_ENTRYBEGIN and S_ENTRYEND directives are repeatedly output, and all embedded directives are evaluated for each LDAP entry in the search result set.

Arguments

datatype=<dataType>	Specifies the data type as defined in main.conf
option=<value>[,<value2>]	Permitted values are listed in Table 13-3.

Table 13-3S_ENTRYBEGIN arguments

Option	Description
serversidesort	Indicates that results should be sorted on the server (This could cause a decrease in server performance.)
sizelimit	A non-negative number specifying how many entries to return from the search. If not specified, the sizelimit defaults to the defaultsizelimit set in the main.conf file. If set to 0, all entries from the search are returned without being subject to any limit.

Example

```
<!-- S_ENTRYBEGIN "datatype=usersinadmdeptlist" -->
```

S_ENTRYEND

This directive marks the end of an data group. Always paired with S_ENTRYBEGIN to end the block.

Arguments

None

S_ATTRBEGIN

This directive marks the start of a section for handling multivalued attributes.

The S_ATTRBEGIN directive must always be paired with an S_ATTREND directive. There can be multiple S_ATTBEGIN and S_ATTREND blocks in a given HTML template. However, these blocks may not be nested. An S_ATTRBEGIN...S_ATTREND block cannot appear within an S_ENTRYBEGIN...S_ENTRYEND block. An S_ENTRYBEGIN...S_ENTRYEND block cannot appear within an S_ATTRBEGIN...S_ATTREND block.

The section within the S_ATTRBEGIN and S_ATTREND block is iterated for each value of the attribute. This means that any text within the S_ATTRBEGIN and S_ATTREND directives are repeatedly output. All embedded directive are evaluated for each attribute value for the attr specified in the attr argument of this directive.

Arguments

datatype=<dataType>: specifies the data type as defined in the mainconf area of Directory Server.

`attr=<value>`: This refers to the multivalued attribute.

Example:

```
<!--S_ATTRBEGIN “datatype=self” “attr=ou”-->
```

S_ATTREND

This directive marks the end of a data group. Always paired with the S_ATTRBEGIN to end the block.

Arguments

None

S_ATTRIBUTE

The `S_ATTRIBUTE` directive is used for displaying or editing the contents of an attribute. It must always appear between the `S_ENTRYBEGIN` `S_ENTRYEND` block.

Arguments

`attr=<attribute name>`	Causes the corresponding attribute to be displayed. The special attribute ’dn’ is also recognized.
`datatype=<type of entry or list of entries>`	Specifies the data group that overrides the datatype value specified in the S_ENTRYBEGIN directive. If the attribute value is to be displayed from the same data type as specified in the S_ENTRYBEGIN directive, this argument is not required. However, in the case where an attribute value from a different data group needs to be displayed, this argument can be used to override the one specified in the S_ENTRYBEGIN directive.
`type = <how-to-display>`	Renders the attribute on-screen in a particular format. The allowed values are listed in Table 13-4
`option=<value>[,<value2>]`	Permitted values are listed in Table 13-5.
`defaultvalue=<default value>`	Specifies the given default value for the attribute if none is retrieved from the DS
`size=<number>`	Sets the width of the displayed attribute to number

Table 13-4S_ATTRIBUTE type values

Type	Display
text	Display as text
textarea	Show as an HTML TEXTAREA
radio	Show as a radio button
checkbox	Show as a checkbox
password	Show as an HTML password textbox
hidden	Set values in hidden form fields

Table 13-5S_ATTRIBUTE option values

Options	Permitted values
readonly	Indicates that this attribute should not be displayed as editable
quoted	Indicates that the attribute value should be quoted

S_ATTRIBUTE_MULTIVALUED

This directive is used to display multivalued attributes. it can also be used for single valued attributes. However, only text and textarea types are currently supported. This directive must appear between the S_ENTRY_BEGIN and S_ENTRY_END directives.

Arguments

`attr=<attribute name>` This refers to the attribute whose values need to be displayed.

`type=<text or textarea>` The type of form element to be output.

`mode=<single or multiple>` If mode is `single`, the multiple values are returned as a single string. The string is obtained by concatenating the values using the string specified by the separator as a delimiter. If mode is `multiple`, multiple form elements are generated. These form elements have the same name, but different values.

`separator=<separator string>` This string is used to separate multiple values if the mode is specified as `single`.

NOTE There are two ways to submit multi-valued attributes to the backend.

1. Use multiple form elements with the same name, but different values.
2. Submit a single string, with the multiple values separated by a separator string. This separator string can be specified by defining a hidden form element called `valueSeparator`. Its value is the string used for separating multiple values. The back end will then parse the single string and obtain the multiple values for the attribute.

S_SEARCH_PARAMS

This directive is used in conjunction with the S_ENTRYBEGIN directive for listing search results. This directive specifies the number of search results displayed per page (page size), as well as the attribute(s) to use to sort the search results. This directive must appear before the S_ENTRYBEGIN directive that marks the start of the search results listing.

Arguments

`sortattr=<attrlist>`	Specifies the attribute(s) to use to sort the search results. The colon character (:) can be used to specify sorting on more than one attribute.
`step=<page_size>`	Specifies the number of search results to display per page.

Example

```
<!-- S_SEARCH_PARAMS "step=5" "sortattr=uid" -->
```

S_PROGRAM

Provides a way of plugging in a custom class for augmenting page generation. At the point in the template where this directive occurs, a class by the name specified in the class parameter, which implements the iPageGenCustomModule interface, is instantiated and its execute() method invoked.

This is a useful tool since the PageGenerator can only generate output for a simple search. When the data needs to be obtained through composite searches, separate logic must be added to handle it. This directive provides a means to do that.

Arguments:

`lang=<language>`	Specifies the programming language in which the module is implemented.
`class=<class name>`	Specifies the class name to instantiate.

S_SESSION

This directive provides a means to display values of (Http)Session parameters. This is useful to display values that are not part of a user entry. An example of such usage is the display of the time string when a password is about to expire.

Arguments

`param`	Specifies the session parameter whose value needs to be output.

NDAGetPage Servlet

The `NDAGetPage` servlet offers a generic means for displaying the parsed results of a template. Since this servlet extends `NDAServlet`, it is capable of processing form submissions for HTTP methods `GET` and `POST`. While submitting name-value pairs to this servlet, you can specify the operation to be performed (thereby indicating which template should be parsed) via the `op` parameter. The `NDAGetPage` servlet also accepts parameters to be passed to the Page Generator for processing the form.

Determining the Appropriate Template

The op identifier associates operations and usertypes (Administrators) to corresponding template files. The op configuration information is stored in the Directory Server. The default configuration for the English locale can be found under
`cn=ops, cn=opconf, cn=en, cn=domainConfiguration, ou=config, <delgatedadmin_base_suffix>`.

Configuration information is organized by user types:

- Top-level administrator
- Organization Administrator
- Top-level Help Desk Administrator
- Organization Help Desk Administrator
- Group Administrator
- Enduser

The corresponding template files for each user type are located at the following location:
`<delegatedadmin_root>/nda/nda/default/en/templates`

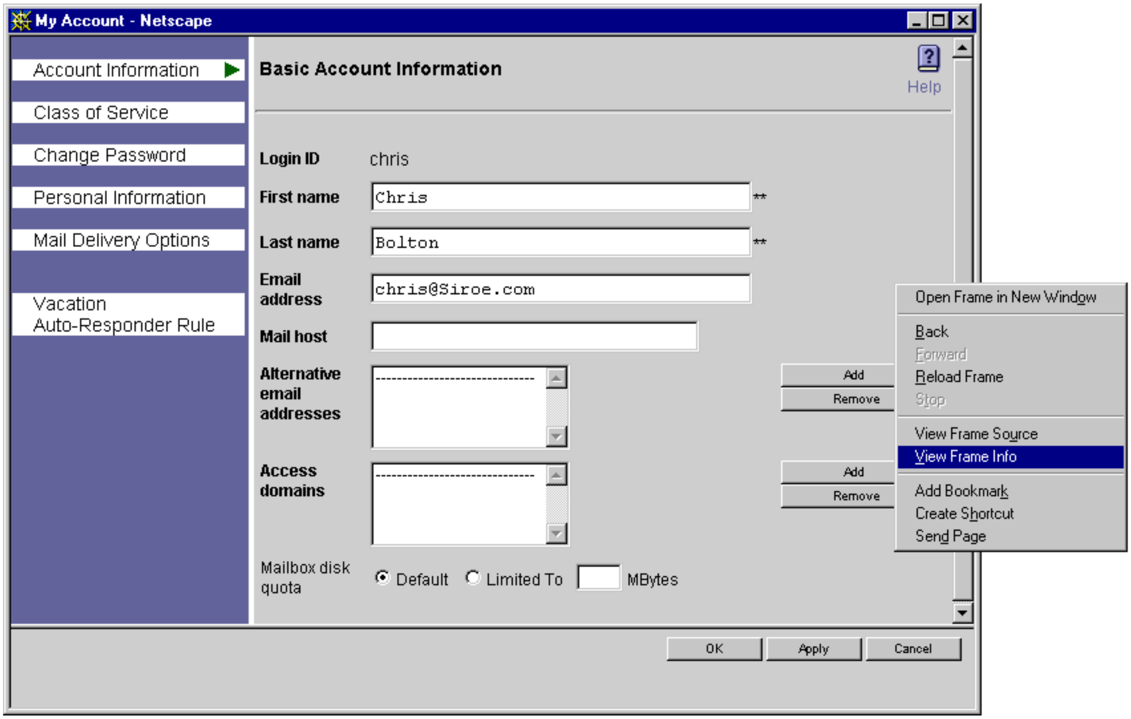
The following parameters determine the template to be parsed and the manner in which it is parsed:

`op=<opname>`	Specifies the value for the operation that will, along with the user type, be used to uniquely identify the template from which to generate the HTML output.
`mode=edit | display`	If `mode=edit`, the attribute values obtained from processing directives in the template will be displayed in a text field as editable. If `mode=display`, the value of the attribute will be displayed as is. The default, if this name-value pair is not specified, is to simply display the value.

For your convenience, Delegated Administrator ships with a file `op.ldif` that lists the default operation-to-template mappings. Use this file when you want to quickly determine which template is associated with a specific operation. For example, if you want to change a field name in the Items tab of the Group Administrator page, you can use the op.ldif file to determine which template you must modify.

To Determine Operation-to-Template Mapping

1. In the Administrator page or dialog box you want to modify, right-click and then choose View Frame Info from the browser menu. For example, to add a field under the Email Address field in the Basic Account Information page, place the cursor under the lable Email Address and right-click.



Basic Account Information

Login ID chris

First name Chris **

Last name Bolton **

Email address chris@Siroe.com

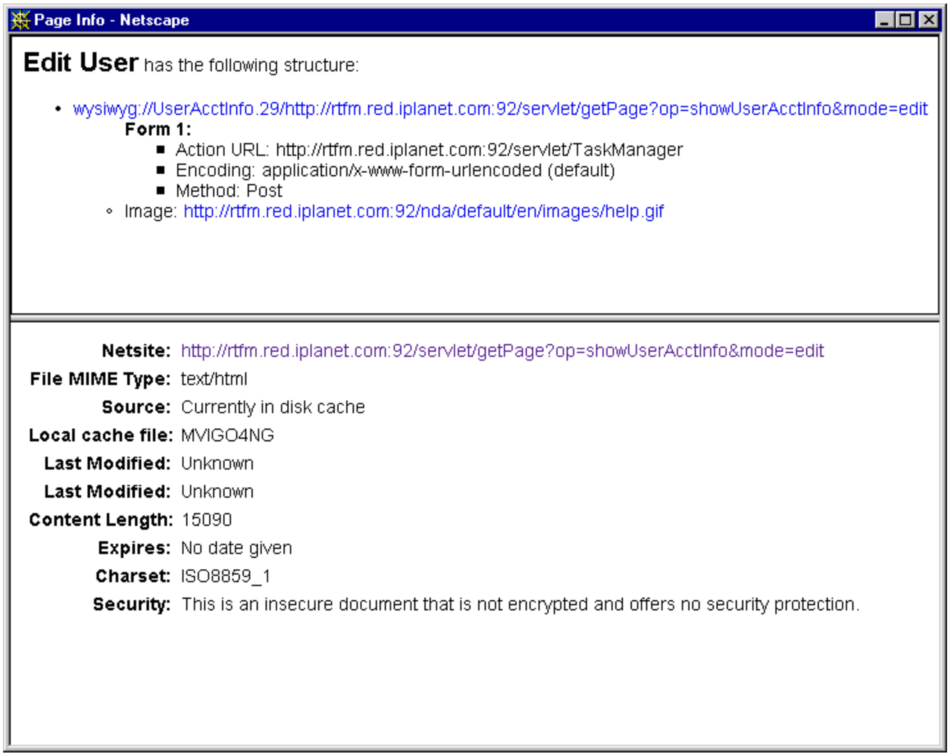
Mail host

Alternative email addresses

Access domains

Mailbox disk quota ● Default ○ Limited To MBytes

2. In the Page Info window, locate the op identifier. In the following example, the string op=ShowUserAcctInfo identifies the operation being performed..



Edit User has the following structure:

- wysiwyg://UserAcctInfo.29/http://rtfm.red.iplanet.com:92/servlet/getPage?op=showUserAcctInfo&mode=edit
  Form 1:
    - Action URL: http://rtfm.red.iplanet.com:92/servlet/TaskManager
    - Encoding: application/x-www-form-urlencoded (default)
    - Method: Post
  - Image: http://rtfm.red.iplanet.com:92/nda/default/en/images/help.gif

Netsite:	http://rtfm.red.iplanet.com:92/servlet/getPage?op=showUserAcctInfo&mode=edit
File MIME Type:	text/html
Source:	Currently in disk cache
Local cache file:	MVIGO4NG
Last Modified:	Unknown
Last Modified:	Unknown
Content Length:	15090
Expires:	No date given
Charset:	ISO8859_1
Security:	This is an insecure document that is not encrypted and offers no security protection.

3. Open the file op.ldif using the following path, where en is the English locale:

   `<delegated_admin_root>/nda/nda/default/en/op.ldif`

4. Search the op.ldif file for the operation you identified in Step 2. Both the operation and its associated template is included in the directory entry. In this example, the operation showUserAcctInfo is associated with the template HomePage.html.

```
dn: cn=showUserAcctInfo, cn=serviceadm, cn=ops, cn=opconf, cn=en,
cn=domainConfiguration, ou=config, o=Siroe
objectclass: top
objectclass: nsValueItem
cn: showUserAcctInfo
nsValueType: nsValueCIS
nsValueCIS: ../templates/enduser/My-acct/HomePage.html
```

Setting Macro Values

The following parameters, if passed to the servlet, make it set corresponding macro values in the session object. As with macros (See "Macros" on page 294), these values are useful for constructing search parameters for looking up datatypes in the directory:

`ispdn=<value of isp dn>`	The base DN, corresponding to the macro `$ISPDN$`.
`domaindn=<value of domain dn>`	The DN for the organization, corresponding to the macro `$DOMAINDN$`.
`deptdn=<value of department dn>`	The DN for the group, corresponding to the macro `$DEPTDN$`.
`admdeptdn=<value of the department of administrators>`	Identifies the user whose DN will be used, corresponding to the macro `$ADMDEPTDN$`. This parameter is useful when you want to set the value of the dn for a particular administrators department/group for subsequent use.
`userdn=<value of user dn>`	The DN for the user account, corresponding to the macro `$USERDN$`.
`selfdn=<value of self dn>`	The Dn for the user who logged in, corresponding to the macro `$SELFDN$`.

Searching a Datatype

The following parameters help pass in information for performing a search on a particular datatype:

`attrname`

`matchtype`

`matchstring`

They can be used in a single search clause, and in muliple search clauses.

Using a Single Search Clause

The following code is from the template file `<delegatedadmin_root>/nda/nda/default/en/templates/isp/DomDomSearchCriteria.html`. This section of the file generates the Search form in Figure 13-2:

```
<form name="searchForm" method="post" action="/servlet/getPage"
target="Right">
  <input type=hidden name="op" value="showDomDSResults">
  <input type=hidden name="attrname1" value="o">
  <input type=hidden name="searchdatatype" value="subdomains">
  <input type=hidden name="listrange" value="0-0">
<table width="100%" border="0" cellspacing="5" cellpadding="0">
  <tr>
    <td>
      <table border="0" cellspacing="5" cellpadding="0">
        <tr>
          <td colspan="4"><font face="PrimaSans BT, Verdana,
sans-serif" size="-1"><b>Search for
            <select name="searchType" onChange='handleTypeChange()'>
              <option selected>Organizations</option>
              <option>Groups</option>
              <option>Users</option>
              <option>Mail Lists</option>
            </select>
</b></font></td>
        <tr>
          <td colspan="4">&nbsp;</td>
        </tr>
        <tr>
          <td align="left"><font face="PrimaSans BT, Verdana,
sans-serif" size="-1">Name</font></td>
          <td align="left"><font face="PrimaSans BT, Verdana,
sans-serif" size="-1">
            <select name="matchtype1">
```

```
              <option selected>contains</option>

              <option>begins with</option>

              <option>ends with</option>

              <option>is</option>

         <option>doesn’t contain</option>

              <option>is not</option>

              <option>sounds like</option>

            </select>

          </font></td>

          <td align="left"><font face="PrimaSans BT, Verdana,
sans-serif" size="-1">

            <input type="text" name="matchstring1" size="16"
maxlength="32">

          </font></td>

        </tr>

        <tr>

          <td colspan="4"><font face="PrimaSans BT, Verdana,
sans-serif" size="-1">

            <input type="checkbox" name="nestedSearch"
onClick=’handleNestedSearch(this)’>

            Include Nested Organizations</font></td>

        </tr>

        <tr>

          <td colspan="4"><font face="PrimaSans BT, Verdana,
sans-serif" size="-1">Number of Items to Find:

            <input type="text" name="searchsizelimit" size="3"
maxlength="3" value=

<!-- S_ENTRYBEGIN "datatype=defaultlistsizetype" -->

<!-- S_ATTRIBUTE "attr=nsvaluecis" "type=text" "option=quoted" -->

<!-- S_ENTRYEND -->

>

            (Maximum

<!-- S_ENTRYBEGIN "datatype=maxlistsizetype" -->
<!-- S_ATTRIBUTE "attr=nsvaluecis" "type=text" "option=readonly" -->
<!-- S_ENTRYEND -->
)</font></td>
        </tr>
        <tr>
          <td colspan="4">&nbsp;</td>
        </tr>
        <tr>
          <td colspan="4"><font face="PrimaSans BT, Verdana, 
sans-serif" size="-1">
            <input type="button" name="actionButton" width="90" 
value="Search" onClick='handleSubmit()'>
            </font></td>
        </tr>
      </table>
    </td>
  </tr>
</table>
</form>
</body>
</html>
```

Arguments. The action field for the form is specified as `action="/servlet/getPage'`

`searchdatatype=<the datatype you are searching on>` This parameter corresponds to one of the types listed in the `mainconf` area of the Directory Server against the identifier datatype. It helps retrieve the search parameters like base suffix and filter for the specified datatype.

`attrname=<attribute name from directory>` Specifies the attribute name that will be used to construct the filter for the search. It is the top-level administrator's responsibility to ensure that the attribute specified here exists in one of the objectclasses that the returned entries belong to.

`matchtype=<a match type>` Indicates the type of match to be made. In the above example it was 'contains'. Any of the match types from the list of matchtypes specified in `mainconf` area of the Directory Server against the identifier matchtype can be substituted here. The string must match precisely that specified in `mainconf`.

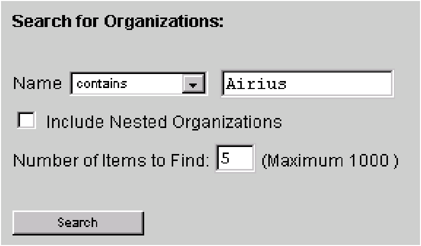
`matchstring=<search string entered by the user>` This is the value entered by the user in the form to specify the substring to search for. In the previous example in this section, you would enter `net` in this text field.

Although the servlet name is `NDAGetPage`, the name `getPage` is resolved by the servlet engine to `NDAGetPage` through the `servlets.properties` and `rule.properties` files in the Web Server.These are located in the following directory:

```
<webserver_root>/config
```

In these files, the class name corresponding to the alias is specified. The file may also contain other such aliases

Figure 13-2 Single search clause



Search for Organizations:

Name contains Airius

□ Include Nested Organizations

Number of Items to Find: 5 (Maximum 1000)

Once the user submits the information in the Search form, the following information is passed to the back end:

```
attrname: o

matchtype: contains

matchstring: Airius.
```

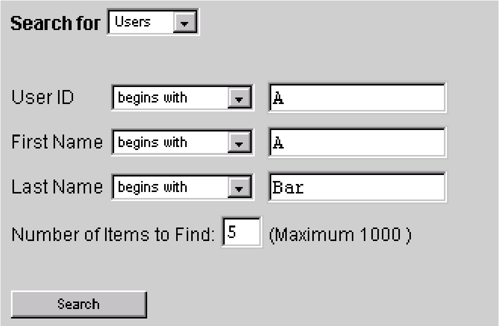
Using a Multiple Search Clause

The following is a section of the template file `<delegatedadmin_root>/nda/nda/default/en/templates/my-depts/DeptUserSearchSearchCriteria.html`. The file generates the form in Figure 13-3:

```
<form name="searchForm" method="post" action="/servlet/getPage"
target="Right">

  <input type=hidden name="op" value="showDeptUSResults">

  <input type=hidden name="attrname1" value="uid">

  <input type=hidden name="attrname2" value="givenname">

  <input type=hidden name="attrname3" value="sn">

  <input type=hidden name="searchdatatype" value="deptusers">

<table width="100%" border="0" cellspacing="5" cellpadding="0">

  <tr>

    <td>

      <table border="0" cellspacing="5" cellpadding="0">

        <tr>

          <td colspan="4"><font face="PrimaSans BT, Verdana,
sans-serif" size="-1"><b>Search for

            <select name="searchType" onChange='handleTypeChange()'>

              <option>Groups</option>

              <option selected>Users</option>

            </select>

</b></font></td>

        <tr>

          <td colspan="4">&nbsp;</td>

        </tr>

        <tr>
```

```
          <td align="left"><font face="PrimaSans BT, Verdana,
sans-serif" size="-1">User ID</font></td>

          <td align="left"><font face="PrimaSans BT, Verdana,
sans-serif" size="-1">

            <select name="matchtype1">

              <option selected>contains</option>

              <option>begins with</option>

              <option>ends with</option>

              <option>is</option>

         <option>doesn’t contain</option>

              <option>is not</option>

              <option>sounds like</option>

            </select>

          </font></td>

          <td align="left"><font face="PrimaSans BT, Verdana,
sans-serif" size="-1">

            <input type="text" name="matchstring1" size="16"
maxlength="32">

          </font></td>

        </tr>

        <tr>

          <td align="left"><font face="PrimaSans BT, Verdana,
sans-serif" size="-1">First Name</font></td>

          <td align="left"><font face="PrimaSans BT, Verdana,
sans-serif" size="-1">

            <select name="matchtype2">

              <option selected>contains</option>

              <option>begins with</option>

              <option>ends with</option>

              <option>is</option>

         <option>doesn’t contain</option>

              <option>is not</option>

              <option>sounds like</option>
            </select>
          </font></td>
          <td align="left"><font face="PrimaSans BT, Verdana,
sans-serif" size="-1">
            <input type="text" name="matchstring2" size="16"
maxlength="32">
          </font></td>
        </tr>
        <tr>
          <td align="left"><font face="PrimaSans BT, Verdana,
sans-serif" size="-1">Last Name</font></td>
          <td align="left"><font face="PrimaSans BT, Verdana,
sans-serif" size="-1">
            <select name="matchtype3">
              <option selected>contains</option>
              <option>begins with</option>
              <option>ends with</option>
              <option>is</option>
         <option>doesn’t contain</option>
              <option>is not</option>
              <option>sounds like</option>
            </select>
          </font></td>
          <td align="left"><font face="PrimaSans BT, Verdana,
sans-serif" size="-1">
            <input type="text" name="matchstring3" size="16"
maxlength="32">
          </font></td>
        </tr>
        <tr>
          <td colspan="4"><font face="PrimaSans BT, Verdana,
sans-serif" size="-1">Number of Items to Find:
            <input type="text" name="searchsizelimit" size="3"
maxlength="3" value=
<!-- S_ENTRYBEGIN "datatype=defaultlistsizetype" -->
<!-- S_ATTRIBUTE "attr=nsvaluecis" "type=text" "option=quoted" -->
<!-- S_ENTRYEND -->
>
            (Maximum
<!-- S_ENTRYBEGIN "datatype=maxlistsizetype" -->
<!-- S_ATTRIBUTE "attr=nsvaluecis" "type=text" "option=readonly" -->
<!-- S_ENTRYEND -->
)</font></td>
        </tr>
        <tr>
          <td colspan="4">&nbsp;</td>
        </tr>
        <tr>
          <td colspan="4"><font face="PrimaSans BT, Verdana,
sans-serif" size="-1">
            <input type="button" name="actionButton" width="90"
value="Search" onClick='handleSubmit()'>
            </font></td>
        </tr>
      </table>
    </td>
  </tr>
</table>
</form>
```

Figure 13-3 Multiple search clauses



Search for: Users

User ID: begins with — A

First Name: begins with — A

Last Name: begins with — Bar

Number of Items to Find: 5 (Maximum 1000)

Three sets of `attrname`, `matchtype` and `matchstring` are submitted. The following information is passed on to the back end as a result of the user's search:

```
attrname1: uid
matchtype1: begins with
matchstring1: A
attrname2: givenname
matchtype2: begins with
matchstring2: A
attrname3: sn
```

matchtype3: begins with

```
matchstring3: Bar
```

Customizing the Display of Search Results

You can customize the way in which search results are displayed. You can change the number of results displayed at a time, as well as specify the attribute upon which to sort the results.

Sorting on Multiple Attributes

The directive `S_SEARCH_PARAMS` is used to specify the attributes to sort on. You can specify multiple attributes to sort on by separating them with a colon. For example:

```
<!-- S_SEARCH_PARAMS "step=5" "sortattr=o:cn" -->
```

Results are listed in pages with five entries each, and sorted first on `o` and then on `cn`. You need to specify this directive before the `S_ENTRYBEGIN....S_ENTRYEND` block for this datatype in the template.

Customizing HTML Templates

The following are examples of the types of changes you can make to Delegated Administrator's HTML Templates.

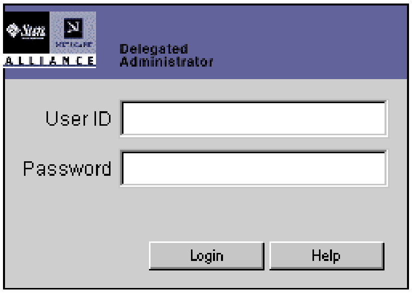
To Change the Banner or Logo on the Login Page

In the file `<ndaroot>/nda/nda/login.htm`, replace the links to `TopBannerLogo_trans.gif` and `iDAbanner_blueback.gif` with a link to a file containing your logo/banner.

In the following example, the graphic `iplanet.gif` was replaced with `sunnet.gif`.

```
<tr><td><a href="http://www.iplanet.com/" target="_top"><img
src="/nda/default/en/images/sunnet.gif" width="62" height="26"
border="0"><img
src="/nda/default/en/images/iDAbanner_blueback.gif" width="82"
height="26" border="0"></a></td></tr>
```

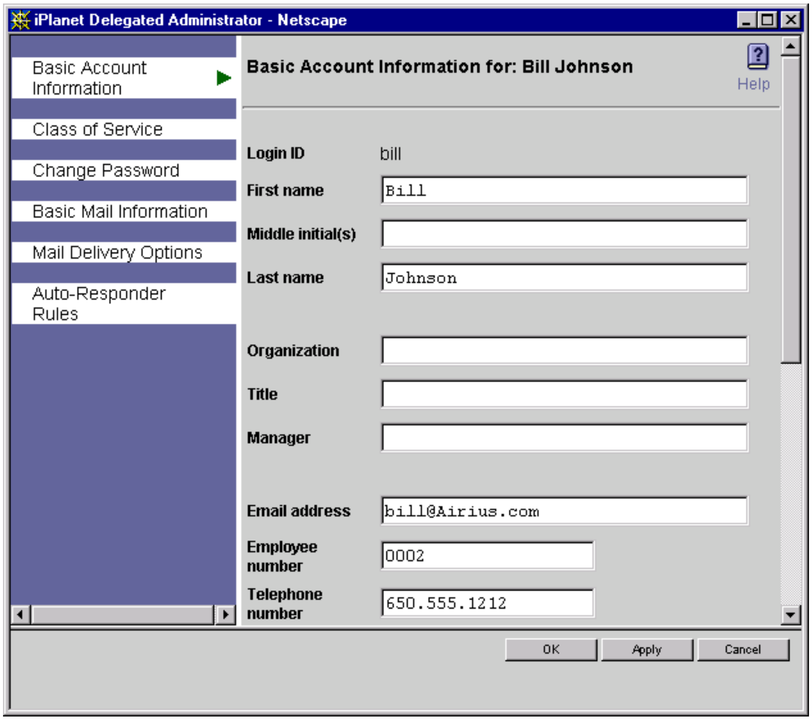
Figure 13-4 The iPlanet logo is replaced with the Sun-Netscape Alliance logo.



Adding a Field to an HTML Template

While the default Delegated Administrator templates may work well for many companies, you may want to add fields to your templates to expose additional types of information already stored in your user directory. For example, many companies assign an Employee Number when an individual is hired. For such companies, it's useful to include this number along with the user's name and userID in the Basic Information template. You can add a field to the New User and Edit User pages for entering this Employee Number.

Figure 13-5 The Employee Number field is added to the Basic Information window.



Basic Account Information for: Bill Johnson

Login ID	bill
First name	Bill
Middle initial(s)	
Last name	Johnson
Organization	
Title	
Manager	
Email address	bill@Airius.com
Employee number	0002
Telephone number	650.555.1212

To add a field to the New User and Edit User pages, use the attribute `employeeNumber` from `inetOrgPerson`. In this example, a field for Employee Number is added to the Basic Information window for a user account. The following files are modified:

- `<delegatedadmin_root>/nda/nda/default/en/templates/dialogs/CreateUserNavBar.html`
- `<delegatedadmin_root>/nda/nda/default/en/templates/dialogs/CreateUserBasic.html`
- `<delegatedadmin_root>/nda/nda/default/en/templates/dialogs/EditUserNavBar.html`
- `<delegatedadmin_root>/nda/nda/default/en/templates/dialogs/EditUserBasic.html`

When a new user entry is created, the administrator enters the user’s Employee Number. Delegated Administrator saves the user entry with this information.

To Add a Field for an Existing Attribute

1. In the file `CreateUserNavBar.html`, find the line containing `telephonenumber`.
2. Add a line just before this line and use `employeenumber` as the attribute name.

```
<!-- CreateUserBasic -->
      var createUserBasic = new Object();
      createUserBasic["uid"]="";
      createUserBasic["givenname"]="";
      createUserBasic["middleinitials"]="";
      createUserBasic["sn"]="";
      createUserBasic["cn"]="";
      createUserBasic["userpassword"]="";
      createUserBasic["confirm_userpassword"]="";
      createUserBasic["mail"]="";
      createUserBasic["employeenumber"]="";
      createUserBasic["telephonenumber"]="";
      createUserBasic["facsimiletelephonenumber"]="";
      createUserBasic["mobile"]="";
      createUserBasic["pager"]="";
      createUserBasic["o"]="";
      createUserBasic["title"]="";
      createUserBasic["manager"]="";
      createUserBasic["postaladdress"]="";
      createUserBasic["labeleduri"]="";
      createUserBasic["description"]="";
      createUserBasic["preferredlanguage"]="";
```

3. In the file `CreateUserBasic.html`, find the HTML code that outputs the `telephonenumber`. This is a table row and is delimited by the `<tr>`and `</tr>` HTML tags.
4. Insert a new table row, copying the one for `telephonenumber`, and replacing all occurrences of `telephonenumber` with `employeenumber`.
5. Insert a new table row, similar to the one for the `telephonenumber`, replacing all occurrences of `telephonenumber` with employeenumber"

```
 <tr>
      <td><b><font face="PrimaSans BT, Verdana, sans-serif"
size="-1">Employee
        number</font></b></td>
      <td>
        <input type="text" name="add_employeenumber" size="20"
onChange="handleValueChange(’employeenumber’);" value="">
      </td>
    </tr>
    <tr>
      <td><b><font face="PrimaSans BT, Verdana, sans-serif"
size="-1">Telephone
        number</font></b></td>
      <td>
        <input type="text" name="add_telephonenumber" size="20"
onChange="handleValueChange(’telephonenumber’);" value="">
      </td>
    </tr>
    <tr
```

6. In the file `EditUserNavBar.html`, locate two lines that contain the attribute `telephonenumber`. Insert two similar lines for the attribute `employeenumber`.

   The `<!-- S_ATTRIBUTE -->` directive is processed by the Page Generator, and will result in the substitution of the attribute value from the user entry

```
<!-- S_ATTRIBUTE “attr=o” “type=text” “option=readonly,quoted” -->
 editUserBasicOrig[“employeenumber”]=
<!-- S_ATTRIBUTE “attr=employeenumber” “type=text”
“option=readonly,quoted” -->
      editUserBasicOrig[“title”]=
      editUserBasicOrig[“telephonenumber”]=
<!-- S_ATTRIBUTE “attr=telephonenumber” “type=text”
“option=readonly,quoted” -->
      editUserBasicOrig[“title”]=
```

7. In the file EditUserBasic.html, insert a row for `employeenumber`.

Adding a JPEG Image to a Template

Companies sometimes include a digital image of each employee with the individual's basic account information. The image might captured for the employee's badge, and simply stored in the directory. Or it might be made available through a company phonebook for identification purposes.

Before you can add a JPEG image to a template, you must enable JPEG support in Diretory Server, and add the image to the user's entry.

To Enable JPEG Image Support in the Directory Server

1. In the Directory Server Console, click Directory, then click the Delegated Administrator base suffix.
2. Click Domain, and then click Users.
3. Select a user, and then right click on the user's name.
4. Open the properties Editor. Editor Entry dialog is displayed
5. In the Editor Entry dialog, click Advanced. Property Editor dialog is displayed
6. In the Property Editor dialog box, from the Edit menu, choose Add Attribute.
7. From Add Attribute Window select JPEG photo. Make sure Property JPEG image is added.
8. Click Replace in Property jpeg image. Choose the JPEG file you want to add.
9. Click OK and save it.

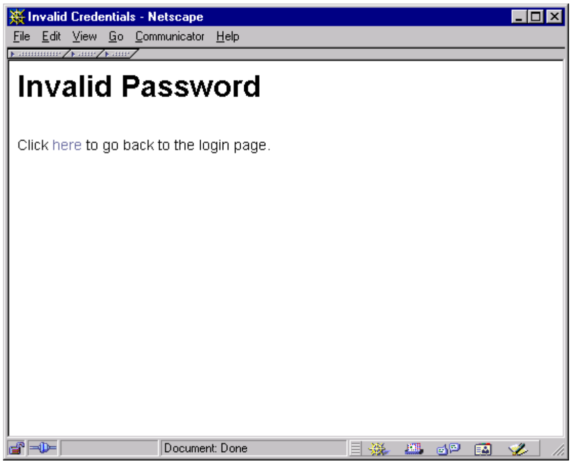
Changing an Error Message

In this example, the standard "Invalid Credentials" error message—usually displayed when a user enters the wrong password in the Login page—is changed to "Invalid Password."

1. In the file `<delegatedadmin_root>/nda/classes/netscape/nda/servlet/resource.properties`, find the resource strings that begin with `Page-invalidCredentialsMsg`.
2. Change the error message by making the appropriate changes to the HTML code that is output.
3. Be sure to set the `MsgLength` to the correct value. The Page Generator will use this length to read the lines of HTML code to output.

```
Page-invalidCredentialsMsgContentType=text/html

Page-invalidCredentialsMsgLength=6

Page-invalidCredentialsMsg0=<html><head><meta
http-equiv="Content-Type" content="text/html;
charset=iso-8859-1">

Page-invalidCredentialsMsg1=<title>Invalid
Password</title></head>

Page-invalidCredentialsMsg2=<body bgcolor="#FFFFFF"
link="#666699" vlink="#666699" alink="#333399">

Page-invalidCredentialsMsg3=<h1>Invalid Password</h1>

Page-invalidCredentialsMsg4=<br>Click <a
href="javascript:window.history.back()">here</a> to go back to
the login page.

Page-invalidCredentialsMsg5=</body></html>
```

Figure 13-6 “Invalid Credentials” messages is changed to “Invalid Password.”



Invalid Credentials - Netscape
File Edit View Go Communicator Help

Invalid Password

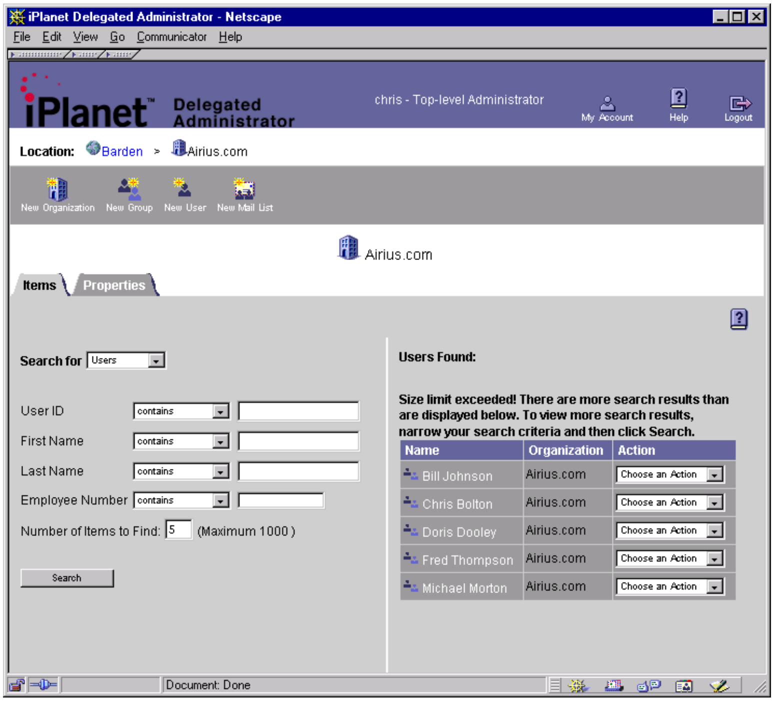
Click here to go back to the login page.

Changing Search Criteria

You can modify the search criteria used when searching users in the directory. In this example, the Employee Number is substituted for Organization in the types of search criteria displayed in the Top-level Administrator page.

1. In the file `<delegatedadmin_root>/nda/nda/default/en/templates/isp/DomUserSearchCriteria.html`, find the form element named `attrname4`.
2. Change the value of this form element from `nsdadomain` to `employeenumber`.
3. Find the section of the HTML code that outputs the table row for the `Last Name`. The next row outputs the criteria for `Organization`. Change this to output `Employee Number`.

Figure 13-7 In the Search interface, the Employee Number field takes the place of the Organization field.


iPlanet Delegated Administrator - Netscape
File Edit View Go Communicator Help
iPlanet™ Delegated Administrator
chris - Top-level Administrator
My Account
Help
Logout
New Organization
New Group
New User
New Mail List
Items
Properties
Search
Document: Done

Location: Barden > Airius.com

Airius.com

Search for: Users

User ID	contains	
First Name	contains	
Last Name	contains	
Employee Number	contains	

Number of Items to Find: 5 (Maximum 1000)

Users Found:

Size limit exceeded! There are more search results than are displayed below. To view more search results, narrow your search criteria and then click Search.

Name	Organization	Action
Bill Johnson	Airius.com	Choose an Action
Chris Bolton	Airius.com	Choose an Action
Doris Dooley	Airius.com	Choose an Action
Fred Thompson	Airius.com	Choose an Action
Michael Morton	Airius.com	Choose an Action

Chapter 14

Customizing Configuration in the Directory

Delegated Administrator uses iPlanet Directory Server to store the configuration information which controls the user experience. If no customized configuration information is available for an organization, Delegated Administrator uses default configuration information. Delegated Administrator enables you to customize the user experience based on your organization. Within an organization, the user experience can be further customized on a per-language basis. When you customize Delegated Administrator in these ways, you must modify the configuration information in the directory.

This chapter includes the following topics:

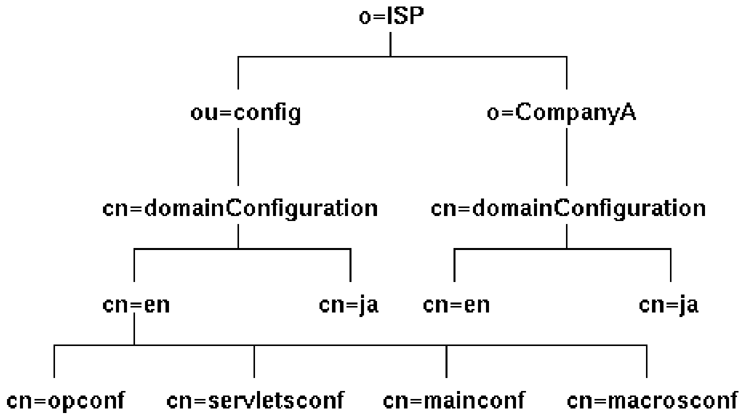
- Default Configuration Information
- Customizing Configuration Information
- Configuration Management Utilities

Default Configuration Information

The default configuration information is loaded into the Directory server during its installation. The Top-level entry for the configuration information subtree is:

```
cn=domainConfiguration, ou=config, o=ISP
```

Figure 14-1 The Default Configuration Information Tree



As shown in Figure 14-1, the default configuration tree stores information in subtrees on a per-language basis. When a user logs in, the configuration information corresponding to the user's preferred language (specified via the `preferredLanguage` attribute in the user's entry, or the browser language preference) is used. When an administrator creates a customized configuration for an organization, by default, the configuration information tree is stored under the organization entry. Figure 1 illustrates a customized configuration information tree stored for the organization represented by `o=CompanyA, o=ISP`.

The examples in this chapter are for the English language locale. Configuration information for other locales would be located under their corresponding entries. For example, configuration information entries for the Japanese locale would have a `cn=jn` component instead of `cn=en` in their distinguished names (DNs).

The configuration information is categorized into four major areas and stored under the following relative distinguished names (RDNs):

- `cn=mainconf`
- `cn=servletsconf`
- `cn=opconf`
- `cn=macrosconf`

cn=mainconf

In Figure 2, this section of the subtree contains configuration entries that specify miscellaneous configuration parameters that control the Delegated Administrator behavior when it performs searches (such as the time limit and size limit for searches) as well as the datatypes used in conjunction with the Page Generator. Each datatype defines the search parameters, including the search base, the search scope and the search filter. For example, the following entry defines the search parameters for the datatype `allsubdomains`:

```
dn: cn=allsubdomains, cn=datatypes, cn=mainconf, cn=en,
cn=domainConfiguration,ou=config, o=ISP
objectclass: top
objectclass: extensibleObject
cn: allsubdomains
iDAhandle: allsubdomains
iDAdisplayText: All Nested Domains
iDAbaseDN: $DOMAINDN$
iDAscope: SUBTREE
iDAfilter: objectclass=nsManagedDomain
```

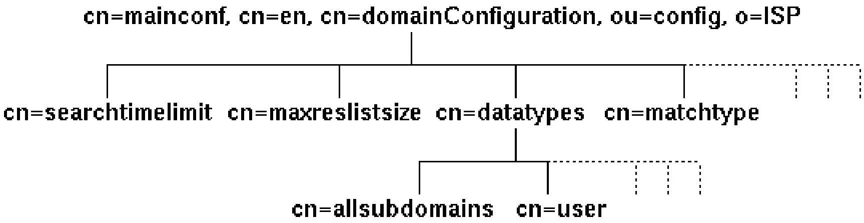
The above entry specifies that the search for the datatype `allsubdomains` is a subtree search starting from the base DN `$DOMAINDN$.` (This base DN is expanded at run time to the appropriate DN.) The search filter used is `objectclass=nsManagedDomain`.

A Delegated Administrator HTML file may contain a directive of the form:

```
<!-- S_ENTRYBEGIN "datatype=allsubdomains" "option=excludebase" -->
```

When the Page Generator encounters this directive, it performs a search for the datatype `allsubdomains` and uses the above entry to define various search parameters. The `excludebase` option instructs the Page Generator to exclude the base DN itself from the result set, if the base itself satisfies the search criteria. For more information about the Page Generator, see "How the Templates Work" on page 288.

Figure 14-2 cn=mainconf



cn=servletsconf

This section of the configuration information tree (see Figure 3) controls the Delegated Administrator behavior when creating new objects. When an administrator creates a new object, such as a new user or a new organization, Delegated Administrator will populate the entry with certain objectclasses and attributes that are defined by the corresponding object definition entry. For example, the following entry controls the creation of new user objects:

```
dn: cn=User, cn=objects, cn=servletsconf, cn=en,
cn=domainConfiguration, ou=config, o=ISP
objectclass: top
objectclass: extensibleObject
cn: User
iDAobjectclass: top
iDAobjectClass: person
iDAobjectClass: organizationalPerson
iDAobjectClass: inetOrgPerson
iDAobjectClass: mailRecipient
iDAobjectClass: nsMessagingServerUser
iDAobjectClass: nsManagedPerson
iDArequiredAttribute: cn
iDArequiredAttribute: sn
iDArequiredAttribute: uid
iDArequiredAttribute: userPassword
```

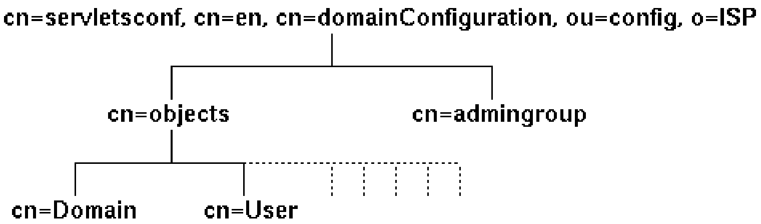
```
dn: cn=User, cn=objects, cn=servletsconf, cn=en,
cn=domainConfiguration, ou=config, o=ISP
iDAattribute: nsdadomain $DomainContainerName$
iDAattribute: owner $ThisDeptAdminGroupDN$
iDArdnAttribute: uid
iDAdataTypeIdent: enduser
iDAsearchFilter: objectClass=nsManagedPerson
iDAparentDN: “ou=People, $DomainContainerDN$”
iDAcnComposition: $givenname$ $sn$
```

The above entry specifies that the new user entry will have the following objectclasses:

- `top`
- `person`
- `organizationalPerson`
- `inetOrgPerson`
- `mailRecipient`
- `nsMessagingServerUser`
- `nsManagedPerson`

The RDN attribute for the user entry will be `uid`. It also specifies the various required attributes that will be populated by Delegated Administrator. Furthermore, the location where this new user entry will be created and how the `cn` attribute will be composed are also specified by this configuration entry.

Figure 14-3 cn=servletsconf


cn=servletsconf, cn=en, cn=domainConfiguration, ou=config, o=ISP
cn=objects
cn=admingroup
cn=Domain
cn=User

cn=opconf

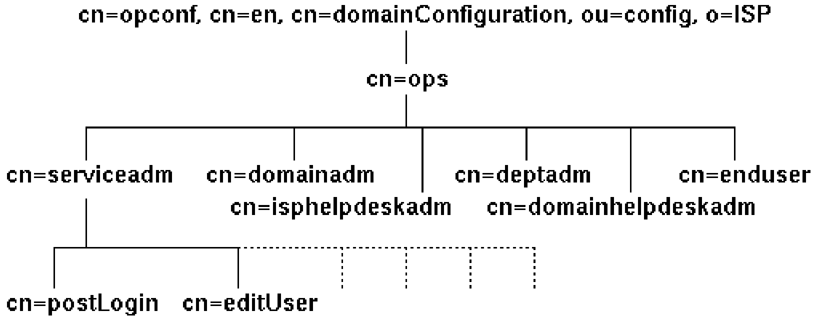
This section of the configuration information tree defines the mapping from an operation to a template which is an HTML file. The `NDAGetPage` servlet works in conjunction with the Page Generator to create a graphical user interface (GUI) page. The NDAGetPage servlet is invoked with an operation (`op`) as a parameter. Delegated Administrator determines the corresponding template (HTML file) based on the type of user such as Top Level Administrator, End User, and so on.

Figure 4 illustrates how these configuration entries are organized based on the type of user. For each user type, entries are defined for each operation. For example, when the Top Level Administrator clicks on the link to edit a user entry, the NDAGetPage servlet is invoked with `editUser` as the operation. The HTML file that is displayed in response to this operation is controlled by the following entry:

```
dn: cn=editUser, cn=serviceadm, cn=ops, cn=opconf, cn=en,
cn=domainConfiguration, ou=config, o=ISP
objectclass: top
objectclass: nsValueItem
cn: editUser
nsValueType: nsValueCIS
nsValueCIS: ../templates/dialogs/EditUserFrame.html
```

The above entry specifies that the HTML template to use is `../templates/dialogs/EditUserFrame.html`

Figure 14-4 cn=opconf



cn=macrosconf

The Page Generator uses macros for dynamically substituting context-specific information. As in the example above for the datatype `allsubdomains`, the macro `$DOMAINDN$` will be substituted with a specific DN when an administrator is navigating through the organization hierarchy.

Customizing Configuration Information

Customizing configuration information involves modifying the configuration information entries. When you modify these entries, it helps to have a working knowledge of the following:

- Customizing the default configuration
- Customizing configuration for an organization
- The `domain.map` file
- The Lookup algorithm

Customizing the Default Configuration

To customize the default configuration information, you need to modify the configuration information entries that control Delegated Administrator behavior when no custom configuration information is available for a specific organization. For example, to change the time limit when a search times out, you can modify the following entry:

```
dn: cn=searchtimelimit, cn=mainconf, cn=en,
cn=domainConfiguration, ou=config, o=ISP
objectclass:top
objectclass: nsValueItem
cn: searchtimelimit
nsValueType: nsValueCIS
nsValueCIS: 10
nsValueDescription: Default server side timeout value for a
search
```

You can increase the time limit to 30 seconds by modifying the `nsValueCIS` attribute in the above entry to 30. Similarly, you can customize any of the entries in the `cn=opconf` section to change the templates that are used in response to operation requests. You can change the datatype definitions to modify the search criteria, or add new datatypes of your own by defining the search base DN, the search scope and the search filter.

Any change made to the default configuration information will affect all the organizations that do not define their own configuration information.

Customizing Configuration for an Organization

If you have a separate configuration information tree for a particular organization, then you can make changes to the entries for this organization's configuration tree. For example, changes made to the configuration tree for companyA (Figure 14-1) will only affect users who belong to companyA. To create a new configuration information tree for an organization, refer to the section on Configuration Management Utilities.

The domain.map File

The domain.map file can be used to specify the location where the configuration information tree for an organization can be found. By default, Delegated Administrator will look for this information directly under the entry for this organization. For example, in Figure 14-1, Delegated Administrator will attempt to locate the configuration information for companyA under the following base DN:

```
dn: cn=domainConfiguration, o=companyA, o=ISP
```

If the configuration information tree is located elsewhere, you can use the domain.map file to specify this location. This file is located in the <DelegatedAdmin_root>/nda/nda directory. If the configuration information is located under the base DN cn=domainConfiguration,cn=someplaceelse,o=ISP, you can specify the following line (use a single line) in the domain.map file:

```
o=companyA,o=ISP companyA
cn=domainConfiguration,cn=someplaceelse,o=ISP
```

The first element specifies the organization to which this directive is applicable. The second element tells Delegated Administrator where it can find customized templates (HTML files) for this organization. The last element tells it where the configuration information tree is located.

The Lookup Algorithm

The Delegated Administrator attempts to locate the configuration information tree for an organization in the following order:

1. If the domain.map file specifies the location for the configuration information, Delegated Administrator uses the information stored in the subtree at that location.
2. If there is no entry in the domain.map file, Delegated Administrator attempts to locate the configuration information in the default location (cn=domainConfiguration) below the entry for the organization.
3. If Delegated Administrator cannot locate the configuration information after steps 1 and 2 above, it uses the default configuration information

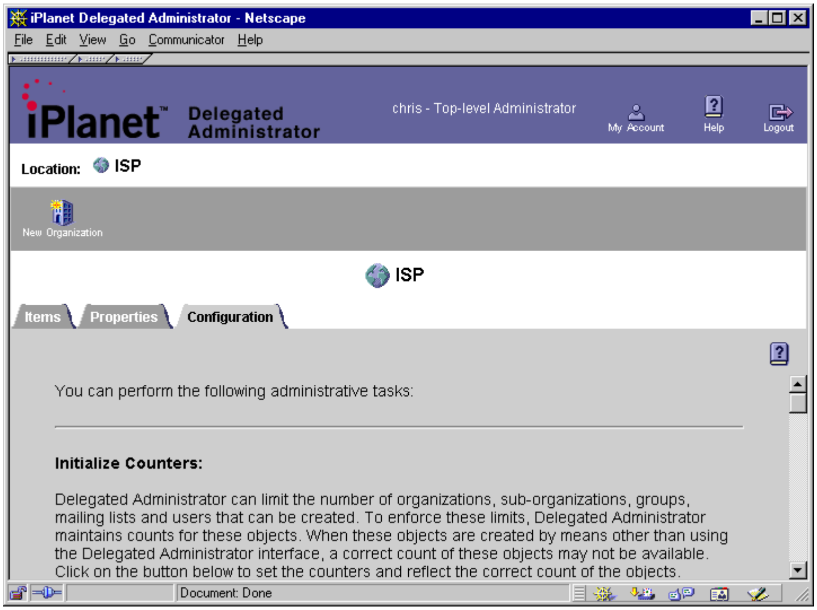
   (cn=domainConfiguration,ou=config,o=ISP).

Configuration Management Utilities

To facilitate the process of customizing configuration information for an organization, Delegated Administrator provides two basic configuration management utilities. These are available to the Top-level Administrator and the Organization Administrator under the Configuration Tab.

Using the Configuration Management Tab

Top-level Administrators and Organization Administrators can use the Configuration Tab to manage certain basic configuration related tasks.


iPlanet Delegated Administrator - Netscape
File Edit View Go Communicator Help
iPlanet Delegated Administrator
chris - Top-level Administrator
My Account
Help
Logout
Location: ISP
New Organization
ISP
Items
Properties
Configuration
Document: Done

You can perform the following administrative tasks:

Initialize Counters:

Delegated Administrator can limit the number of organizations, sub-organizations, groups, mailing lists and users that can be created. To enforce these limits, Delegated Administrator maintains counts for these objects. When these objects are created by means other than using the Delegated Administrator interface, a correct count of these objects may not be available. Click on the button below to set the counters and reflect the correct count of the objects.

Reloading Configuration

Delegated Administrator reads and caches the configuration information at start-up (when a Delegated Administrator servlet is invoked for the first time after a web server start or restart). Ordinarily, any changes to the configuration information tree will be effective only after the web server is restarted.

You can, however, force Delegated Administrator to reload the configuration information by using the Configuration Tab.

Copying Configuration

You can begin the process of creating customized configuration information for an organization by first copying the default configuration information (or configuration information from another organization). The Configuration Tab aids you in this process by creating the necessary entries and ACIs for Delegated Administrator to function correctly. Once you have a copy of the configuration information tree, you can then modify various entries to provide the desired customized behavior.

Using Directory Server Console and Command-Line Utilities

To modify the configuration information, you can use the Directory Server Console or command line utilities such as `ldapmodify`. For more information see, the *iPlanet Directory Server Administrator's Guide*.

Chapter 15

Extending Servlets

A servlet is a server-side program that gives Java-enabled servers additional features. This chapter describes how iPlanet Delegated Administrator 4.5 uses servlets and tells you how to extend the capabilities of those servlets to meet the needs of your enterprise. It assumes a basic knowledge of Java servlet programming.

The chapter contains the following sections:

- iPlanet Delegated Administrator 4.5 Servlets
- Accessing the Session Object
- Accessing the TaskData Object
- Extending Authentication and Logout Servlets
- Extending Task Servlets
- Compiling and Packaging Your Java Classes

In addition to the information contained in this chapter, full documentation (in javadocs) for the public iPlanet Delegated Administrator 4.5 Java classes is available at `http://docs.iplanet.com/docs/manuals/deladmin/45/utility_scripts`.

iPlanet Delegated Administrator 4.5 Servlets

iPlanet Delegated Administrator 4.5 functionality is defined by Java class files called servlets. These servlets control how users are authenticated, how HTML pages are generated and displayed, and how tasks (such as creating users or groups) are executed. You can extend and customize some servlets to meet the specific needs of your enterprise.

This section describes the architecture of Delegated Administrator's servlets, lists the elements of iPlanet Delegated Administrator 4.5 that you can extend and customize, and explains the basics of extending and customizing servlets. The rest of this chapter covers the details of servlet customization.

Servlet Architecture

Most iPlanet Delegated Administrator 4.5 servlets fall into one of four categories: authentication, logout, task, or page generation. The differences between these categories are as follows:

- When users or administrators log in to iPlanet Delegated Administrator 4.5, authentication servlets look them up in the user directory, confirm their identity, and then determine what level of access they have to the directory.
- When users or administrators log out of iPlanet Delegated Administrator 4.5, a logout servlet closes their connections, and performs any other logout procedures.
- When users or administrators perform operations, such as creating groups or deleting mailing lists, task servlets carry out the backend actions.
- When users or administrators click buttons or links, page-generation servlets dynamically determine what pages should appear based on access level and task results and then pass the HTML code for those pages to the Web Server.

iPlanet Delegated Administrator 4.5 servlets inherit their basic functionality from a class called `NDAServlet`. Two special servlets manage task and page generation operations: `NDATaskManager` and `NDAGetPage`. `NDATaskManager` determines which task servlets handle which operation requests. `NDAGetPage` handles all page generation requests.

NDAServlet

The `NDAServlet` class is the foundation of all iPlanet Delegated Administrator 4.5 servlets. It inherits its functionality from a core Java class called `HTTPServlet`. `NDAServlet` implements `doGet` and `doPost` as `final` methods. The `doGet` method calls the `doPost` method that, in turn, invokes the following three methods:

- `preprocess`
- `execute`
- `postprocess`

Any classes that extend `NDAServlet` must implement the `execute` method. In addition, these classes may also implement the `preprocess` and `postprocess` methods.

preprocess

The `preprocess` method is a hook for adding a preprocessing function to an existing servlet in iPlanet Delegated Administrator 4.5. It has the following syntax:

```
protected void preprocess(javax.servlet.http.HttpSession s,
                     javax.servlet.http.HttpServletRequest req,
                     javax.servlet.http.HttpServletResponse res)
throws javax.servlet.ServletException, java.io.IOException
```

The `preprocess` method takes the following parameters:

- `s`, which is the `HttpSession` object from the servlet engine
- `req`, which is the `HttpServletRequest` object from the servlet engine
- `res`, which is the `HttpServletResponse` object from the servlet engine

execute

`execute` is the primary method for servlets that extend `NDAServlet.` All servlets in iPlanet Delegated Administrator 4.5 must implement this method. The `execute` method has the following syntax:

```
protected abstract void execute(javax.servlet.http.HttpSession s,
                      javax.servlet.http.HttpServletRequest req,
                      javax.servlet.http.HttpServletResponse res)
throws javax.servlet.ServletException, java.io.IOException
```

The `execute` method takes the following parameters:

- `s`, which is the `HttpSession` object from the servlet engine
- `req`, which is the `HttpServletRequest` object from the servlet engine
- `res`, which is the `HttpServletResponse` object from the servlet engine

postprocess

The postprocess method is a hook for adding a postprocessing function to an existing servlet in iPlanet Delegated Administrator 4.5. It has the following syntax:

```
protected void postprocess(javax.servlet.http.HttpSession s,
                     javax.servlet.http.HttpServletRequest req,
                      javax.servlet.http.HttpServletResponse res)
throws javax.servlet.ServletException, java.io.IOException
```

The postprocess method takes the following parameters:

- s, which is the HttpSession object from the servlet engine
- req, which is the HttpServletRequest object from the servlet engine
- res, which is the HttpServletResponse object from the servlet engine

NDATaskManager

When a user or administrator performs a task using iPlanet Delegated Administrator 4.5's HTML forms, a hidden tag containing the name of the task is passed to NDATaskManager. When NDATaskManager receives this request, it opens a file called resource.properties, looks up the name of the class that corresponds to the task name (from the hidden tag), executes the task by running the class, and then returns information about the result to the user.

Each class that contains a task must contain a method called doIt that defines the actions required to complete the task. The doIt method has the following syntax:

```
public void doIt(TaskData td)
throws java.lang.Exception
```

The doIt method takes the following parameter:

- td - the task input data

For more information on the relationships between NDATaskManager, resource.properties, and task classes, see “Extending Task Servlets,” which begins on page 351.”

NDAGetPage

When a user or administrator clicks a link or selects an option that leads to another screen, a hidden tag containing the name of the page generation operation is passed to NDAGetPage. When NDAGetPage receives this request, it looks up the operation name in the configuration directory, and then dynamically generates the page that the user or administrator sees. For more information on NDAGetPage, “NDAGetPage Servlet” on page 302.

The Session Object

Often, servlets require information about a user’s iPlanet Delegated Administrator 4.5 session in order to execute properly. For instance, a servlet that modifies a user’s personal information must know the user’s distinguished name (DN) in order to make changes in the user directory. To make it easy to obtain this kind of information, Delegated Administrator uses a Session object. The Session object is a collection of name-value pairs that contain user DNs, Lightweight Directory Access Protocol (LDAP) connection values, and other session information.

For more information on Delegated Administrator’s session object, see “Accessing the Session Object,” which begins on page 342.”

Servlets and iPlanet Web Server

In order to make servlets easy to manage and use, iPlanet Web Server uses two properties files. The first file, called rules.properties, maps paths (such as /servlet/TaskManager) to simple names (such as TaskManager). The second file, servlets.properties, maps simple names to actual servlet classes and, if necessary, can include initial arguments and class path information.

By default, iPlanet Delegated Administrator 4.5 creates an iPlanet Web Server document root called /servlets. This document root maps to /nda/classes, the subdirectory of your server root containing the JAR files in which Delegated Administrator’s servlets are stored.

What You Can Customize

Although you can extend or customize almost any iPlanet Delegated Administrator 4.5 servlet, the code for some servlets is quite complex and involved. The following are the most typically customized types of servlets:

- Authentication servlets
- Task servlets for the creation, modification, and deletion of directory entries
- Logout servlets

Authentication and logout servlets are discussed in “Extending Authentication and Logout Servlets,” which begins on page 347.”

Task servlets are discussed in “Extending Task Servlets,” beginning on page 351.”

Accessing the Session Object

The iPlanet Delegated Administrator 4.5 `Session` object contains information about a user or administrator’s interactions with Delegated Administrator. Servlets can use the information in this object to analyze data or to determine what operations to perform. For instance, a servlet that logs a user out of Delegated Administrator may check the `Session` object to determine when the user first logged in, and then record the total length of time that the user spent within the application. Another servlet might accept a user’s request to change his or her password, and then check the `Session` object to obtain the user’s DN.

Methods and Keys

In order to access the contents of the `Session` object, you use two methods, `getAttribute` and `setAttribute`. The `getAttribute` method is used to retrieve data from the `Session` object. The `setAttribute` method is used to set new values for data in the `Session` object. The data in the `Session` object is stored as pairs of keys and values. A key is a string that identifies a type of data while a value is the data itself.

The `getAttribute` and `setAttribute` methods are defined in the `javax.servlet.http.HttpSession` interface and then extended by `netscape.nda.util.TempHttpSession`. The methods have the following syntax:

getAttribute

`public java.lang.Object getAttribute(java.lang.String` *name*`)`

where *name* is the name of a key in the `Session` object. All keys for the `Session` object are listed in Table 15-1.

setAttribute

`public void setAttribute(java.lang.String` *name*`, java.lang.Object` *value*`)`

where *name* is the name of a key in the `Session` object and *value* is the new value for the key. All keys for the `Session` object are listed in Table 15-1.

Keys

The data in the `Session` object is referred to by keys, individual strings that specify types of values. The different keys in the `Session` object are specified in the `SessionConstants` interface. Table 15-1 describes the keys that are stored in the `Session` object.

Table 15-1 Session Object Keys and What They Contain

Session Object Key	What It Contains
`QUERY_STRING`	The most recently entered LDAP query.
`USER_AGENT`	Information about the user's browser.
`ACCEPT_LANG`	The langurage value set for the session based on the user's language priference or the browser language (ie: en, eg, ja)
`DOMAIN`	The name of the domain that the user authenticated against. "Default" otherwise.
`USERNAME`	The currently authenticated user's user name.
`PASSWORD`	The currently authenticated user's password as entered on the change password screen.
`NEWPASSWORD`	The new password as entered on the change password screen.
`USER_TYPE`	A string specifying the current user's user type. Possible values are `ServiceAdminGroup`, `DomainAdminGroup`, `DeptAdminGroup`, `ServiceHelpDeskAdminGroup`, `DomainHelpDeskAdminGroup`, or `user`.

Table 15-1 Session Object Keys and What They Contain *(Continued)*

Session Object Key	What It Contains
DATABASE_CACHE_CLASS	The full name of the class that implemented the Database Cache (default value: netscape.nda.pagegenNDACasche)
LDAP_PROXY_AUTH	A boolean value specifying whether authentication by proxy is allowed by the user directory.
CHAR_SET_ENCODING	The CharacterSet encoding.
SERVLET_RESOURCE_SET	The ResourceSet for servlets.
AUTH_DOMAIN_DN	The DN of the authenticated user's domain.
SELF_DN	The authenticated user's DN.
SELF_PASSWD	The authenticated user's password.
ISP_DN	The DN of the Internet Service Provider (ISP). This key is only used in hosted environments.
DCROOT_DN	The Internet Service Provider's DC (domain component) DN (for example, dc=com, dc=siroe). This key is only used in hosted environments.
DOMAIN_DN	The domain DN.
DOMAIN_CONTAINER_DN	The domain container DN.
NEW_DOMAIN_CONTAINER_DN	The new domain container DN.
DOMAIN_CONTAINER_NAME	The name of the domain container.
ADM_DEPT_DN	The administration department DN.
DEPT_DN	The department DN.
FAMILY_GROUP_DN	The family group DN.
MAIL_LIST_DN	The mail list DN.
USER_DN	The user DN.
ICS_RESOURCE_DN	The ICS_RESOURCE_DN.
DOMAIN_ORGANIZATION_DN	The current domain organization DN.
DOMAIN_ORGANIZATION_LIST	The list of current domain organization DNs.
ANCESTOR_DOMAIN_DNS	The DNs of any ancestor domains (domains located above the current domain in the directory tree).
ANCESTOR_DEPT_DNS	The DNs of any ancestor departments (departments located above the current department in the directory tree).

Table 15-1 Session Object Keys and What They Contain *(Continued)*

Session Object Key	What It Contains
`NESTED_ANCESTOR_DOMAIN_DNS`	The DNs of any nested ancestor domains (domains located above the current domain but below another domain in the directory tree).
`NESTED_ANCESTOR_DEPT_DNS`	The DNs of any nested ancestor departments (departments located above the current department but below another department in the directory tree).
`NESTED_SUBDEPT_DNS`	The DNs of any nested sub-departments.
`STATUS_TITLE`	The title of the status message shown after an operation is completed
`STATUS_MESSAGE`	The status message shown after an operation is completed

`CLI_STATUS`	Used by CLI to indicate the results of an operation. CLI stores results in the format *object*`:` *task*. For example:
	`user@test.com: create user`
	`test.com: modify domain`

`PASSWORD_EXPIRING`	A boolean value that specifies whether the currently authenticated user's password is about to expire. A `TRUE` value indicates that the password is about to expire.
`EXCEPTION_MESSAGE`	The error message string returned as part of and exception throuwn during page generation
`STOPTASK`	A command to stop the task.

Accessing the TaskData Object

The `TaskData` object contains information about a task that is currently running within a given session. Task servlets can use the information in this object when performing operations. For example, a servlet that creates a user may look up the distinguished name (DN) information for the new user in the `TaskData` object. Another servlet might accept a user's request to delete a group, and then check the `TaskData` object's response field to determine the result of the operation.

Constructor and Fields

To create a TaskData object that will contain the input for a task, use the following constructor method:

```
TaskData(javax.servlet.http.HttpSession s,
         javax.servlet.http.HttpServletRequest req,
         javax.servlet.http.HttpServletResponse res,
ConfigurationSet config,
ResourceSet resource,
java.lang.String charSetEnc,
DatabaseInterface di)
```

where req, res, config, resource, charSetEnc, and di are the fields in which the TaskData object stores information. Table 15-2 lists these fields and what they contain.

Table 15-2 TaskData Object Fields and What They Contain

TaskData Field	What It Contains
`charSetEnc`	A string identifying the character set encoding of the data in the `TaskData` object.
`config`	An object of type `netscape.nda.util.ConfigurationSet`. For more information on objects of this type, see the online reference documentation (javadocs).
`di`	An object of type `netscape.nda.database.DatabaseInterface`. For more information on objects of this type, see the online reference documentation (javadocs).
`req`	The object of type `javax.servlet.http.HttpServletRequest` that contains the task request.
`res`	The object of type `javax.servlet.http.HttpServletResponse` that contains the response to `req` received from the server
`resource`	An object of type `netscape.nda.util.ResourceSet`. For more information on objects of this type, see the online reference documentation (javadocs).
`s`	The object of type `javax.servlet.http.HttpSession` that represents the session in which the task was requested.

Extending Authentication and Logout Servlets

This section tells you how to extend `NDAServlet` by customizing two `NDAServlet` subclasses, `NDABasicAuth`, which handles basic authentication, and `NDALogout`, which handles logout. You can apply the principles discussed in this section when extending `NDAServlet` for use in different applications.

What Extending NDAServlet Involves

When extending `NDAServlet`, you must do five things:

1. Create a Java source file that extends the `NDAServlet` class.
2. Compile the Java source file into a class file.
3. Copy the class file to the correct location.
4. Change the `servlets.properties` file.
5. Restart your web server.

The following section, “Creating a Java Source File,” tells you how to create a Java source file that extends the `NDAServlet` class. “Compiling and Packaging Your Java Classes,” which begins on page 354, tells you how to compile classes, copy files, and change `servlets.properties`.

Creating a Java Source File

The first step in extending `NDAServlet` is to create a Java source file for your custom class. This section explains how to do this using two example classes, `CustomBasicAuth`, which performs a customized version of basic authentication, and `CustomLogout,` which performs a customized logout procedure.

CustomBasicAuth

One example of a class that extends `NDAServlet` is `NDAAuth`. This class provides basic authentication services for iPlanet Delegated Administrator 4.5. Any authentication classes that iPlanet Delegated Administrator 4.5 uses are extensions of `NDAAuth`.

For example, a class called `NDABasicAuth` handles basic user ID and password authentication. In addition, a class called `NDACertAuth` handles certificate-based authentication, and a class called `NDASSOAuth` handles single sign-on authentication.

If you want to write your own authentication servlet, you can do so by extending `NDAAuth` and its subclasses (`NDABasicAuth`, `NDACertAuth`, and `NDASSOAuth`).

For example, suppose you want your enterprise to use the authentication mechanism in NDABasicAuth, but you want to extend the authentication servlet to also log details about each newly authenticated session. To do this, you can create a class called CustomBasicAuth that implements the postprocess method. Once authentication is complete, postprocess records information about the session and notes the current time for retrieval when the user logs out. The code for CustomBasicAuth looks like this:

```
package mycom.auth;

import netscape.nda.servlet.*;
import javax.servlet.*;
import javax.servlet.http.*;
import java.text.DateFormat;
import java.util.Date;
import mycom.auth.CustomSessionConstants;

public class CustomBasicAuth extends NDABasicAuth implements
   CustomSessionConstants
{

   protected void postprocess(HttpSession s, HttpServletRequest
                              req, HttpServletResponse res)
   {
      System.out.println(this.getClass().getName() + ":
                         postprocess called!");
      // This is where you can add code to create a log report
      String uid = req.getParameter(USERNAME);
      System.out.println(this.getClass().getName() + ": UserName:
                         " + uid);
      if(null == s) {
      return;
   }
   String userDn = (String) s.getAttribute(SELF_DN);
   String authOrgDn = (String) s.getAttribute(AUTH_DOMAIN_DN);
   String userAgent = (String) s.getAttribute(USER_AGENT);
   String lang = (String) s.getAttribute(ACCEPT_LANG);
   System.out.println(this.getClass().getName() + ":" +
                      "\n\tDN: " + userDn +
                      "\n\tOrg DN: " + authOrgDn +
                      "\n\tBrowser: " + userAgent +
                      "\n\tPref. lang: " + lang);
                      Date loginTime = new Date();
   String loginTimeString =
      DateFormat.getDateTimeInstance(DateFormat.LONG,DateFormat.
                                     LONG) format(loginTime);
   s.setAttribute(CUSTOM_LOGIN_TIME_KEY,loginTimeString);
}
```

In order to store the login time for later retrieval, CustomBasicAuth uses the setAttribute method to store a value called CUSTOM_LOGIN_TIME_KEY in a class called CustomSessionConstants. The CustomSessionConstants class is simply a Java interface that is defined as follows:

```
package mycom.auth;
public interface CustomSessionConstants
{
   public static final String CUSTOM_LOGIN_TIME_KEY =
   "customlogintime";
}
```

CustomLogout

When a user logs out, you might use an extended version of NDALogout to record the times when his or her session began and ended. To do this, you would write a class called CustomLogout that implements the execute method. The code for CustomLogout looks like this:

```
package mycom.auth;

import netscape.nda.servlet.*;
import javax.servlet.*;
import javax.servlet.http.*;
import java.text.DateFormat;
import java.util.Date;
import mycom.auth.CustomSessionConstants;
import java.io.*;

public class CustomLogout extends NDALogout implements
CustomSessionConstants
{
   protected void execute(HttpSession s,
                          HttpServletRequest req,
                          HttpServletResponse res)
                          throws ServletException, IOException
   {
   System.out.println(this.getClass().getName() + ": execute
                      called!");
   // add code here to report the logout event
   // we will print out the time when this occurred
   if(null != s) {

   String loginTimeString =
      (String)s.getAttribute(CUSTOM_LOGIN_TIME_KEY);
   String uid = req.getParameter(USERNAME);
   String userDn = (String)s.getAttribute(SELF_DN);
   String authOrgDn = (String)s.getAttribute(AUTH_DOMAIN_DN);
   Date logoutTime = new Date();
   String logoutTimeString =
      DateFormat.getDateTimeInstance(DateFormat.LONG,DateFormat.
                                     LONG).format(logoutTime);
   System.out.println(this.getClass().getName() + ": \n\tDN: " +
                      userDn +
                      "\n\tOrg DN: " + authOrgDn +
                      "\n\tLogged in at: " + loginTimeString +
                      "\n\tLogged out at: " + logoutTimeString);
   } else {
   // Most likely, the session has timed out.
   System.out.println(this.getClass().getName() + ": User logged
                      out from a timed out session");
   }
super.execute(s,req,res);
}
```

CustomLogout uses the getAttribute method to retrieve the value for CUSTOM_LOGIN_TIME_KEY from the CustomSessionConstants class.

Extending Task Servlets

In iPlanet Delegated Administrator 4.5, a task is any operation that creates, modifies, or deletes a directory entry. Delegated Administrator uses the methods in the netscape.nda.util.Task class to perform tasks. Subclasses of Task define specific operations involving objects. For example, CreateUser contains the code necessary to create a new user object. Similarly, ModifyUser contains the code necessary to modify a user object.

iPlanet Delegated Administrator 4.5 uses the NDATaskManager servlet to manage tasks. Any HTML form that calls this servlet must contain a hidden value that specifies the type of task to perform. When a user or administrator submits the form, NDATaskManager interprets the hidden value and then invokes the appropriate Task subclass for the requested operation.

To determine the correct Task subclass to invoke, NDATaskManager consults the resource.properties file. Once it identifies and invokes the correct subclass, NDATaskManager calls the subclass's doIt method. This method processes the operation. You can extend a Task subclass and override its doIt method to create customized behavior.

The doIt method has the following syntax:

```
public void doIt(TaskData td) throws java.lang.Exception
```

where *td* is the task input data contained in netscape.nda.servlet.TaskData.

What Extending a Task Servlet Involves

When extending a subclass of Task, you must do five things:

1. Create a Java source file that extends the Task subclass.
2. Compile the Java source file into a class file.
3. Change the servlets.properties file or resource.properties file.
4. Copy the class file to the correct location.
5. Restart your web server.

The following section, "Creating a Java Source File," tells you how to create a Java source file that extends a Task subclass. "Compiling and Packaging Your Java Classes," which begins on page 354, tells you how to compile classes, change servlets.properties and resource.properties, and copy files.

Creating a Java Source File

The first step in extending a Task subclass is to create a Java source file for your custom class. This section explains how to do this using two examples, CustomCreateUser and CustomModifyUser.

CustomCreateUser

The CustomCreateUser class extends iPlanet Delegated Administrator 4.5’s default CreateUser class by adding some additional attributes. The class’s doIt method first performs any operations in CreateUser and then adds additional attributes. The code for the class is as follows:

```
package mycom.tasks;
import netscape.nda.servlet.*;
import javax.servlet.*;
import javax.servlet.http.*;
public class CustomCreateUser extends CreateUser
{
   public CustomCreateUser()
   {
      super();
   }
   public void doIt(TaskData td)
      throws Exception
   {
   System.out.println(this.getClass().getName() + ": preprocess
                      called!");
   super.doIt(td);
   System.out.println(this.getClass().getName() + ": postprocess
                      called!");
   // add some extra attributes
   // modify user specified attributes
   }
}
```

CustomModifyUser

The CustomModifyUser class extends iPlanet Delegated Administrator 4.5’s default ModifyUser class by modifying additional attributes. The class’s doIt method first performs any operations in ModifyUser and then modifies the additional attributes. The code for the class is as follows:

```
package mycom.tasks;
import netscape.nda.servlet.*;
import javax.servlet.*;
import javax.servlet.http.*;
public class CustomModifyUser extends ModifyUser
{
   public CustomModifyUser()
   {
      super();
   }
   public void doIt(TaskData td)
```

```
      throws Exception
   {
      System.out.println(this.getClass().getName() + ":
                         preprocess called!");
      super.doIt(td);
      System.out.println(this.getClass().getName() + ":
                         postprocess called!");
      // add some extra attributes
      // modify user specified attributes
   }
}
```

Compiling and Packaging Your Java Classes

Once you have written the Java source code for your custom servlets, you are ready to compile and package them. This process involves doing the following:

1. Compiling your source files.
2. Modifying `servlets.properties` or `resource.properties`.
3. Packaging and copying your classes.
4. Restarting the Web Server.

This section tells you how to perform these steps.

Compiling Your Source Files

Compiling your Java source files into classes for use with iPlanet Delegated Administrator 4.5 is a four-part process that involves understanding Delegated Administrator's Java Development Kit (JDK) and system requirements, setting your classpath, writing a makefile, and compiling your source.

JDK and System Requirements

In order for your servlets to work with iPlanet Delegated Administrator 4.5, you must compile them using version 1.2.2 of the JDK compiler (or a compatible product). If you are compiling on a Sun workstation, make sure you are running Solaris 2.6.

Setting Your Classpath

In order to successfully compile your classes, you must install iPlanet Delegated Administrator 4.5 and set your classpath to include its Java classes.

On UNIX, this involves setting the CLASSPATH environment variable to include the nda/classes subdirectory of your server root. On Windows NT, you set the classpath by opening the System Control Panel, selecting the Environment tab, and then adding the nda/classes subdirectory of your server root to the CLASSPATH system variable.

For more information on setting your classpath, see your system and JDK documentation.

Writing a Makefile

A makefile is a set of instructions that the make program uses to turn source files into executable code. The contents of a makefile vary depending on what you are compiling, but typically include a set of directives that specify which compiler to use, what flags to pass to the compiler, and how to process different source files.

A makefile for the CustomBasicAuth, CustomLogout, CustomCreateUser, and CustomModifyUser classes discussed earlier in this chapter might look like this:

```
JAVABINPATH = /share/builds/components/jdk/1.2.2/SunOS/bin
IDAHOME = /export/user/work/ida/ida45home
IWSHOME = /export/user/work/ida/nes41
CLASSPATH =
".:$(IWSHOME)/bin/https/jar/servlets.jar:$(IDAHOME)/nda/classes/
ldapjdk.jar:$(IDAHOME)/nda/classes/ida45.jar:$(IDAHOME)/nda/clas
ses/xpclass.jar"
all:
   $(JAVABINPATH)/javac -d . -classpath $(CLASSPATH) *.java
   - mkdir javadoc
   $(JAVABINPATH)/javadoc -d javadoc -classpath $(CLASSPATH)
   *.java
```

When you run make from within the directory that contains your source files, it looks for a file called Makefile (you can also specify a makefile by using the -f flag). When it finds the makefile, make executes the all command.

In the makefile example just shown, the first seven lines specify constants that make uses to compile source files. The final five lines contain the all command, which first compiles all Java source files using the -d flag and then creates javadocs for the compiled classes.

For more information on makefiles and the make program, see your compiler documentation or your system man pages for make.

Compiling Your Source Files

Once you have written your makefile, you are ready to compile your Java source files into Java class files. To do this, make sure that your makefile is in the correct directory (typically the same directory as your source files) and then run `make`.

Modifying Properties Files

Once you have compiled your source files into Java classes, you are ready to modify iPlanet Delegated Administrator 4.5 so that it will use your custom servlets by changing its properties files. Delegated Administrator uses two properties files when working with servlets: `servlets.properties` and `resource.properties`.

servlets.properties

The `servlets.properties` file is used by iPlanet Delegated Administrator 4.5 to execute non-task servlets. It is stored in the `https-`*yourServerIdentifier*`/config` subdirectory of the folder where your instance of Netscape Enterprise Server or iPlanet Web Server is installed (where *yourServerIdentifier* is the name of your web server instance). The `servlets.properties` file maps servlet names to classes and specifies any classpath information or initial arguments for specific servlets. It has the following syntax:

```
servlet.servletName.code=servletClassName

[servlet.servletName.classpath=classpath]

servlet.servletName.initArgs=[initArgs]
```

Variables in the `servlets.properties` file are defined as follows:

- *servletName* is the name of the servlet that you are mapping
- *servletClassName* is the complete class name for the servlet (such as `netscape.nda.servlet.myservlet`)
- *classpath* is the path to the directory in which the class is located (using forward slashes only, such as `/ida/idaclasses`)
- *initArgs* are any initial arguments that the class takes.

The `classpath` line of `servlets.properties` is optional. If your class does not take any initial arguments, just enter the following:

```
servlet.servletName.initArgs=
```

resource.properties

The `resource.properties` file is used by iPlanet Delegated Administrator 4.5 to execute tasks. It is stored in the `nda/classes/netscape/nda/servlet` subdirectory of your iPlanet Delegated Administrator 4.5 installation root directory. The file maps servlet names (as specified in `servlets.properties`) to Java classes. It has the following syntax:

```
class-servletName=servletClassName
```

Variables in the `resource.properties` file are defined as follows:

- *servletName* is the name of the servlet that you are mapping.
- *servletClassName* is the complete class name for the servlet (such as `netscape.nda.servlet.myservlet`).

Examples

The following parts of `servlets.properties` and `resource.properties` files show how you might map the `CustomBasicAuth`, `CustomLogout`, `CustomCreateUser`, and `CustomModifyUser` classes described earlier in this chapter. Code Example 1 shows part of a sample `servlets.properties` file. Code Example 2 shows part of a sample `resource.properties` file.

Code Example 1 Part of a sample `servlets.properties` file.

```
#
# Custom authentication servlet
#
servlet.auth.code=mycom.auth.CustomBasicAuth
servlet.auth.initArgs=

#
# Custom logout servlet
#
servlet.logout.code=mycom.auth.CustomLogout
servlet.logout.initArgs=
```

Code Example 2 Part of a sample `resource.properties` file.

```
class-CreateUser=mycom.tasks.CustomCreateUser
class-DeleteUser=mycom.tasks.CustomDeleteUser
class-ModifyUser=mycom.tasks.CustomModifyUser
```

Packaging and Copying Your Classes

When you have finished modifying `servlets.properties` and `resource.properties`, you are ready to package your files in a Java Archive (JAR) and then copy them to the appropriate directory.

To Package Your Files In a JAR

1. Navigate to the folder where your class files are located.
2. From the command line execute the following:

   `jar -c` *jarFileName.jar sourceFileNames*

   where *jarFileName.jar* is the destination JAR file (such as `myclasses.jar`) and *sourceFileNames* are the names of your class files.

To Copy Your JAR File

1. Navigate to the directory where your JAR file is stored.
2. Copy the file to the `/nda/classes` subdirectory of your iPlanet Delegated Administrator 4.5 server root.

Restarting the Web Server

When you have finished packaging your files in a JAR and copying them to the `nda/classes` directory, you must restart the Web Server. For more information on how to do this, see the documentation that came with your web server software.

Part 5

Appendixes

Appendix A

Using an Existing User Directory

If you have already deployed Netscape Directory Server and populated it with users and groups, you must modify both your user directory tree and the Delegated Administrator framework so that the two will work together. The changes you make depend upon your existing directory structure.

NOTE If you have already installed Netscape Delegated Administrator 4.1x and are upgrading to iPlanet Delegated Administrator 4.5, see "Upgrading from Delegated Administrator Version 4.11" on page 387.

This appendix provides general guidelines to help you edit your directory entries to allow them to be managed by Delegated Administrator. It includes the following topics:

- Modifying Your User Directory
- Configuring Delegated Administrator for Other Tree Structures
- The Delegated Administrator Directory Information Tree (DIT)
- Defining Object Types

Modifying Your User Directory

If Delegated Administrator detects during installation that you already have data stored at your desired suffix, it will install all required configuration information in the directory. But it will NOT modify or add to existing user, group, or organization data. Before Delegated Administrator can manage your existing user data, you must manually make the following changes in your user directory:

- Add Delegated Administrator object classes and attributes to all user, group, and organization entries.
- Add Delegated Administrator ACIs to the root of the tree and to each organization node.
- Add Administrator groups at the root level and at each organization level.
- Compute and store the number of objects in the tree.

NOTE The updates to user data described in this appendix require advanced experience with Netscape Directory Server, the LDAP Data Interchange Format (LDIF), and Access Control Instructions (ACIs). For comprehensive documentation on these topics, see the Directory Server Administrator's Guide.

In the following steps and examples, there is one container node for all users under each organization. There may be any number of organizations under the root entry for the user data tree, and organizations may be nested.

Step 1: Create a Top-level Administrator

It is necessary to create a Top-level Administrator entry in your directory to initiate the delegation process before Delegated Administrator is installed. The new Top-level Administrator serves an the entry point to the Delegated Administrator User Interface.

The new or existing user entry must contain the DN appropriate to your base suffix and the specific attributes in the following example.

1. Create a new, or modify existing user.

   The example DN in this step assumes the organization o=Siroe exists under the base suffix o=ISP and chris belongs to o=Siroe. Alter the construct to reflect the DN for your directory.

   ```
   uid=chris, ou=People, o=Siroe, o=ISP
   ```

2. Add the following attribute to the Top-level Administrator group entry: `dn: cn=Service Administrators, ou=Groups, o=ISP`

   ```
   uniqueMember: uid=chris, ou=People, o=Siroe, o=ISP
   ```

3. Add the following attribute to the user entry.

   ```
   memberOf: cn=Service Administrators, ou=Groups, o=ISP
   ```

The user is now Top-level Administrator with the permissions afforded to that category of user.

Step 2: Modify user entries.

1. Each user entry must contain the nsManagedPerson object class.
2. In each user entry, add the attribute `nsdaDomain`. The value of the attribute must be the name of the organization that the user belongs to.

Example:

```
dn: uid=scarter, ou=Users, o=Siroe.com, o=ISP
objectclass: top
objectclass: person
objectclass: organizationalperson
objectclass: inetorgperson
objectclass: nsManagedPerson
uid: scarter
userpassword: password
cn: Sam Carter
sn: Carter
givenname: Sam
nsdaDomain: Siroe.com
telephoneNumber: 650.555.1212
mail: scarter@Siroe.com
```

Step 3: Modify Organization Entries.

1. Each organization entry must contain the nsManagedDomain object class.

2. Add the following attributes to each organization entry (sample values are listed, indicating the maximum number of objects of various types which may be created in the organization):

   ```
   nsmaxusers: 1000

   nsmaxdepts: 100

   nsmaxmaillists: 1000

   nsmaxdomains: 10
   ```

Example:

```
# Siroe domain
#
dn: o=Siroe.com, o=ISP
objectclass: top
objectclass: organization
objectclass: nsManagedDomain
description: Domain Root for Siroe.com
nsMaxUsers: 1000
nsMaxDepts: 100
nsMaxMailLists: 1000
nsMaxDomains: 10
o: Siroe.com
```

3. The following ACIs must be added to each organization entry, replacing `o=Siroe.com, o=isp` with the DN of the entry. The file `isp.ldif` contains the default Delegated Administrator ACIs, and is available for download at `http://docs.iplanet.com/docs/manuals/deladmin/45/scripts/isp.ldif`.

```
aci:(targetattr="*")(targetfilter=(objectClass=nsManagedDomain))
 (version 3.0; acl "Domain Adm domain access"; allow
 (read,search) groupdn="ldap:///cn=Domain Administrators,
 ou=Groups, o=Siroe.com, o=isp";)

aci: (target="ldap:///cn=Domain Administrators, ou=Groups,
 o=Siroe.com,o=isp")(targetattr="*")(targetfilter=(|(objectClas
s=nsManagedDeptAdminGroup)(objectClass=nsManagedDept)))(version
 3.0; acl "Domain Adm dept access"; allow (read,search)
 groupdn="ldap:///cn=Domain Administrators, ou=Groups, o=Siroe.c
 om, o=isp";)

aci: (target="ldap:///cn=Domain Help Desk Administrators,
 ou=Groups, o=Siroe.com,
 o=isp")(targetattr="*")(targetfilter=(|(objectClass=nsManagedDe
 ptAdminGroup)(objectClass=nsManagedDept)))(version 3.0; acl
 "Domain Adm dept access"; allow (read,search,write)
 groupdn="ldap:///cn=Domain Administrators, ou=Groups,
 o=Siroe.com, o=isp";)
```

```
aci: (target="ldap:///cn=Domain Department
 Administrators,ou=Groups,o=Siroe.com,o=isp")(targetattr="*")(t
argetfilter=(|(objectClass=nsManagedDeptAdminGroup)(objectClass
=nsManagedDept)))(version 3.0; acl "Domain Adm dept access";
 allow (read,search,write) groupdn="ldap:///cn=Domain
 Administrators, ou=Groups,o=Siroe.com, o=isp" or
 groupdn="ldap:///cn=Domain Department Administrators, ou=Groups,
 o=Siroe.com, o=isp";)

aci:(target="ldap:///ou=*,o=Siroe.com,o=isp")(targetattr="*")(t
argetfilter=(objectClass=nsManagedOrgUnit))(version 3.0; acl
 "Domain Adm org unit access"; allow
 (read,search,write)groupdn="ldap:///cn=Domain Administrators,
 ou= Groups, o=Siroe.com, o=isp";)

aci: (target="ldap:///ou=*,
 o=Siroe.com,o=isp")(targetattr="*")(targetfilter
 =(|(objectClass=nsManagedDept)(objectClass=nsManagedDeptAdminGr
 oup)(objectClass=nsManagedMailList)))(version 3.0; acl "Domain
 Adm dept access"; allow (all) groupdn="ldap:///cn=Domain
 Administrators, ou=Groups, o=Siroe.com, o=is p";)

aci:(targetattr="*")(targetfilter=(objectClass=nsManagedPerson))
 (version 3.0;acl "Domain Adm user access";
 allow(read,search,add) groupdn="ldap:///cn=Domain
 Administrators, ou=Groups,o=Siroe.com, o=isp";)

aci:(targetattr="*")(targetfilter=(&(objectClass=nsManagedPerson
 )(&(!(memberOf=cn=Service Administrators,
 ou=Groups,o=isp))(&(!(memberOf=cn=Service Help Desk
 Administrators, ou=Groups, o=isp))(!(memberOf=cn=Domain
 Administrators, ou=Groups, o=Siroe.com, o=isp))))))(version
 3.0; acl "Domain Adm user modify access"; allow
 (write,delete)groupdn="ldap:///cn=Domain Administrators,
 ou=Groups, o=Siroe.com, o=isp";)

aci: (target="ldap:///o=*,
 o=Siroe.com,o=isp")(targetattr="*")(targetfilter=
 (|(objectClass=nsManagedDomain)(objectClass=nsManagedDeptAdminG
 roup)(objectClass=nsManagedOrgUnit)(objectClass=nsManagedDept)(
 objectClass=nsManagedMailList)))(version 3.0; acl "Domain Adm
 access"; allow (all) groupdn="ldap:///cn =Domain Administrators,
 ou=Groups, o=Siroe.com, o=isp";)
```

```
aci:(targetattr="*")(targetfilter=(|(objectClass=nsManagedDomain
 )(objectClass=nsManagedPerson)))(version 3.0; acl "DHDA access";
 allow (read,search) groupdn="ldap:///cn=Domain Help Desk
 Administrators, ou=Groups, o=Siroe.com, o= isp";)

aci:(targetattr="*")(targetfilter=(objectClass=nsManagedMailList
 ))(version 3.0; acl "DHDA mail list access"; allow (all)
 groupdn="ldap:///cn=Domain HelpDesk Administrators, ou=Groups,
 o=Siroe.com, o=isp";)

aci:(targetattr="userPassword")(targetfilter=(&(objectClass=nsMa
 nagedPerson)(&(!(memberOf=cn=Service Administrators, ou=Groups,
 o=isp))(&(!(memberOf=cn=S ervice Help Desk Administrators,
 ou=Groups, o=isp))(&(!(memberOf=cn=Domain Administrators,
 ou=Groups, o=Siroe.com, o=isp))(!(memberOf=cn=Domain Help Desk
 Administrators, ou=Groups, o=Siroe.com, o=isp)))))))(version
 3.0; acl "D HDA user write access"; allow (write)
 groupdn="ldap:///cn=Domain Help Desk Administrators, ou=Groups,
 o=Siroe.com, o=isp";)
```

Step 4: Create Start and Login Pages for Each Organization.

Each organization must have its own Start page and Login page.

If you want to replace the default organization Siroe.com with your own organization, modify its Start and Login pages.

1. In the file `<delegatedadmin_root>/nda/nda/start.htm`, modify the following line, replacing `o=Siroe.com` with the base DN for the organization:

   ```
   var domain = "o=Siroe.com";
   ```

2. In the file `<delegatedadmin_root>/nda/nda/login.htm`, modify the following line, replacing `o=Siroe.com` with the base DN for the organization:

   ```
   var domain = "o=Siroe.com";
   ```

If you're creating a new organization, or modifying an existing one, first determine the location of the files for the new organization. For example, the files for the default Delegated Administrator organization Siroe.com are stored here:

```
<delegatedadmin_root>/nda/nda/default/en
```

If organization ABC replicates this structure, its organization files will be stored here:

`<delegatedadmin_root>/nda/nda/ABC/en`

Once you've determined appropriate file location, follow these steps to create the new Start and Login pages for the organization:

1. Copy these files to the directory where your organization files are stored:

   `<delegatedadmin_root>/nda/nda/start.htm`

   `<delegatedadmin_root>/nda/nda/login.htm`

2. In the file `start.htm`, modify the following line, replacing `o=Siroe.com` with the base DN for the organization:

   ```
   var domain = "o=Siroe.com";
   ```

3. In the file `login.htm`, modify the following line, replacing `o=Siroe.com` with the base DN for the organization:

   ```
   var domain = "o=Siroe.com";
   ```

Step 5: Modify the Root Entry.

1. The root entry of the tree - the parent of all top-level organizations - must contain the object class `nsManagedISP`.

   Example

   ```
   dn: o=ISP
   objectclass: top
   objectclass: organization
   objectclass: nsManagedISP
   o: ISP
   ```

2. Add the following ACIs must to the root entry, replacing `o=isp` with the DN of the entry.

```
aci:(targetattr!="userPassword")(targetfilter=(objectClass=nsMan
 agedPerson))(version 3.0; acl "Anonymous access to User
 entries"; allow (read,search) userdn="ldap:///anyone";)

aci:(target="ldap:///cn=postmaster,o=isp")(targetattr="*")(versi
 on 3.0; acl "Anonymous access to Postmaster entry"; allow
 (read,search) userdn="ldap:///anyone";)

aci:(target="ldap:///cn=domainConfiguration,
 ou=config,o=isp")(targetattr="*")(version 3.0; acl "Anonymous
 access to Configuration entry"; allow (read,search)
 userdn="ldap:///anyone";)

aci:(targetattr="objectClass||uid||mail||userCertificate")(targe
 tfilter=(objectClass=nsManagedPerson))(version 3.0; acl "NDAUser
 access"; allow (read,search) userdn="ldap:///uid=NDAUser,
 ou=config, o=isp";)

aci:(targetattr="objectClass||o||nsNumDomains")(targetfilter=(ob
 jectClass=nsManagedISP))(version 3.0; acl "NDAUser access";
 allow (read,search) userdn="ldap:///uid=NDAUser, ou=config,
 o=isp";)

aci:(targetattr="objectClass||o||nsNumUsers||nsNumDepts||nsNumMa
 ilLists||nsNumDomains||nsMaxUsers||nsMaxDepts||nsMaxMailLists||
 nsMaxDomains")(targetfilter=(objectClass=nsManagedDomain))(vers
 ion 3.0; acl "NDAUser access"; allow (read,search)
 userdn="ldap:///uid=NDAUser, ou=config, o=isp";)

aci:(targetattr="objectClass||cn||nsNumUsers||nsNumDepts||nsMaxU
 sers||nsMaxDepts")(targetfilter=(objectClass=nsManagedDept))(ve
 rsion 3.0; acl "NDAUser access"; allow (read,search)
 userdn="ldap:///uid=NDAUser, ou=config, o=isp";)

aci:(targetattr="objectClass||cn||nsNumUsers||nsMaxUsers")(targe
 tfilter=(objectClass=nsManagedMailList))(version 3.0; acl
 "NDAUser access"; allow (read,search)
 userdn="ldap:///uid=NDAUser, ou=config, o=isp";)

aci:(targetattr="nsNumDomains")(targetfilter=(objectClass=nsMana
 gedISP))(version 3.0; acl "NDAUser access"; allow (write)
 userdn="ldap:///uid=NDAUser, ou=config, o=isp";)

aci:(targetattr="nsNumUsers||nsNumDepts||nsNumMailLists||nsNumDo
 mains")(targetfilter=(objectClass=nsManagedDomain))(version 3.0;
 acl "NDAUser access"; allow (write) userdn="ldap:///uid=NDAUser,
 ou=config, o=isp";)
```

```
aci:(targetattr="nsNumUsers||nsNumDepts")(targetfilter=(objectCl
 ass=nsManagedDept))(version 3.0; acl "NDAUser access"; allow
 (write) userdn="ldap:///uid=NDAUser, ou=config, o=isp";)

aci:(targetattr="nsNumUsers")(targetfilter=(objectClass=nsManage
 dMailList))(version 3.0; acl "NDAUser access"; allow (write)
 userdn="ldap:///uid=NDAUser, ou=config, o=isp";)

aci:(targetattr="*")(targetfilter=(objectClass=nsManagedISP))(ve
 rsion 3.0; acl "SA root node access"; allow (read,search)
 groupdn="ldap:///cn=Service Administrators, ou=Groups, o=isp";)

aci:(targetattr="*")(targetfilter=(|(objectClass=nsManagedDomain
 )(objectClass=nsManagedOrgUnit)(objectClass=nsManagedDeptAdminG
 roup)(objectClass=nsManagedDept)(objectClass=nsManagedMailList)
 (objectClass=nsManagedPerson)))(version3.0; acl "SA domain
 access"; allow (all) groupdn="ldap:///cn=Service Administrators,
 ou=Groups, o=isp";)

aci:(targetattr="*")(targetfilter=(|(objectClass=nsManagedISP)(|
 (objectClass=nsManagedDomain)(objectClass=nsManagedPerson))))(v
 ersion 3.0; acl "SHDA rootnode access"; allow (read,search)
 groupdn="ldap:///cn=Service Help Desk Administrators, ou=Groups,
 o=isp";)

aci:(targetattr="userPassword")(targetfilter=(&(objectClass=nsMa
 nagedPerson)( &(!(memberOf=cn=Service Administrators, ou=Groups,
 o=isp))(!(memberOf=cn=Service Help Desk Administrators,
 ou=Groups, o=isp)))))(version 3.0; acl "SHDAuser write access";
 allow (write) groupdn="ldap:///cn=Service Help Desk
 Administrators, ou=Groups, o=isp";)

aci:(targetattr="*")(targetfilter=(|(objectClass=nsManagedDept)(
 objectClass=nsManagedDeptAdminGroup)))(version 3.0; acl "Dept
 Adm dept access"; allow (read,search)
 userdn="ldap:///o=isp??sub?(memberOf=cn=Department
 Administrators*)" and
 groupdnattr="ldap:///o=isp?nsDAModifiableBy";)

aci:(targetattr="nsNumUsers||nsNumDepts||uniqueMember")(targetfi
 lter=(|(objectClass=nsManagedDept)(objectClass=nsManagedDept)))
 (version 3.0; acl "Dept Adm dept access"; allow (write)
 userdn="ldap:///o=isp??sub?(memberOf=cn=Department
 Administrators*)" and
 groupdnattr="ldap:///o=isp?nsDAModifiableBy";)
```

```
aci:(targetattr="*")(targetfilter=(|(objectClass=nsManagedDeptAd
 minGroup)(objectClass=nsManagedDept)))(version 3.0; acl "Dept
 Adm dept access"; allow (all)
 userdn="ldap:///o=isp??sub?(memberOf=cn=Department
 Administrators*)" and groupdnattr="ldap:///o=isp?owner";)

aci:(targetattr="*")(targetfilter=(objectClass=nsManagedPerson))
 (version 3.0;acl "Dept Adm user modify access"; allow
 (write,delete)
 userdn="ldap:///o=isp??sub?(memberOf=cn=Department
 Administrators*)" and groupdnattr="ldap:///o =isp?owner";)

aci:(targetattr="*")(targetfilter=(objectClass=nsManagedPerson))
 (version 3.0;acl "Dept Adm user create access"; allow (add)
 userdn="ldap:///o=isp??sub?(memberOf=cn=Department
 Administrators*)";)

aci:(targetattr="*")(targetfilter=(objectClass=nsManagedPerson))
 (version 3.0;acl "User self modification"; allow (read,search)
 userdn="ldap:///self";)

aci:(targetattr!="uid||ou||owner||nsDAModifiableBy||nsDACapabili
 ty||mail||mailAlternateAddress||memberOf||nsDADomain")(targetfi
 lter=(objectClass=nsManagedPerson))(version 3.0; acl "User self
 modification"; allow (write) userdn="ldap:///self";)

aci: (targetfilter=(objectClass=nsManagedPerson))(version 3.0;
 acl "User self deletion"; deny (delete) userdn="ldap:///self";)

aci:(targetattr="memberOf")(targetfilter=(objectClass=nsManagedP
 erson))(version 3.0; acl "Administrator self promotion or
 demotion"; deny (write) userdn="ldap:///self";)

aci:(targetattr="*")(targetfilter=(objectClass=nsManagedMailList
 ))(version 3.0; acl "Mail list create access"; allow (add)
 userdn="ldap:///o=isp??sub?(nsDACapability=mailListCreate)";)

aci:(targetattr!="nsMaxUsers")(targetfilter=(objectClass=nsManag
 edMailList))(version 3.0; acl "Mail list owner access"; allow
 (read,search,write,delete) groupdnattr="ldap:///o=isp?owner";)

aci: (target="ldap:///ou=COS, o=ISP")(targetattr="*")(version
 3.0; acl"Access to all for read/search"; allow (read,search)
 userdn="ldap:///all";)
```

Step 6: Create Group Containers.

1. Create a group container named ou=Groups under the root of the tree, and then create a container named ou=Groups under each organization.
2. Each ou=Groups container entry must include the `nsManagedOrgUnit` object class.

   Examples:

```
dn: ou=Groups, o=isp
objectclass: top
objectclass: organizationalUnit
objectclass: nsManagedOrgUnit
ou: Groups

dn: ou=Groups, o=Siroe.com, o=isp
objectclass: top
objectclass: organizationalUnit
objectclass: nsManagedOrgUnit
ou: Groups
```

3. Add the following ACIs to each group container entry except for the one directly under the root of the tree. Using this example, replace `o=Siroe.com, o=isp` with the DN of the entry.

```
aci:(targetattr="uniqueMember")(targetfilter=(&(objectClass=nsMa
 nagedMailList)(mgmanJoinability=all)))(version 3.0; acl "User
 self subscribe access"; allow (selfwrite) userdn="ldap:///uid=*,
 ou=People, o=Siroe.com, o=isp";)

aci:(targetattr!="uniqueMember||mgrpRfc822MailMember")(targetfil
 ter=(&(objectClass=nsManagedMailList)(mgmanHidden=false)))(vers
 ion 3.0; acl "User mail list access when visible"; allow
 (read,search) userdn="ldap:///uid=*, ou=People, o=Siroe.com,
 o=isp";)

aci:(targetattr="uniqueMember||mgrpRfc822MailMember")(targetfilt
 er=(&(objectClass=nsManagedMailList)(mgmanMemberVisibility=all)
 ))(version 3.0; acl "Usermail list member access"; allow
 (read,search) userdn="ldap:///uid=*, ou=People, o=Siroe.com,
 o=isp";)

aci:(targetattr="uniqueMember||mgrpRfc822MailMember")(targetfilt
 er=(&(objectClass=nsManagedMailList)(mgmanMemberVisibility=rest
 ricted)))(version 3.0; acl"User mail list access - group"; allow
 (read,search)groupdnattr="ldap:///o=isp?mgmanMemberVisibilityGr
 oup";)

aci:(targetattr="uniqueMember||mgrpRfc822MailMember")(targetfilt
 er=(&(objectClass=nsManagedMailList)(mgmanMemberVisibility=anyo
 ne)))(version 3.0; acl "User mail list access - public"; allow
 (read,search) userdn="ldap:///anyone";)
```

Step 7: Add New Administrator Groups.

1. Create the following administrator groups under the ou=Groups node which is directly below the root entry of the tree. Using this example, you would replace `o=isp` with the DN of the root of your tree, and replace the two `uniquemember` values with the DNs of existing administrator users. Example:

```
dn: cn=Service Administrators, ou=Groups, o=isp
objectclass: top
objectclass: groupOfUniqueNames
objectclass: nsManagedDept
objectclass: inetAdmin
cn: Service Administrators
nsmaxusers: Unlimited
adminrole: Service Administrators
uniquemember: uid=chris, ou=People, o=Siroe.com, o=isp


dn: cn=Service Help Desk Administrators, ou=Groups, o=isp
objectclass: top
objectclass: groupOfUniqueNames
objectclass: nsManagedDept
objectclass: inetAdmin
cn: Service Help Desk Administrators
nsmaxusers: Unlimited
adminrole: Service Help Desk Administrators
uniquemember: uid=fred, ou=People, o=Siroe.com, o=isp
```

2. Create the following administrator groups in the ou=Groups node under each organization in the tree (replace `o=Siroe.com, o=isp` with the DN of the organization):

```
dn: cn=Domain Administrators, ou=Groups, o=Siroe.com, o=isp
 objectclass: top
objectclass: groupOfUniqueNames
objectclass: nsManagedDept
objectclass: inetAdmin
cn: Domain Administrators
adminrole: Domain Administrators
nsmaxusers: Unlimited

dn: cn=Domain Department Administrators, ou=Groups, o=Siroe.com,
 o=isp
objectclass: top
objectclass: groupOfUniqueNames
objectclass: nsManagedDept
objectclass: inetAdmin
cn: Domain Department Administrators
adminrole: Domain Department Administrators
nsmaxusers: Unlimited

dn: cn=Domain Help Desk Administrators, ou=Groups, o=Siroe.com,
 o=isp
objectclass: top
objectclass: groupOfUniqueNames
objectclass: nsManagedDept
objectclass: inetAdmin
cn: Domain Help Desk Administrators
adminrole: Domain Help Desk Administrators
nsmaxusers: Unlimited
```

Step 8: Update the Containers for People.

The container node for users in each organization (ou=People by default) must include the objectclass nsManagedOrgUnit and the following ACI (replace o=Siroe.com, o=isp with the DN of the organization):

```
dn: ou=People, o=Siroe.com, o=isp
objectclass: top
objectclass: organizationalUnit
objectclass: nsManagedOrgUnit
ou: People
aci:(targetattr!="userPassword")(targetfilter=(objectClass=nsMan
 aged Person))( version 3.0; acl "User access to all users in
 domain"; allow (read,search) userdn="ldap:///uid=*, ou=People,
 o=Siroe.com, o=isp";)
```

Step 9: Create Non-Administrator Groups.

1. If non-administrator groups are to be managed by Delegated Administrator, they should be created under ou=Groups for each organization. In early versions of Delegated Administrator, these groups were called Departments. If you want to create non-administrator groups manually rather than through the GUI, the group should look like the sample below. In this example, replace Group1 with the name of the group, o=Siroe.com, o=isp with the DN of the organization, and substitute existing group members for the uniquemember value:

```
dn: cn=Group1, ou=Groups, o=Siroe.com, o=isp
objectclass: top
objectclass: groupOfUniqueNames
objectclass: nsManagedDept
cn: Group1
nsmaxusers: 20
nsmaxdepts: 10
uniquemember: uid=bill, ou=People, o=Siroe.com, o=isp
nsdamodifiableby: cn=Department Administrators, cn=Group1,
 ou=Groups, o=Siroe .com, o=isp
```

2. Create an administrator group under each such group. In the following example, replace Group1 with the name of the group, o=Siroe.com, o=isp with the DN of the organization, and substitute an existing administrator user or users for the uniquemember value:

```
dn: cn=Department Administrators, cn=Group1, ou=Groups,
 o=Siroe.com, o=isp
objectclass: top
objectclass: groupOfUniqueNames
objectclass: nsManagedDeptAdminGroup
objectclass: inetAdmin
cn: Department Administrators
adminrole: Department Administrators
uniquemember: uid=doris, ou=People, o=Siroe.com, o=isp
```

Step 10: Initialize the Object Counters.

Delegated Administrator keeps track of the number of objects in the user data tree such as users, groups, organizations, and mailing lists . After manually making changes to the tree, including the steps above to make an existing tree manageable by Delegated Administrator, the object counters must be initialized.

Initializing the object counters may be achieved in the Delegated Administrator user interface by Top-level Administrators.

1. Login as a top-level administrator and click the Configuration tab.
2. Click the Initialize Counters button in the Initialize Counters section of the Configuration tab interface.
3. The Initializing Counters window appears and completes the initialization task.
4. When the task is complete, click Close.

   If for any reason you do not want to continue the initialization process it may be interupted by clicking the Stop or Stop and Close buttons at the bottom of the Initializating Counters window.

Configuring Delegated Administrator for Other Tree Structures

Delegated Administrator is flexible in the range of Directory Information Tree (DIT) structures that it can manage. By creating or modifying entries in the configuration stored in the directory under the `cn=objects,cn=servletsconf` node, you can configure Delegated Administrator to work with your existing user directory. You can specify this configuration for the root level so that it applies to objects in all organizations, or for an organization level so that different organizations can have different object definitions.

This appendix provides general information to help you define the configuration that best describes your DIT structure. In most cases, changing one of the attribute values in an entry described here will not produce a change in the existing objects of that type. However, new objects will conform to the new definition (content and location).

NOTE The updates to user data described in this appendix require advanced experience with Netscape Directory Server, the LDAP Data Interchange Format (LDIF), and Access Control Instructions (ACIs). For comprehensive documentation on these topics, see the Directory Server Administrator's Guide.

The Delegated Administrator Directory Information Tree (DIT)

The Delegated Administrator configuration for the DIT structure and for the contents of managed objects is located under the cn=objects,cn=servletsconf node. It consists of object definitions where each object type corresponds to an entry in the directory as summarized in Table A-2.

Table A-1 Delegated Administrator objects and directory entries

Object	Type of Directory Entry
ServiceAdminGroup	Top-level Administrator Group
ServiceHelpDeskAdminGroup	Top-level Help Desk Administrator Group
Domain	Organization
DomainAdminGroup	Organization Administrator Group

Table A-1 Delegated Administrator objects and directory entries

Object	Type of Directory Entry
DomainHelpDeskAdminGroup	Organization Help Desk Administrator Group
DomainDeptAdminGroup	Department Administrator Group
UsersOrgUnit	Subtree containing users
DeptsOrgUnit	Subtree containing groups
Department	Non-administrator group
DeptAdminGroup	Department Administrator Group
User	User

You can modify these object definitions to include information that matches your directory tree. Some examples:

- A list of objectclasses that should be added when an entry of this type is created
- A list of attributes that should get added by default when an object of this type created.
- Required attributes
- The RDN to use for this entry (For example, whether a User entry should use `cn=bill` or `uid=bill`.)
- A list of other objects that should automatically get created as child entries under this object when it is created.
- The parent DN under which to create this object.

Defining Object Types

Delegated Administrator lets you modify existing objects as well as define new ones. The default object type definition for User is shown below.

```
dn: cn=User, cn=objects, cn=servletsconf, cn=en,
 cn=domainConfiguration, ou=config, o=ISP
objectclass: top
objectclass: extensibleObject
cn: User
iDAobjectclass: top
iDAobjectClass: person
iDAobjectClass: organizationalPerson
iDAobjectClass: inetOrgPerson
iDAobjectClass: mailRecipient
iDAobjectClass: nsMessagingServerUser
iDAobjectClass: nsManagedPerson
iDArequiredAttribute: cn
iDArequiredAttribute: sn
iDArequiredAttribute: uid
iDArequiredAttribute: userPassword
iDAattribute: nsdadomain $DomainContainerName$
iDAattribute: owner $ThisDeptAdminGroupDN$
iDArdnAttribute: uid
iDAdataTypeIdent: enduser
iDAsearchFilter: objectClass=nsManagedPerson
iDAparentDN: "ou=People, $DomainContainerDN$"
```

The syntax for defining an object is:

```
[ object <OBJ_NAME> { [ <KEY_SINGLE_VALUE> | <KEY_MULTI_VALUE> ]*
} ]*
<OBJ_NAME> : [ascii-characters]*
<KEY_SINGLE_VALUE> : <SINGLE_KEY> <SINGLE_VALUE>
<KEY_MULTI_VALUE> : <ATTRIBUTE_KEY_THREE_VALUE>
 <ATTRIBUTE_KEY_FOUR_VALUE>
<SINGLE_KEY> : objectClass | requiredAttribute | rdnAttribute |
 searchFilter | objectToManage
<SINGLE_VALUE> : [ascii-characters]*
<ATTRIBUTE_KEY_THREE_VALUE> : <ATTRIBUTE_KEY> <ATTRIBUTE_NAME>
<ATTRIBUTE_VALUE>
<ATTRIBUTE_KEY_FOUR_VALUE> : <ATTRIBUTE_KEY> <ATTRIBUTE_NAME>
<ATTRIBUTE_VALUE> true
<ATTRIBUTE_KEY> : attribute
<ATTRIBUTE_NAME> : [ascii-characters]*
<ATTRIBUTE_VALUE> : [ascii-characters]*
```

Here’s an example of how you can use ldapmodify to modify an existing object definition. Delegated Administrator uses one container node for all users under each organization. The default name of the container is ou=People. If in your user directory, the container node is cn=Users, you can use ldapmodify to change the definition. In the following example, the definition for ou=People is deleted and then the definition for cn=Users is added to the entry which defines UserOrgUnit.

```
ldapmodify -D "cn=directory manager" -w password -h host_name
dn: cn=UsersOrgUnit, cn=objects, cn=servletsconf, cn=en,
 cn=domainConfiguration, ou=config, o=isp
changetype: modify
delete: idaattribute
idaattribute: ou "People"
-
add: idaattribute
idaattribute: cn "Users"
```

In the following example, a new object is created for a conference room (using the standard LDAP schema for "room"):

```
dn: cn=ConferenceRoom, cn=objects, cn=servletsconf, cn=en,
 cn=domainConfiguration, ou=config, o=isp
objectclass: top
objectclass: extensibleObject
cn: ConferenceRoom
idaobjectclass: top
idaobjectclass: room
idaattribute: description
idaattribute: roomNumber
idaattribute: seeAlso
idaattribute: telephoneNumber
idardnattribute: cn
idarequiredattribute: cn
idadatatypeident: conferenceroom
idasearchfilter: objectClass=room
idaparentdn: "ou=Rooms, $DomainContainerDN$"
```

Quotation marks. In order to specify values that include white-space characters, you must enclose them in matching quotation marks. This makes it possible to use two sets of quotation marks at once when necessary. Examples:

```
"space separated value"

’another example’

`”yet another quote”`
```

Macros. Some values may be macros. The following macros are defined in Delegated Administrator:

- $ISPDN$
- $DOMAINDN$
- $DEPTDN$
- $USERDN$
- $SELFDN$

Most of these are defined internally by the servlets. Their value can be set by passing new values for the macros to the getPage servlet from the templates.

Table A-2 provides information about object definitions you can modify in Delegated Administrator.

Table A-2 Configurable object definitions in Delegated Administrator

Object Definition	Syntax	Description
iDAobjectClass	`iDAobjectClass <oc>`	objectClass value to add to the entry when creating the entry in the directory. Multiple objectClass values can be specified.
iDArequiredAttribute	`iDArequiredAttribute <attr>`	Attribute values required when creating the entry in the directory. Multiple attribute values can be specified. In the absence of an attribute specified here, the entry will not be created.
iDArdnAttribute	`iDArdnAttribute <attr>`	Attribute to be used as the entry's RDN. Only one attribute can be specified. For example, iDA uses uid as the rdn for the user entries. In order to change the rdn to cn, change the value of iDArdnAttribute in the user definition entry to cn.
iDAsearchFilter	`iDAsearchFilter <filter>`	The search filter to use to find such entries in the directory.
iDAattribute	`iDAattribute <attr> <value> [true]`	Attribute and its default value. Multiple attribute values can be specified. Multi-valued attributes can be defined by using the same `<attr>` value. By default, the attribute values specified override any user submitted values for these attributes. The optional fourth parameter (true) indicates that the user submitted values should be used in place of the default values.
iDAobjectToManage	`iDAobjectToManage <object>`	Additional object to manage immediately beneath this entry in the DIT.

Table A-2 Configurable object definitions in Delegated Administrator *(Continued)*

Object Definition	Syntax	Description
iDAparentDN	`iDAparentDN <dn>`	The directory entry beneath which the new object should be created. Multiple parent DN values can be specified. The order in which they are specified is significant. The servlet will check each value in order, and the first one to evaluate to non-null will be used as the parent DN. Example: By default, the Delegated Administrator creates users under `ou=People`, `<DOMAINDN>`. If you wanted the users to be created directly under the domain entry instead of under a container (`ou=People`), you would edit the value of this attribute to be `$DomainContainerDN$`.
iDAdataTypeIdent	`iDAparentDN <identifier>`	This defines the identifier used by other configuration entries for locating user/admin types. You would need to set this value for an object that is a new user/administrator type.

Appendix B

Upgrading from Delegated Administrator Version 4.11

This appendix describes modifcations you must make to your directory information tree (DIT) in order to upgrade an existing Netscape Delegated Administrator 4.11 installation to iPlanet Delegated Administrator 4.5. The appendix contains the following topics:

- Changes from Version 4.11 to Version 4.5
- Modifying the User Directory
- Add New Objectclasses and Attributes
- Importing New Configuration Information
- Changing Container Names
- Initializing the Object Counters

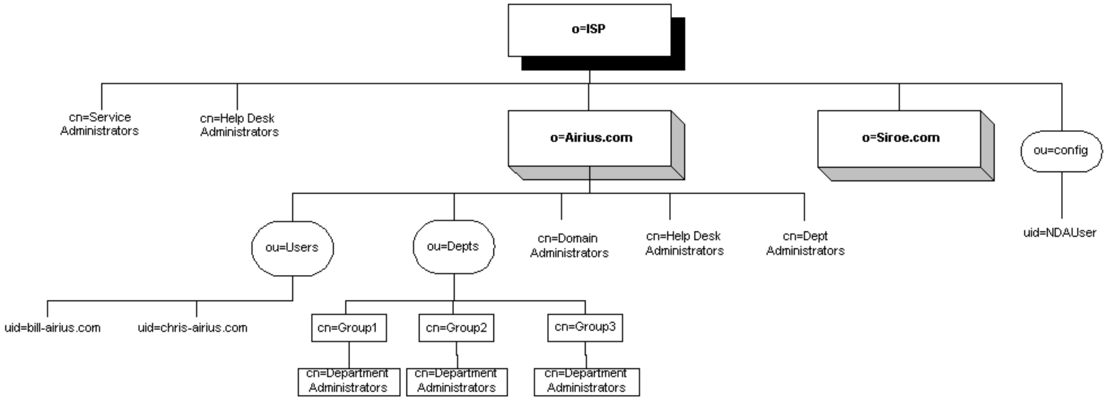
NOTE If your directory data is stored in a in an older version of Netscape Directory Server, you must first upgrade Directory Server to version 4.12 before you make the modifications described in this appendix. For more information, see the documentation for Netscape Directory Server.

Changes from Version 4.11 to Version 4.5

In order to support user directories that are already deployed, Delegated Administrator 4.5 uses a new, highly flexible DIT model. It defines a new grammar that is capable of creating an abstract representation of the user tree which can be interpretted by the back end. By making a few changes in your existing user directory, and representing your existing tree in terms of the new grammar, you can use Delegated Administrator 4.5 to with the user directory you created using version 4.11.

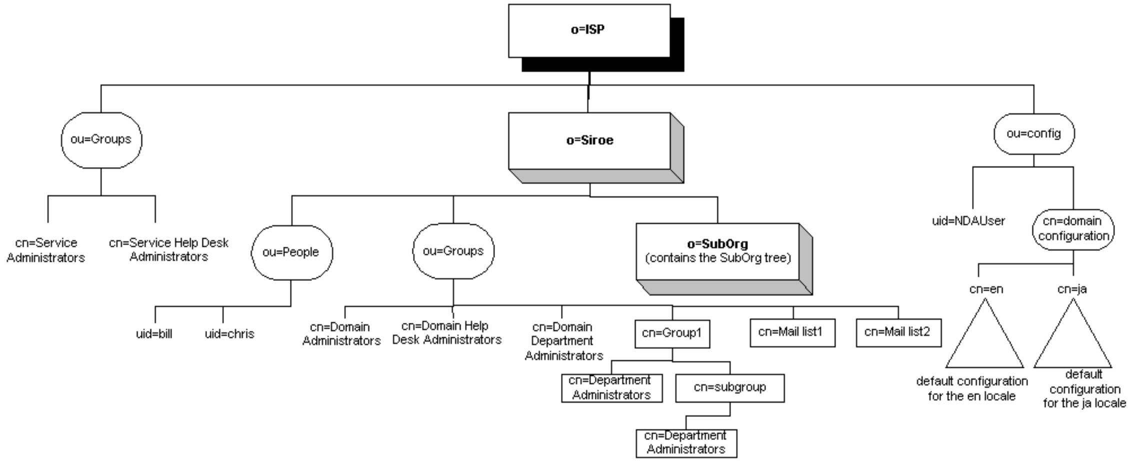
Figure B-1 illustrates the default DIT used in Delegated Administrator 4.11.

Figure B-1 Default DIT used in Delegated Adminstrator 4.11



Changes and additions were necessary to introduce flexibitlity in the support of arbitrary DITs. Figure B-2 illustrates the resulting default DIT used in Delegated Administrator 4.5.

Figure B-2 Default DIT in Delegated Administrator 4.5


o=ISP
ou=Groups
o=Siroe
ou=config
cn=Service Administrators
cn=Service Help Desk Administrators
ou=People
ou=Groups
o=SubOrg
(contains the SubOrg tree)
uid=NDAUser
cn=domain configuration
cn=en
cn=ja
uid=bill
uid=chris
cn=Domain Administrators
cn=Domain Help Desk Administrators
cn=Domain Department Administrators
cn=Group1
cn=Mail list1
cn=Mail list2
cn=Department Administrators
cn=subgroup
cn=Department Administrators
default configuration for the en locale
default configuration for the ja locale

Modifying the User Directory

Before Delegated Administrator 4.5 can work with the administrators created using Delegated Administrtor 4.11, you must modify entries at the Top level and at the Organization level of your existing tree.

Step 1: Modify Entries at the Top Level

1. Rename the top level cn=Help Desk administrators group to `cn=Service Help Desk Administrators`.
2. Create `ou=Groups, <base suffix>`
3. Move the Service Help Desk and Service Administrator Groups to under `ou=Groups, <base suffix>`.
4. Add the `cn=domainConfiguration` tree under `ou=config, <base suffix>`.

Step 2: Modify Entries at the Organization Level

1. Rename `cn=Dept Administrators, <domain dn>` to `cn=Domain Department Administrators, <domain dn>`.
2. Rename `cn=Help Desk administrators` to `cn=Domain Help Desk Administrators`.
3. Move the `cn=Domain Administrators` group, `cn=Domain Help DeskAdministrators` group and the `cn=Domain Department Administrator` group to under `ou=Depts, <domain dn>`

Add New Objectclasses and Attributes

New ACIs, objectclasses, and attributes were added in Delegated Administrator 4.5. Before you install version 4.5, you must modify the following entries created by Delegated Administator 4.11:

- The Top-level entry
- All Organization entries
- The NDAUser entry
- All Administrator Group entries
- All OrgUnit entries
- All Department or Group entries
- All User entries

Step 1: Modify the Top-level Entry

1. Add the new Top Level ACI replacing the old.

   If you had made changes to the original Delegated Adminisstrator 4.11 ACIs, you may need to make corresponding changes in the new set for iDA4.5. The following ACIs need to be added at the Top Level :

```
# Allow anonymous read and search access to user entries
#
aci: (targetattr != “userPassword”)
 (targetfilter=(objectClass=nsManagedPerson))
 (version 3.0; acl “Anonymous access to User entries”;
 allow (read,search) userdn=”ldap:///anyone”;)
#
# Allow anonymous read and search access to postmaster entry
#
aci: (target=”ldap:///cn=postmaster, o=ISP”)
 (targetattr=”*”)
 (version 3.0; acl “Anonymous access to Postmaster entry”;
 allow (read,search) userdn=”ldap:///anyone”;)
#
# ------------------------------------------------
# NDAUser access control
#
# Allow read and search access to uid, mail, and userCertificate
# attributes of user entries
#
aci: (targetattr=”objectClass||uid||mail||userCertificate”)
 (targetfilter=(objectClass=nsManagedPerson))
 (version 3.0; acl “NDAUser access to user attributes”; allow
(read,search)
 userdn=”ldap:///uid=NDAUser, ou=config, o=ISP”;)
#
# Allow read and search access to nsManagedISP entries
#
aci: (targetattr=”objectClass||o||nsNumDomains”)
 (targetfilter=(objectClass=nsManagedISP))
 (version 3.0; acl “NDAUser access to toplevel attributes”; allow
(read,search)
 userdn=”ldap:///uid=NDAUser, ou=config, o=ISP”;)
#
# Allow read and search access to domain entries
#
aci:
(targetattr=”objectClass||o||nsdaorgid||nsNumUsers||nsNumDepts||
nsNum MailLists||nsNumDomains
 ||nsMaxUsers||nsMaxDepts||nsMaxMailLists||nsMaxDomains”)
 (targetfilter=(objectClass=nsManagedDomain))
 (version 3.0; acl “NDAUser access to domain entries”; allow
(read,search)
 userdn=”ldap:///uid=NDAUser, ou=config, o=ISP”;)
```

```
#
# Allow read and search access to department entries
#
aci:
(targetattr=”objectClass||cn||nsNumUsers||nsNumDepts||nsMaxUsers
||ns MaxDepts”)
 (targetfilter=(objectClass=nsManagedDept))
 (version 3.0; acl “NDAUser access to dept entries”; allow
(read,search)
 userdn=”ldap:///uid=NDAUser, ou=config, o=ISP”;)
#
# Allow read and search access to nsManagedOrgUnit entries
#
aci: (targetattr=”objectClass”)
 (targetfilter=(objectClass=nsManagedorgUnit))
 (version 3.0; acl “NDAUser access to orgunits”; allow
(read,search)
 userdn=”ldap:///uid=NDAUser, ou=config, o=ISP”;)
#
# Allow read and search access to mail list entries
#
aci: (targetattr=”objectClass||cn||nsNumUsers||nsMaxUsers”)
 (targetfilter=(objectClass=nsManagedMailList))
 (version 3.0; acl “NDAUser access to mail lists”; allow
(read,search)
 userdn=”ldap:///uid=NDAUser, ou=config, o=ISP”;)
#
# Allow write access to nsNumDomains attribute of nsManagedISP
entries
#
aci: (targetattr=”nsNumDomains”)
 (targetfilter=(objectClass=nsManagedISP))
 (version 3.0; acl “NDAUser write access to toplevel”; allow
(write)
 userdn=”ldap:///uid=NDAUser, ou=config, o=ISP”;)
#
# Allow write access to nsNum* attributes of all domain entries
#
aci:
(targetattr=”nsNumUsers||nsNumDepts||nsNumMailLists||nsNumDomain
s”)
 (targetfilter=(objectClass=nsManagedDomain))
 (version 3.0; acl “NDAUser write access to domains”; allow
(write)
 userdn=”ldap:///uid=NDAUser, ou=config, o=ISP”;)
#
# Allow write access to nsNum* attributes of all department
entries
#
aci: (targetattr=”nsNumUsers||nsNumDepts”)
 (targetfilter=(objectClass=nsManagedDept))
 (version 3.0; acl “NDAUser write access to depts”; allow (write)
 userdn=”ldap:///uid=NDAUser, ou=config, o=ISP”;)
#
```

```
# Allow write access to nsNumUsers attribute of all mail list
entries
#
aci: (targetattr=”nsNumUsers”)
 (targetfilter=(objectClass=nsManagedMailList))
 (version 3.0; acl “NDAUser write access to mail lists”; allow
(write)
 userdn=”ldap:///uid=NDAUser, ou=config, o=ISP”;)
#
# -----------------------------------------------
# Service Administrator access control
#
# Allow read and search access to all ISP nodes
#
aci: (targetattr=”*”)
 (targetfilter=(objectClass=nsManagedISP))
 (version 3.0; acl “SA root node access”; allow (read,search)
 groupdn=”ldap:///cn=Service Administrators, ou=Groups, o=ISP”;)
#
# Allow all access to all domains, organizational units,
departments,
# mail lists and users
#
aci: (targetattr=”*”)
 (targetfilter=(|(objectClass=nsManagedDomain)
 (objectClass=nsManagedOrgUnit)
 (objectClass=nsManagedDeptAdminGroup)
 (objectClass=nsManagedDept)
 (objectClass=nsManagedMailList)
 (objectClass=nsManagedPerson)))
 (version 3.0; acl “SA domain access”; allow (all)
 groupdn=”ldap:///cn=Service Administrators, ou=Groups, o=ISP”;)
#
# -----------------------------------------------
# Service Help Desk Administrator access control
#
# Allow read and search access to all ISP nodes, domains, and
users
#
aci: (targetattr=”*”)
 (targetfilter=(|(objectClass=nsManagedISP)
 (|(objectClass=nsManagedDomain)
 (objectClass=nsManagedPerson))))
 (version 3.0; acl “SHDA root node access”; allow (read,search)
 groupdn=”ldap:///cn=Service Help Desk Administrators, ou=Groups,
o=ISP”;)
#
# Allow all access to all mail lists
#
aci: (targetattr=”*”)
 (targetfilter=(objectClass=nsManagedMailList))
 (version 3.0; acl “SHDA mail list access”; allow (all)
 groupdn=”ldap:///cn=Service Help Desk Administrators, ou=Groups,
o=ISP”;)
#
```

```
# Allow write access to userPassword attribute of all users
except
# Service Administrators and Service Help Desk Administrators
#
aci: (targetattr=”userPassword||passwordExpirationTime”)
 (targetfilter=(&(objectClass=nsManagedPerson)
 (&(!(memberOf=cn=Service Administrators, ou=Groups, o=ISP))
 (!(memberOf=cn=Service Help Desk Administrators, ou=Groups,
o=ISP)))))
 (version 3.0; acl “SHDA user write access”; allow (write)
 groupdn=”ldap:///cn=Service Help Desk Administrators, ou=Groups,
o=ISP”;)
#
# ------------------------------------------------
# Specific Department Administrator access control
#
# Allow read and search access to all depts s/he can view
#
aci: (targetattr=”*”)
 (targetfilter=(|(objectClass=nsManagedDept)
 (objectClass=nsManagedDeptAdminGroup)))
 (version 3.0; acl “Dept Adm dept access”; allow (read,search)
 userdn=”ldap:///o=ISP??sub?(memberOf=cn=Department
Administrators*)” and
 groupdnattr=”ldap:///o=ISP?nsDAModifiableBy”;)
#
# Allow write access to nsNumUsers, nsNumDepts, and uniqueMember
attributes
# of the dept entry s/he can modify
#
aci: (targetattr=”nsNumUsers||nsNumDepts||uniqueMember”)

(targetfilter=(|(objectClass=nsManagedDept)(objectClass=nsManage
dDept)))
 (version 3.0; acl “Dept Adm dept write”; allow (write)
 userdn=”ldap:///o=ISP??sub?(memberOf=cn=Department
Administrators*)” and
 groupdnattr=”ldap:///o=ISP?nsDAModifiableBy”;)
#
# Allow all access to the depts s/he owns
#
aci: (targetattr=”*”)
 (targetfilter=(|(objectClass=nsManagedDeptAdminGroup)
 (objectClass=nsManagedDept)))
 (version 3.0; acl “Dept Adm all access to dept”; allow (all)
 userdn=”ldap:///o=ISP??sub?(memberOf=cn=Department
Administrators*)” and
 groupdnattr=”ldap:///o=ISP?owner”;)
#
# Allow read, search, write and delete access to all users in dept
#
aci: (targetattr=”*”)
 (targetfilter=(&(objectClass=nsManagedPerson)
 (&(!(memberOf=cn=Service Administrators, ou=Groups, o=ISP))
 (&(!(memberOf=cn=Service Help Desk Administrators, ou=Groups,
o=ISP))
 (&(!(memberOf=cn=Domain Administrators*))
 (!(memberOf=cn=Domain Help Desk Administrators*)))))))
 (version 3.0; acl “Dept Adm user access”; allow
(read,search,write,delete)
 userdn=”ldap:///o=ISP??sub?(memberOf=cn=Department
Administrators*)” and g
 roupdnattr=”ldap:///o=ISP?owner”;)
#
# Allow add access to create new users
#
aci: (targetattr=”*”)
 (targetfilter=(objectClass=nsManagedPerson))
 (version 3.0; acl “Dept Adm user create access”; allow (add)
 userdn=”ldap:///o=ISP??sub?(memberOf=cn=Department
Administrators*)”;)
#
# Allow a department administrator to add self to any
group/subgroup that they
# administer
#
aci: (targetattr=”memberOf||owner”) (version 3.0; acl
 “Dept Adm access to add self to group and subgroups”; allow
(write)
 userdn=”ldap:///o=ISP??sub?(memberOf=cn=Department
Administrators*)” and
 userdn=”ldap:///self”;)
#
# ------------------------------------------------
# User access control
#
# Allow read and search access to self
#
aci: (targetattr=”*”)
 (targetfilter=(objectClass=nsManagedPerson))
 (version 3.0; acl “User self read,search”; allow (read,search)
 userdn=”ldap:///self”;)
#
# Allow write access to self except for uid, ou, owner,
# nsDAModifiableBy, nsDACapability, mail, mailAlternateAddress,
# memberOf, and nsDADomain attributes
#
aci:
(targetattr!=”uid||ou||owner||nsDAModifiableBy||nsDACapability
 ||mail||mailAlternateAddress||memberOf||nsDADomain”)
 (targetfilter=(objectClass=nsManagedPerson))
 (version 3.0; acl “User self modification”; allow (write)
 userdn=”ldap:///self”;)
#
# Deny delete access to self
#
aci: (targetfilter=(objectClass=nsManagedPerson))
 (version 3.0; acl “User self deletion”; deny (delete)
 userdn=”ldap:///self”;)
```

```
#
# ------------------------------------------------
# Mail List access control
#
# Allow designated users to create mail lists
#
aci: (targetattr=”*”)
 (targetfilter=(objectClass=nsManagedMailList))
 (version 3.0; acl “Mail list create access”; allow (add)
 userdn=”ldap:///o=ISP??sub?(nsDACapability=mailListCreate)”;)
#
# Allow mail list owner read, search, write, and delete access to
# the mail lists s/he owns except for the nsMaxUsers attribute
#
aci: (targetattr!=”nsMaxUsers”)
 (targetfilter=(objectClass=nsManagedMailList))
 (version 3.0; acl “Mail list owner access”; allow
(read,search,write,delete)
 groupdnattr=”ldap:///o=ISP?owner”;)
#
# ------------------------------------------------
# ------------------------------------------------
#
aci:
(targetattr=”nsNumDomains”)(targetfilter=(objectClass=nsManagedI
SP))(version 3.0; acl “Write Counters”; allow
(write) groupdn=”ldap:///cn=Service Administrators, ou=Groups,
o=ISP”;)
aci: (targetfilter=(objectClass=nsValueItem))(version 3.0; acl
“SA domain access”; allow (all)
groupdn=”ldap:///cn=Service Administrators, ou=Groups,o=ISP”;)
```

2. Add objectclass: nsUniquenessDomain

For more indepth information on iDA 4.5 schema, see Appendix B "Delegated Administrator Schema" in the Deployment and Customization Guide.

Step 2: Modify Each Organization Entry

1. Add the following new attributes with appropriate values for each.

   - nsMaxDomains
   - nsNumDomains
   - nsMaxMailLists
   - nsNumMailLists

2. Remove the following attribute

   nsDefaultMaxDeptSize

3. Add the new Domain Level ACI replacing the old. If you had made ACI changes to the original NDA4.11 ACI at the domain level, you may need to make corresponding changes in the new set for iDA4.5. The following acis need to be added at the domain level :

```
# Allow read and search access to this domain and its subdomains
#
aci: (targetattr=”*”)
 (targetfilter=(objectClass=nsManagedDomain))
 (version 3.0; acl “Domain Adm domain access”; allow
(read,search)
 groupdn=”ldap:///cn=Domain Administrators, ou=Groups, o=Siroe,
o=ISP”;)
#
# Allow read and search access to the Domain Administrators group
#
aci: (target=”ldap:///cn=Domain Administrators, ou=Groups,
o=Siroe, o=ISP”)
 (targetattr=”*”)
 (targetfilter=(|(objectClass=nsManagedDeptAdminGroup)
 (objectClass=nsManagedDept)))
 (version 3.0; acl “Domain Adm dept access”; allow (read,search)
 groupdn=”ldap:///cn=Domain Administrators, ou=Groups, o=Siroe,
o=ISP”;)
#
# Allow read, search, and write access to the Domain Help Desk
# Administrators group
#
aci: (target=”ldap:///cn=Domain Help Desk Administrators,
ou=Groups, o=Siroe, o=ISP”)
 (targetattr=”*”)
 (targetfilter=(|(objectClass=nsManagedDeptAdminGroup)
 (objectClass=nsManagedDept)))
 (version 3.0; acl “Domain Adm dept access”; allow
(read,search,write)
 groupdn=”ldap:///cn=Domain Administrators, ou=Groups, o=Siroe,
o=ISP”;)
#
```

```
# Allow read and search access to this domain and its subdomains
# Allow read, search, and write access to all Domain Department
# Administrators group for Domain and Domain Dept Admins
#
aci: (target=”ldap:///cn=Domain Department Administrators,
ou=Groups, o=Siroe, o=ISP”)
 (targetattr=”*”)
 (targetfilter=(|(objectClass=nsManagedDeptAdminGroup)
 (objectClass=nsManagedDept)))
 (version 3.0; acl “Domain Adm dept access”; allow
(read,search,write)
 groupdn=”ldap:///cn=Domain Administrators, ou=Groups, o=Siroe,
o=ISP” or
  groupdn=”ldap:///cn=Domain Department Administrators,
ou=Groups, o=Siroe, o=ISP”;)
#
# Allow read and search access to all organizational units in this
domain
#
aci: (target=”ldap:///ou=*, o=Siroe, o=ISP”)
 (targetattr=”*”)
 (targetfilter=(objectClass=nsManagedOrgUnit))
 (version 3.0; acl “Domain Adm org unit access”; allow
(read,search,write)
 groupdn=”ldap:///cn=Domain Administrators, ou=Groups, o=Siroe,
o=ISP”;)
#
# Allow all access to the departments and mail lists in this
domain
#
aci: (target=”ldap:///ou=*, o=Siroe, o=ISP”)
 (targetattr=”*”)
 (targetfilter=(|(objectClass=nsManagedDept)
 (objectClass=nsManagedDeptAdminGroup)
 (objectClass=nsManagedMailList)))
 (version 3.0; acl “Domain Adm dept access”; allow (all)
 groupdn=”ldap:///cn=Domain Administrators, ou=Groups, o=Siroe,
o=ISP”;)
#
# Allow read, search, and add access to all users in domain and
subdomains
#
aci: (targetattr=”*”)(targetfilter=(objectClass=nsManagedPerson))
 (version 3.0; acl “Domain Adm user access”; allow
(read,search,add)
 groupdn=”ldap:///cn=Domain Administrators, ou=Groups, o=Siroe,
o=ISP”;)
#
# Allow write and delete access to all users in domain s/he owns
# except for Service Administrators and Service Help Desk
Administrators
#
aci:
(targetattr=”*”)(targetfilter=(&(objectClass=nsManagedPerson)
# Allow read and search access to this domain and its subdomains
 (&(!(memberOf=cn=Service Administrators, ou=Groups, o=ISP))
 (!(memberOf=cn=Service Help Desk Administrators, ou=Groups,
o=ISP)))))
 (version 3.0; acl “Domain Adm user modify access”; allow
(write,delete)
 groupdn=”ldap:///cn=Domain Administrators, ou=Groups, o=Siroe,
o=ISP”;)
#
# Allow all access to subdomains and their organizational units,
# departments, and mail lists
#
aci: (target=”ldap:///o=*, o=Siroe, o=ISP”)
 (targetattr=”*”)
 (targetfilter=(|(objectClass=nsManagedDomain)
 (objectClass=nsManagedDeptAdminGroup)
 (objectClass=nsManagedOrgUnit)
 (objectClass=nsManagedDept)
 (objectClass=nsManagedMailList)))
 (version 3.0; acl “Domain Adm access”; allow (all)
 groupdn=”ldap:///cn=Domain Administrators, ou=Groups, o=Siroe,
o=ISP”;)
aci: (targetfilter=(|(objectClass=nsValueItem)
 (objectClass=extensibleObject)))
 (version 3.0; acl “Domain Adm config access”;
 allow (all) groupdn=”ldap:///cn=Domain Administrators,
ou=Groups, o=Siroe, o=ISP”;)
#
# -------------------------------------------------
# Domain Help Desk Administrator access control
#
# Allow read and search access to this domain, its subdomains, and
all users
#
aci: (targetattr=”*”)
 (targetfilter=(|(objectClass=nsManagedDomain)
 (objectClass=nsManagedPerson)))
 (version 3.0; acl “DHDA access”; allow (read,search)
 groupdn=”ldap:///cn=Domain Help Desk Administrators, ou=Groups,
o=Siroe, o=ISP”;)
#
# Allow all access to all mail lists
#
aci: (targetattr=”*”)
 (targetfilter=(objectClass=nsManagedMailList))
 (version 3.0; acl “DHDA mail list access”; allow (all)
 groupdn=”ldap:///cn=Domain Help Desk Administrators, ou=Groups,
o=Siroe, o=ISP”;)
#
# Allow write access to userPassword attribute of all users in
domain except for
# Service Administrators, Service Help Desk Administrators, and
Domain Administrators
#
```

```
# Allow read and search access to this domain and its subdomains
aci:
(targetattr=”userPassword||passwordExpirationTime”)(targetfilter
=(&(objectClas s=nsManagedPerson)
 (&(!(memberOf=cn=Service Administrators, ou=Groups, o=ISP))
 (&(!(memberOf=cn=Service Help Desk Administrators, ou=Groups,
o=ISP))
 (&(!(memberOf=cn=Domain Administrators, ou=Groups, o=Siroe,
o=ISP))
 (!(memberOf=cn=Domain Help Desk Administrators, ou=Groups,
o=Siroe, o=ISP)))))))
 (version 3.0; acl “DHDA user write access”; allow (write)
 groupdn=”ldap:///cn=Domain Help Desk Administrators, ou=Groups,
o=Siroe, o=ISP”;)
aci: (targetattr=”uniqueMember”)

(targetfilter=(&(objectClass=nsManagedMailList)(mgmanJoinability
=all)))
 (version 3.0; acl “User self subscribe access”; allow
(selfwrite)
 userdn=”ldap:///uid=*, ou=People, o=Siroe, o=ISP”;)
#
# Allow users read and search access to mail lists in their domain
#
aci: (targetattr!=”uniqueMember||mgrpRfc822MailMember”)

(targetfilter=(&(objectClass=nsManagedMailList)(mgmanHidden=fals
e)))
 (version 3.0; acl “User mail list access when visible”; allow
(read,search)
 userdn=”ldap:///uid=*, ou=People, o=Siroe, o=ISP”;)
#
# Allow users read and search access to members of mail lists in
their domain
#
aci: (targetattr=”uniqueMember||mgrpRfc822MailMember”)

(targetfilter=(&(objectClass=nsManagedMailList)(mgmanMemberVisib
ility=all)))
 (version 3.0; acl “User mail list member access”; allow
(read,search)
 userdn=”ldap:///uid=*, ou=People, o=Siroe, o=ISP”;)
```

Step 3: Modify the NDAUser Entry

Set the NDAUser userpassword to auth (default password set in the servlet/resource.properties file). You may want to change this password in both places after installing iDA against the user DIT.

Step 4: Modify Administrator Group Entries

All administrator groups should be modified as follows

1. Add objectclass: nsManagedDeptAdminGroup to the entry.
2. Add objectclass: inetAdmin to the entry.
3. Remove objectclass: nsManagedDept from the entry, if it exists.
4. Add adminRole: <rdn of the Administrative Group entry> e.g.
5. To the Service Administrators group add the attribute -> adminRole: Service Administrators
6. Remove nsNumUsers and nsMaxUsers from the Administrator group entry if they exist.
7. For the Department level Administrator groups, rename the group rdn from cn=Dept Administrators to cn=Department Administrators. Make corresponding changes from Dept to Department in all places where this dn exists as an attribute value.

Step 5: Modify OrgUnit Entries

Add objectclass: nsManagedOrgUnit to the ou=Users & ou=Depts entries.

Step 6: Modify Department or Group Entries

1. Add attributes nsNumDepts & nsMaxDepts with appropriate values to each entry.
2. Change the attribute name ’owner’ to ’nsDAModifiableBy’ and retain the old attribute value.

Step 7: Modify User Entries

Since UID translation is no longer supported in iDA4.5, the uid value in each entry needs to be changed to just the userID without the domain name suffixed to it. Corresponding changes would need to be made in the user tree if UID translation was on. For example:

uid=bill-Airius.com will now become uid=bill.

All references to the user entry would need to be modified accordingly.

1. Change the attribute name ’nssearchfilter’ to ’nsDADomain’ and retain the old attribute value.
2. Change the attribute name ’ou’ to ’memberOf’ and retain the old attribute value.

Importing New Configuration Information

Delegated Administrator 4.5 configuration information, which formerly existed on the file system, has been moved into the directory server. This allows other applications to access the configuration and leverage the DIT structure information. This arrangement also allows other applications to garner additional useful information on predefined search datatypes and other generic parameters from the configuration. Since this information was absent in the NDA4.11 DIT, it needs to be imported into the user tree.

To Import Configuration Changes

1. Change the base suffix from the default value of o=ISP to the appropriate suffix value in each of the ldifs.
2. Download the file config.zip on the download site: http://docs.iplanet.com/docs/manuals/deladmin.html.
3. Import the following LDIF files in the order in which they are listed :
   - config.ldif
   - main.ldif
   - op.ldif
   - macros.ldif
   - servlets.ldif

   For detailed information on importing LDIF files into the directory, see the documentation that comes with Netscape Directory Server.

Changing Container Names

In Delegated Adminstrator 4.11, the container for user entries was ou=Users; the container for group entries was ou=Depts. In version 4.5, the container for user entries is ou=People; the container for group entries is ou=Groups. Before you can use Delegated Administrator 4.5 with entries created under version 4.11, you must reconcile these differences. You can do this using one of two methods. You can change the version 4.11 DIT to match the new container names in version 4.5. This is the recommended method. Or you can change the version 4.5 configuration to match the old container names in the version 4.11 DIT. Consider the size and complexity of your DIT in determining which method to use.

Table B-1 Container names

Container type	Delegated Administrator 4.11	Delegated Administrator 4.5
People	ou=Users	ou=People
Group	ou=Depts	ou=Groups

Step 1: Change the Version 4.11 Container Names

Since it is not possible to simply rename an entry’s DN in the directory, the users & people’s container would need to be repopulated if you use this approach.

1. Change the existing people container (ou=Users) to ou=People.
2. Change the existing groups container (ou=Dept) to ou=Groups.

Step 2: Change the Version 4.5 Container Names

1. Change the iDA4.5 configuration entry for the people container object to use ou=Users.

2. Change the iDA4.5 configuration entry for thegroup container object to use ou=Depts.

   This would need to be done in servlets.ldif before importing it in the above step. The following changes would need to be made:

```
dn: cn=UsersOrgUnit, cn=objects, cn=servletsconf, cn=en,
cn=domainConfiguration,
ou=config, o=ISP
objectclass: top
objectclass: extensibleObject
cn: UsersOrgUnit
iDAobjectclass: top
iDAobjectClass: organizationalUnit
iDAobjectClass: nsManagedOrgUnit
iDArequiredAttribute: ou
iDArdnAttribute: ou
iDAattribute: ou “People”  “Users”
iDAattribute: aci ‘(targetattr!=”userPassword”)
(targetfilter=(objectClass=nsManagedPerson))
(version 3.0; acl “User access to all users in domain”;
allow (read,search) userdn=”ldap:///uid=*, ou=People,
$DomainContainerDN$”;)’ iDAparentDN: $DomainContainerDN$
dn: cn=DeptsOrgUnit, cn=objects, cn=servletsconf, cn=en,
cn=domainConfiguration, ou=config, o=ISP
objectclass: top
objectclass: extensibleObject
cn: DeptsOrgUnit
iDAobjectclass: top
iDAobjectClass: organizationalUnit
iDAobjectClass: nsManagedOrgUnit
iDArequiredAttribute: ou
iDArdnAttribute: ou
iDAattribute: ou “Groups” “Depts”
iDAobjectToManage: DomainAdminGroup
iDAobjectToManage: DomainHelpDeskAdminGroup
iDAobjectToManage: DomainDeptAdminGroup
iDAparentDN: $DomainContainerDN$
```

3. In servlets.ldif and main.ldif, change occurances of People to Users; change occurances of Users to Dept.

4. In the ACIs for at the Top level and at the Organization leve, change all occurances of People to Users; change all occurances of Groups to Depts.

Initializing the Object Counters

Delegated Administrator keeps track of the number of objects in the user data tree such as users, groups, organizations, and mailing lists . After manually making changes to the tree, including the steps above to make an existing tree manageable by Delegated Administrator, the object counters must be initialized. This task is typically performed only by Top-level Administrators.

To Initialize the Object Counters

1. Login as a Top-level administrator and click the Configuration tab.
2. Click the Initialize Counters button in the Initialize Counters section of the Configuration tab interface. The Initializing Counters window appears and completes the initialization task.
3. When the task is complete, click Close. If for any reason you do not want to continue the initialization process it may be interupted by clicking the Stop or Stop and Close buttons at the bottom of the Initializating Counters window.

Appendix C

Delegated Administrator Schema

Schema files are stored in <NSHOME>/slapd-<serverID>/config during installation (where <NSHOME> is the installation directory and <serverID> is the name given to the Directory Server instance).

Modifications to directory object classes are stored in slapd.user_oc.conf. Modifications to directory attributes are stored in slapd.user_at.conf. Modifying other schema files may result in interoperability problems.

The object classes listed in this appendix were designed specifically for use with iPlanet Delegated Administrator 4.5. For a comprehensive listing of all schema supported by Directory Server, refer to the Netscape Directory Server Schema Reference.

This appendix includes the following topics:

- LDAP Overview
- Delegated Administrator Object Classes
- Delegated Administrator Attributes

LDAP Overview

Netscape Directory Server includes object classes and object class attributes defined by the Lightweight Directory Access Protocol (LDAP) and extensions to the standard LDAP schema developed by Netscape and by the Internet Engineering Task Force (IETF) that extend the basic functionality of LDAP.

Initially developed at the University of Michigan, LDAP is a lightweight version of the X.500 Directory Access Protocol (DAP). LDAP has become an Internet standard for directory services that run over TCP/IP.

Netscape Directory Server version 3.0 and later supports LDAPv2 and LDAPv3.

How LDAP Works

One or more LDAP servers contain the data that make up the LDAP directory. An LDAP client connects to an LDAP server and submits a query to request or update directory information. As long as access rights are granted to the client, the LDAP server responds to the query. The LDAP server may also refer the query to another LDAP server for response.

An LDAP directory stores information in object-oriented hierarchies of entries. Each entry is uniquely identified by a distinguished name, or DN. the DN consists of the name of the entry plus a path of names tracing the entry back to the top of the directory hierarchy.

Object Classes

In LDAP, an object class defines the collection of attributes that can be used to define an entry. The LDAP standard provides these basic types of object classes:

- Groups in the directory, including unordered lists of individual objects or groups of objects.
- Locations, such as the country name and description.
- Organizations in the directory.
- People in the directory.

Object Class Inheritance

An entry can belong to more than one object class. For example, the entry for a person is defined by the person object class, but may also be defined by attributes in the inetOrgPerson, groupOfNames, and organization object classes

The server's object class structure (its schema) determines the total list of required and allowed attributes for a particular entry. For example, a person entry is usually defined with the following object class structure:

```
objectClass: top

objectClass: person

objectClass: organizationalPerson

objectClass: inetOrgperson
```

In this structure, the inetOrgperson object class should not be placed on an entry until the person and organizationalPerson object classes have been defined on the entry.

Reserved Object Classes

Reserved schema includes object classes that are essential to software operation but not meant for development purposes and object classes reserved for future use. These object classes are not meant to be used to extend server functionality.

Attributes

Directory data is represented as attribute-value pairs. Any specific piece of information is associated with a descriptive attribute. For instance, the commonName, or cn, attribute is used to store a person's name. A person named Jonas Salk can be represented in the directory as

```
cn: Jonas Salk
```

Each person entered in the directory is defined by the collection of attributes in the person object class. Other attributes used to define this entry could include:

```
givenname: Jonas

surname: Salk

mail: jonass@siroe.com
```

Required and Allowed Attributes

Required attributes include the attributes that must be present in entries using the object class. All entries require the objectClass attribute, which lists the object classes to which an entry belongs.

Allowed attributes include the attributes that may be present in entries using the object class. For example, in the person object class, the cn and sn attributes are required. The description, telephoneNumber, seeAlso, and userpassword attributes are allowed but are not required.

Attribute Syntax

Each attribute has a corresponding syntax definition. The syntax definition describes the type of information provided by the attribute.

Attribute syntax is used by the Directory Server to perform sorting and pattern matching.

Object Identifiers (OIDs)

Object identifiers (OIDs) are assigned to all attributes and object classes to conform to the LDAP and X.500 standards. An OID is a sequence of integers, typically written as a dot-separated string. When no OID is specified, the Directory Server automatically uses <ObjectClass name>-oid.

Table C-1 Base OIDs

Group of Objects	Base OID
Netscape	2.16.840.1.113730
Netscape Directory Server	2.16.840.1.113730.3
All Netscape-defined attributes	2.16.840.1.113370.3.1
All Netscape-defined object classes	2.16.840.1.113730.3.2

Extending Server Schema

The Directory Server schema includes hundreds of object classes and attributes that can be used to meet most Directory Server requirements. This schema can be extended with new object classes and attributes that meet evolving requirements for the directory service in the enterprise.

When adding new attributes to the schema, a new object class should be created to contain them (adding a new attribute to an existing object class can compromise the Directory Server's compatibility with existing LDAP clients that rely on the standard LDAP schema and may cause difficulties when upgrading the server).

For more information about extending server schema, refer to the Netscape Directory Server Deployment Manual.

Schema Checking

iPlanet recommends running the Directory Server with schema checking turned on. Schema checking causes the iPlanet Directory Server to check new entries to verify the following:

- object classes and attributes are defined in the directory schema
- attributes required for an object class are contained in the entry
- only attributes allowed by the object class are contained in the entry

Schema checking also occurs when entries are modified and when importing a database using LDIF. For more information, refer to the iPlanet Directory Server Administration Guide.

Delegated Administrator Object Classes

The following sections provide details for these object classes used by Delegated Administrator:

- inetAdmin
- nsManagedDept
- nsManagedDeptAdminGroup
- nsManagedDomain
- nsManagedFamilyGroup
- nsManagedISP
- nsManagedMailList
- nsManagedOrgUnit
- nsManagedPerson
- nsUniquenessDomain

inetAdmin

Supported by
iPlanet Delegated Administrator 4.5, iPlanet Directory Server 4.12

Definition
Auxiliary class identifying an administrator user or group

Superior Class
top

OID
2.16.840.1.113730.3.2.112

Required Attribute	Description
objectClass	Specifies the objects for this object class

Allowed Attributes	**Description**
memberOf	Specifies the user’s administrator group or department membership.
adminRole	Specifies the Administrator role for this administrator entry.

nsManagedDept

Supported by
Netscape Delegated Administrator 4.0, iPlanet Delegated Administrator 4.5, Netscape Directory Server 4.0

Definition
Stores information for a non-administrator group. Every non-administrator group must contain this objectclass in order to be managed by Delegated Administrator.

Superior Class
groupOfUniqueNames

OID
2.16.840.1.113730.3.2.88

Required Attribute	Description
objectClass	Specifies the objects for this object class

Allowed Attributes	Description
nsNumUsers	Tracks the number of users that can be created under this object.

nsMaxUsers	Specifies the maximum number of users that can be created under this entry.
nsNumDepts	Tracks the number of nested departments that can be created under this object.
nsMaxDepts	Specifies the maximum number of group entries that can be created under this entry.
owner	Identifies the distinguished nam (DN) of the person or group with administrative privileges over this entry.
nsdaModifiableBy	**Specifies who has modify access to the object in which this attribute appears.**

nsManagedDeptAdminGroup

Supported by
Netscape Delegated Administrator 4.0, iPlanet Delegated Administrator 4.5, Netscape Directory Server 4.0

Definition
Stores information for a Group of Administrators.

Superior Class
top

OID
2.16.840.1.113730.3.2.111

Required Attribute	Description
objectClass	Specifies the objects for this object class

Allowed Attributes	**Description**

nsManagedDomain

Supported by
Netscape Delegated Administrator 4.0, iPlanet Delegated Administrator 4.5, Netscape Directory Server 4.0

Definition
Stores information for an organization. All organizations must contain this objectclass in order to be managed by Delegated Administrator.

Superior Class
top

OID
2.16.840.1.113730.3.2.86

Required Attribute	Description
objectClass	Specifies the objects for this object class

Allowed Attributes	Description
nsNumUsers	Tracks the number of users created under this entry.
nsMaxUsers	Specifies the maximum number of users that can be created under this entry.
nsNumDepts	Tracks the number of nested departments that can be created under this object.
nsNumMailLists	Tracks the number of mail lists that can be created below this object or the object.
nsMaxMailLists	Specifies the maximum number of mailing lists that can be created under this entry.
nsNumDomains	Tracks the number of sub-organizations that can be created below this object.
nsMaxDepts	Specifies the maximum number of group entries that can be created under this entry.
nsMaxDomains	Specifies the maximum number of sub-organizations allowed to be created under this entry.
owner	Identifies the distinguished name (DN) of the person or group with administrative privileges over this entry.
nsdaModifiableBy	Specifies who has modify access to the object in which this attribute appears.
nsDefaultMaxDeptSize	

nsManagedFamilyGroup

Supported by

Netscape Delegated Administrator 4.0, iPlanet Delegated Administrator 4.5,

Netscape Directory Server 4.0

Definition

Stores information for a family group managed by a delegated administrator. The family group is like a Group, with a few differences. It has been added primarily to support Delegated Administrator deployments using Sun Internet Message Service (SIMS) 4.0.

Superior Class

top

OID

2.16.840.1.113730.3.2.89

Required Attribute	Description
objectClass	Specifies the objects for this object class

Allowed Attributes	**Description**
nsNumUsers	Tracks the number of users that can be created under this object.
nsMaxUsers	Specifies the maximum number of users that can be created under this entry.

nsManagedISP

Supported by

Netscape Delegated Administrator 4.0, iPlanet Delegated Administrator 4.5,

Netscape Directory Server 4.0

Definition

Specifies the default size (in number of users) of a newly created department managed by delegated administrator. For example: `nsDefaultMaxDeptSize: 20`

Syntax

cis

Superior Class

top

OID

2.16.840.1.113730.3.2.85

Required Attribute	Description
objectClass	Specifies the objects for this object class

Supported by

Netscape Delegated Administrator 4.0, iPlanet Delegated Administrator 4.5,

Netscape Directory Server 4.0

Allowed Attributes	Description
nsNumDomains	Tracks the number of sub-organizations that can be created under this object.

nsManagedMailList

Supported by

Netscape Delegated Administrator 4.0, iPlanet Delegated Administrator 4.5,

Netscape Directory Server 4.0

Definition

Stores information for a mail list created by enabled users. A mail list must contain this objectclass in order to be managed by Delegated Administrator.

Superior Class

top

OID

2.16.840.1.113730.3.2.90

Required Attribute	Description
objectClass	Specifies the objects for this object class

Allowed Attributes	**Description**
nsNumUsers	Tracks the number of users that can be created under this object.
nsMaxUsers	Specifies the maximum number of users that can be created under this entry.
owner	Identifies the distinguished name (DN) of the person responsible for the entry.
nsdaModifiableBy	Specifies who has modify access to the object in which this attribute appears.

nsManagedOrgUnit

Supported by

Netscape Delegated Administrator 4.0, iPlanet Delegated Administrator 4.5,

Netscape Directory Server 4.0

Definition

Stores information for an organizational unit managed.

Superior Class

top

OID

2.16.840.1.113730.3.2.87

Required Attribute	Description
objectClass	Specifies the objects for this object class

Allowed Attributes	**Description**
owner	Identifies the distinguished name (DN) of the person responsible for the entry.
nsdaModifiableBy	Specifies who has modify access to the object in which this attribute appears.

nsManagedPerson

Supported by

Netscape Delegated Administrator 4.0, iPlanet Delegated Administrator 4.5,

Netscape Directory Server 4.0

Definition

Stores information about a user. A user entry must contain this object class in order to be managed by Delegated Administrator.

Superior Class

top

OID

2.16.840.1.113730.3.2.91

Required Attribute	Description
objectClass	Specifies the objects for this object class

Allowed Attributes	**Description**

memberOf	Specifies the user's administrator group or department membership.
nsdaDomain	Specify the user's organization.
nsdaCapability	Specifies whether a user can create a mail list.
owner	Identifies the distinguished name (DN) of the person responsible for the entry.
nsdaModifiableBy	Specifies who has modify access to the object in which this attribute appears.

nsUniquenessDomain

Supported by

Netscape Delegated Administrator 4.0, iPlanet Delegated Administrator 4.5,

Netscape Directory Server 4.0

Definition

This objectclass was used as a marker to identify the subtree where the uniqueness of uid should be enforced. The uid uniqueness plugin uses this to determine the scope or sphere of influence for enforcing uniqueness.

Superior Class

top

OID

2.16.840.1.113730.3.2.115

Required Attribute	Description
objectClass	Specifies the objects for this object class

Delegated Administrator Attributes

The following sections provide details for these attributes used by Delegated Administrator:

- adminRole
- memberof
- nsdaCapability
- nsDADomain
- nsdaModifiableBy
- nsDefaultMaxDeptSize
- nsMaxDepts
- nsMaxDomains
- nsMaxMailLists
- nsNumUsers
- nsMaxUsers
- nsNumDepts
- nsNumDomains
- nsNumMailLists
- nsSearchFilter
- owner

adminRole

Origin
iPlanet Delegated Administrator 4.5

Definition
Specifies the administrator role for this administrator entry.

Syntax
cis

OID
2.16.840.1.113730.3.1.601

memberof

Origin
iPlanet Delegated Administrator 4.5

Definition
Specifies the user's administrator group or department membership.

Syntax
dn

OID
1.2.840.113556.1.2.102

nsdaCapability

Origin
iPlanet Delegated Administrator 4.5

Definition
Specifies whether a user can create a mail list.

Syntax
cis

OID
2.16.840.1.113730.3.1.563

nsDADomain

Origin
iPlanet Delegated Administrator 4.5

Definition
Specify the user's organization.

Syntax
cis

OID
2.16.840.1.113730.3.1.600

nsdaModifiableBy

Origin
iPlanet Delegated Administrator 4.5

Definition
Specifies who has modify access to the object in which this attribute appears.

Syntax
dn

OID
2.16.840.1.113730.3.1.565

nsDefaultMaxDeptSize

Origin
Netscape Delegated Administrator 4.0

Definition
Specifies the default size (in number of users) of a newly created group.

Syntax
int

OID
2.16.840.1.113730.3.1.562

nsMaxDepts

Origin

Netscape Delegated Administrator 4.0

Definition

Specifies the maximum number of group entries that can be created under this entry.

Syntax

int

OID

2.16.840.1.113730.3.1.557

nsMaxDomains

Origin

iPlanet Delegated Administrator 4.5

Definition

Specifies the maximum number of sub-organizations allowed to be created under this entry.

Syntax

int

OID

2.16.840.1.113730.3.1.561

nsMaxMailLists

Origin

iPlanet Delegated Administrator 4.5

Definition

Specifies the maximum number of mailing lists that can be created under this entry.

Syntax

int

OID

2.16.840.1.113730.3.1.559

nsNumUsers

Origin

Netscape Delegated Administrator 4.0

Definition

Identifies the number of user accounts in use in delegated administrator.

Syntax

cis

OID

2.16.840.1.113730.3.1.554

nsMaxUsers

Origin

Netscape Delegated Administrator 4.0

Definition

Specifies the maximum number of users that can be created under this entry.

Syntax

int

OID

2.16.840.1.113730.3.1.555

nsNumDepts

Origin

Netscape Delegated Administrator 4.0

Definition

Tracks the number of nested departments that can be created under this object.

Syntax

int

OID

2.16.840.1.113730.3.1.556

nsNumDomains

Origin

Netscape Delegated Administrator 4.0

Definition

Tracks the number of sub-organizations that can be created under this object.

Syntax

int

OID

2.16.840.1.113730.3.1.560

nsNumMailLists

Origin

iPlanet Delegated Administrator 4.5

Definition

Tracks the number of mail lists that can be created under this object or the object containing this attribute.

Syntax

int

OID

2.16.840.1.113730.3.1.558

nsSearchFilter

Origin

Netscape Delegated Administrator 4.0

Definition

Deprecated.

Syntax

cis

OID

2.16.840.1.113730.3.1.564

owner

Origin

LDAP

Definition

Identifies the distinguished name (DN) of the person or group with administrative privileges over the entry. For example: owner: `cn=John Smith, o=Netscape Communications Corp., c=US`

Syntax

dn

OID

2.5.4.32

Appendix D

Delegated Administrator Access Control Instructions (ACIs)

You may find it necessary to modify the Delegated Administrator access control instructions (ACIs). For example, you may want to expand the access privileges of an existing Group administrator, or to create a new type of administrator. This appendix provides information you'll need to understand the access control framework that comes with Delegated Administrator. It does not provide step-by-step instructions for modifying existing ACIs, or for creating new ones.

NOTE Before attempting to modify Delegated Administrator ACIs, you should have a working knowledge of Directory server ACIs and be proficient in modifying them. For detailed information, see the *Directory Server Administrator's Guide*.

Topics included in this appendix are:

- Overview of Delegated Administrator ACIs
- How Group Administrator ACIs Work
- ACI Implementation and Scalability Issues
- Delegated Admininstrator ACIs Explained
- Tips on Customizing Delegated Administrator ACIs

Overview of Delegated Administrator ACIs

At installation, Delegated Administrator creates directory entries for seven types of administrators:

- NDAUser
  (an internal user used by the iPlanet Delegated Administration for authentication and administrative functions)
- Top-level Administrators
  (formerly Service Administrators)
- Top-level Help Desk Administrators
  (formerly Service Help Desk Administrators)
- Organization Administrators
  (formerly Domain Administrators)
- Organization Help Desk Administrators
  (formerly Domain Help Desk Administrators)
- Group Administrators
  (formerly Department Administrators)
- End Users

Delegated Administrator defines specific access control instructions (ACIs) for each of these administrators. The ACIs determine which directory entries an administrator can modify, as well as the types of modifications the administrator can make to the entries. The tables in the following pages summarize administrators' access privileges to directory entries for the four default Delegated Administrator user containers: the Top-level, Organization, Group, and User Account.

Table D-1 Access to the Top-level entry.

This type of user...	Has the following access privileges to the Top-level entry...					
	Read	**Search**	**Write**	**Add**	**Delete**	**Compare**
NDAUser	limited[1]	limited[2]	limited[3]			
Top-level Administrator	full	full	limited[4]			
Top-level Help Desk Administrator	full	full				
Organization Administrator						
Organization Help Desk Administrator						
Group Administrator						
End User as an Administrator)						
NDAUser						

[1] NDAUser can read only the following objectclasses and attributes: `objectclass, o, nsnumdomains.`

[2] NDAUser can search only the following objectclasses and attributes: `objetclass, o nsnumdomains.`

[3] NDAUser can modify only the following attribute: `nsNumbDomains`

[4] Top-level Help Desk Administrator can modify only the following attribute: `nsnumdomains`

Table D-2 Access to an Organization entry,

This type of user...	Has the following access privileges to the Organization entry...					
	Read	**Search**	**Write**	**Add**	**Delete**	**Compare**
NDAUser	limited[1]	limited[2]	limited[3]			
Top-level Administrator	full	full	full	full	full	full

[1] NDAUser can read only the following objectclasses and attributes: `objectclass, nsdaorgid, nsnum, nsmax, o.`

[2] NDAUser can search only the following objectclasses and attributes: `objectclass, nsdaorgid, nsnum*, nsmax*, o.`

[3] NDAUser can modify only the following attribute: `nsnum*, nsmax*`

[4] Organization administrators have full read and search access privileges to all resources within their organizations; they have write, add, delete, and compare privileges to only resources in their suborganizations.

Table D-2 Access to an Organization entry,

This type of user...	Has the following access privileges to the Organization entry...					
	Read	**Search**	**Write**	**Add**	**Delete**	**Compare**
Top-level Help Desk Administrator	full	full				
Organization Administrator	full	full	limited[4]	limited[4]	limited[4]	limited[4]
Organization Help Desk Administrator	full	full				
Group Administrator						
End User as an Administrator)						

[1] NDAUser can read only the following objectclasses and attributes: `objectclass, nsdaorgid, nsnum, nsmax, o.`

[2] NDAUser can search only the following objectclasses and attributes: `objectclass, nsdaorgid, nsnum*, nsmax*, o.`

[3] NDAUser can modify only the following attribute: `nsnum*, nsmax*`

[4] Organization administrators have full read and search access privileges to all resources within their organizations; they have write, add, delete, and compare privileges to only resources in their suborganizations.

Table D-3 Access to a Group entry.

This type of user...	Has the following access privileges to a Group entry...					
	Read	**Search**	**Write**	**Add**	**Delete**	**Compare**
NDAUser	limited[1]	limited[2]	limited[3]			
Top-level Administrator	full	full	full	full	full	full
Top-level Help Desk Administrator	full	full				
Organization Administrator	full	full	full	full	full	full
Organization Help Desk Administrator						

[1] NDAUser can read only the following objectclasses and attributes: `objectclass, cn, nsnumusers, nsmaxusers, nsnumdepts, nsmaxdepts.`

[2] NDAUser can search on only the following objectclasses and attributes: `objectclass, cn, nsnumusers, nsmaxusers, nsnumdepts, nsmaxdepts.`

[3] NDAUser can modify only the following attribute values: `nsnumusers, nsnumdepts.`

Table D-3 Access to a Group entry.

This type of user...	Has the following access privileges to a Group entry...					
	Read	Search	Write	Add	Delete	Compare
Group Administrator	full	full	full			
End User (as an Administrator)						

[1] NDAUser can read only the following objectclasses and attributes: `objectclass, cn, nsnumusers, nsmaxusers, nsnumdepts, nsmaxdepts.`

[2] NDAUser can search on only the following objectclasses and attributes: `objectclass, cn, nsnumusers, nsmaxusers, nsnumdepts, nsmaxdepts.`

[3] NDAUser can modify only the following attribute values: `nsnumusers, nsnumdepts.`

Table D-4 Access to a User Account entry.

This type of user...	Has the following access privileges to a User Account entry...					
	Read	Search	Write	Add	Delete	Compare
NDAUser	limited[1]	limited[2]	limited[3]			
Top-level Administrator	full	full	full	full	full	full
Top-level Help Desk Administrator	full	full	limited[4]			

[1] NDAUser can read only the following objectclasses and attributes: `objectclass, uid, mail, userCertificate`

[2] NDAUser can search only the following objectclasses and attributes: `objectclass, uid, mail, userCertificate`

[3] NDAUser can modify only the following attribute: `nsnumusers, nsmaxusers.`

[4] Top-level Help Desk Administrator can modify passwords for all users within the top level except for the Top-level administrator.

[5] Organization Help Desk Administrators can modify passwords for all users within the organization except for Top-level and Organization administrators.

[6] Group Administrators have full access privileges to only user accounts within their own group. For all other users accounts in the organization, the Group administrator has read-only access.

[7] With anonymous access disabled, an End User can read or search entries for all other users in the organization.

[8] With anonymous access disabled, an End User can modify values for all attributes in his or her own entry except for the following: `uid, ou, owner, nDAModifiableBy, nsDACapability, mail, mailAlternate address, memberOf, and nsDADomain`.

Table D-4 Access to a User Account entry.

This type of user...	Has the following access privileges to a User Account entry...					
	Read	**Search**	**Write**	**Add**	**Delete**	**Compare**
Organization Administrator	full	full	full	full	full	full
Organization Help Desk Administrator	full	full	limited[5]			
Group Administrator	full	limited[6]	limited[6]	limited[6]	limited[6]	limited[6]
End User (as an Administrator)[7]	full	full	limited[8]			

[1] NDAUser can read only the following objectclasses and attributes: `objectclass, uid, mail, userCertificate`

[2] NDAUser can search only the following objectclasses and attributes: `objectclass, uid, mail, userCertificate`

[3] NDAUser can modify only the following attribute: `nsnumusers, nsmaxusers.`

[4] Top-level Help Desk Administrator can modify passwords for all users within the top level except for the Top-level administrator.

[5] Organization Help Desk Administrators can modify passwords for all users within the organization except for Top-level and Organization administrators.

[6] Group Administrators have full access privileges to only user accounts within their own group. For all other users accounts in the organization, the Group administrator has read-only access.

[7] With anonymous access disabled, an End User can read or search entries for all other users in the organization.

[8] With anonymous access disabled, an End User can modify values for all attributes in his or her own entry except for the following: `uid, ou, owner, nDAModifiableBy, nsDACapability, mail, mailAlternate address, memberOf, and nsDADomain`.

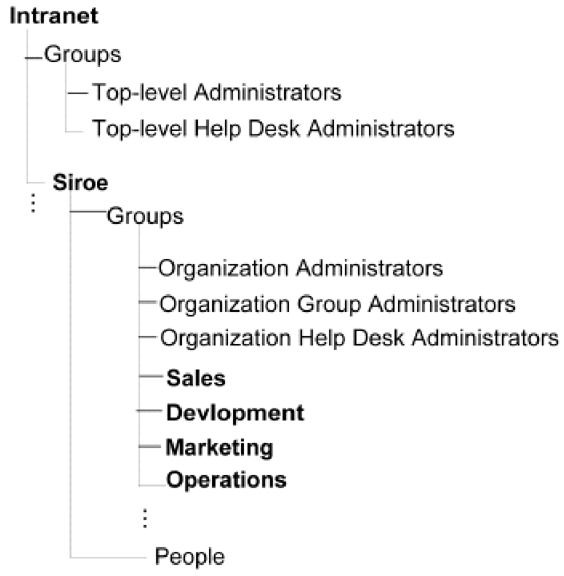
How Group Administrator ACIs Work

Of the seven types of administrators, Group administrators have the most complex set of ACIs. The scenarios in this section illustrate how some of the default ACIs which apply to Group administrators come into play.

ACIs for Adding a User to a Group

The following scenario demonstrates how the Group administrator's ACIs allow him to add a user to many groups. John Doe is a member of the Marketing Division in the Siroe organization. He has just received a promotion to General Manager, and will soon preside over all of the following business divisions: Sales, Development, Marketing, and Operations (see Figure D-1).

Figure D-1 Adding a user to multiple groups.


Intranet
Groups
Top-level Administrators
Top-level Help Desk Administrators
Siroe
Groups
Organization Administrators
Organization Group Administrators
Organization Help Desk Administrators
Sales
Devlopment
Marketing
Operations
People

Doris Dooley is a Group administrator in the Siroe organization. She manages the Delegated Administration group to which John Doe currently belongs, the Marketing group. She also manages the other Delegated Administrator groups that John Doe will soon control: Sales Development, and Operations.

Using Delegated Administrator, Doris adds John Doe to the Sales, Development, and Operations groups.

The following rules are defined in the Group administrator's ACIs, and make it possible for Doris to add John Doe to the three other groups:

- Group Administrators have full access privileges to all users belonging to groups that they are administrators of.
- A Group administrator can manage one or more groups in an organization.
- A user may belong to any number of groups in the organization.
- A Group administrator can add an existing user, one who belongs to a group he or she manages, to any other group he or she manages.

A Group administrator can also create a new user directly into a group he or she manages. For example, Jane Smith is a new employee and will take John Doe's old position in the Marketing Division. Using Delegated Administrator, Doris Dooley navigates to the Marketing group administration page, and creates a new account within the Marketing group for Jane Smith.

Limited Access to Higher-level Administrators

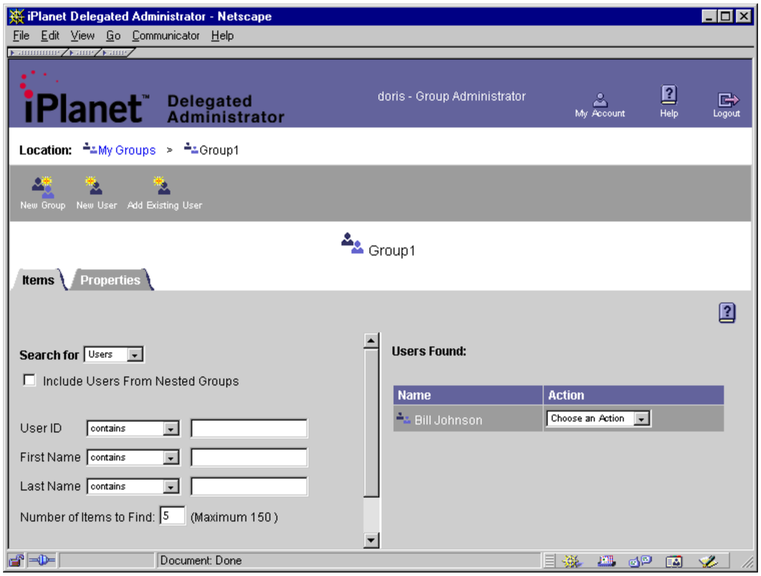
Group administrators have limited access privileges to administrator entries that exist above them in the directory tree. For example, by default, the following administrators exist in the Delegated Administrator tree above Group administrators:

- Top-level Administrators
- Top-level Help Desk Administrators
- Organizational Administrators
- Organizational Help Desk Administrators.

Group administrators cannot modify attribute values in the entries for these users. Group administrators also cannot add these users to, or remove them from, their administrator groups.

ACIs for Modifying Own Entries

Group administrators can manage user accounts within their own groups, and yet they cannot modify some attribute values found within their own user accounts. For example, in the default Siroe organization, Doris Dooley can change the user information for Bill Johnson who is a member of Group 1.



doris - Group Administrator

Location: My Groups > Group1

Group1

Search for Users

□ Include Users From Nested Groups

User ID contains

First Name contains

Last Name contains

Number of Items to Find: 5 (Maximum 150)

Users Found:

Name	Action
Bill Johnson	Choose an Action

Document: Done

As a Group administrator, Doris can use Delegated Administrator to change the values for many attributes in Bill Johnson's directory entry such as, `uid, mail, and mailAlternateAddress.` As an End User, Bill is restricted from modifying the values for these attributes in his own directory entry. These restrictions are defined by the ACIs for End Users (see).

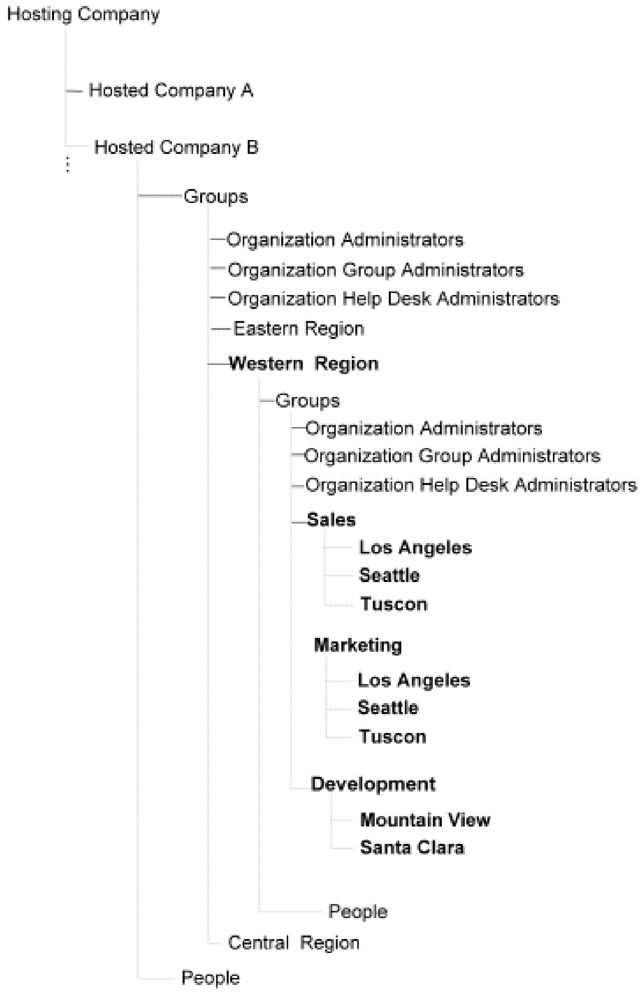
As an End User, Doris is also restricted from changing the values for any of the following attributes found in her own directory entry: `uid, ou, owner, nDAModifiableBy, nsDACapability, mail, mailAlternate address, memberOf, and nsDADomain`. (See .)

Managing Subgroups

Group administrators can create subgroups under the groups they manage. In this scenario, a Group administrator manages three groups named Sales, Marketing, and Development. Under each group, the Group administrator creates two or three subgroups representing office locations. In Figure D-2, the Sales division has employees in Los Angeles, Seattle, and Tuscon offices. Each of the subgroups representing office locations for Sales, Marketing, and Development automatically come under the management of the same Group administrator. He has full ownership, and full access privilges to each of these subgroups. He can also add himself to any of the groups or subgroups he manages.

User Jerry Don physically moves from the Tuscon Sales office to the Los Angeles Sales office. His colleague Mary Doe changes jobs, and transfers from the Tuscon Sales group to the Tuscon Marketing group. The Group Administrator uses Delegated Administrator to remove Jerry Don from the Tuscon Sales group and add him to the Los Angeles Sales group. He then removes Mary Doe from the Tuscon Sales group, and adds her to the Tuscon Marketing group.

Figure D-2 Managing subgroups.



This scenario demonstrates two default ACIs that apply to the Group administrator:

- When a Group administrator creates a subgroup under one of his or her groups, the subgroups automatically come under the Groups administrator's management.
- A Group administrator can add any user from any of the groups under his or her management to a subgroup.

ACI Implementation and Scalability Issues

Delegated Administrator uses iPlanet Directory Server ACIs to define and enforce access control and security for data in the directory tree. As much as possible, Delegated Administrator ACIs have been defined at the root node of the Delegated Administration tree. This increases scalability and allows a larger number of organizations to be supported.

ACIs are defined at the organizational level only when necessary. There are currently 32 ACIs defined at the root node and 17 at the organization level. Out of the 17 at the organization level, 3 ACIs are for mail list management. These can be eliminated if case mailing list management is not essential for deployment.

NOTE The number of ACIs that must be evaluated in the course of any operation impacts Delegated Administrator's performance. iPlanet Directory Server 4.x scales up to 2000 ACIs in the directory tree. If the number of Directory Server ACIs used in a your deployment is very high, and there are more than 150 organizations in the Delegated Administrator tree, you could see a drop in Delegated Administrator's performance. The performance issues may be resolved with the iPlanet Directory Server5.0 . It uses AVL trees instead of linked lists for faster ACI evaluation, and also supports macros in ACIs. This would help move most, if not all, of the Delegated Administrator ACIs to the root node, thus improving scalability immensely.

Top-level Administrators

Service Administrator and Service Help Desk Administrator ACIs are defined at the root node of the Delegated Administrator tree. There is only one Service Administrator group and only one Service Help Desk Administrator group in the entire tree. This makes it possible to define the ACIs using just the `groupdn` to grant these administrators the appropriate access.

Organization Administrators

There are two ways to define ACIs for administrators at the organization level. One way is to define the ACIs at the organization level, as was done in the previous versions of Delegated Administsrator. This method does not require frequent or numerous changes. But a consequence of using this approach is lower performance. If the Delegated Administrator tree must support thousands of organizations, the Directory server must evaluate tens of thousands of ACIs and performanc will slow considerably. The alternative is to make use of groups and object owner or object modifiableBy attributes. This method, while immensely more scalable, requires more maintenance. The approach that is used in Delegated Administrator 4.5 is a combination of the two.

For cases such as the End User read and search access to other users in the organization, which require a huge group membership, the first approach of defining a organization specific ACI was used. In addition, the first approach was also used to eliminate the need for nsDAModifiableBy and owner attributes as much as possible.

The more scalable approach of administrator groups and object owner attributes was used for Groups, Group Administrator groups, and Group members. At the organization level, users can belong to one of three administrator groups: Organization Administrators, Organization Help Desk Administrators, and Group Administrators. Users who do not belong to any of these groups are considered to be End Users. Every manageable resource in the organization (groups and users) must have an owner or modifiableBy attribute which specifies who can manage it.

To define the ACI, Delegated Administrator uses the userdn to specify all users who belong to a particular administrator group, and -ed with the groupdnattr. This specifies the administrator group that can manage the object (specified in the owner or the modifiableBy attribute of the object). The userdn attribute is used to limit the number of the users belonging to a particular group. The groupdnattr attribute is used to limit the number of users even more. Only users who belong to the actual administrator group which owns or can modify the targeted object can belong to the group.

There were some special requirements for defining default ACIs in Delegated Administsrator 4.5. The default ACIs use two kinds of access: general modify access and owner access. General modify access is usually a subset of the owner access. For example, in the case of Group Administrators, there are some tasks that all the Group Administrators in the organization should be able to perform, such as adding existing users to their group. There are also some tasks that only the specific Group Administrators in the organization can perform, such as managing the users in their group.

In order to differentiate the capabilities for Group Administrators, two administrator groups are used: one containing the list of all Group Administrators in the organization (organization Department Administrators), and another containing just the Group Administrators for the Group (the actual Group Administrators). The common capabilities for all Group Administrators are defined using the organization Department Administrators group in conjunction with the owner or the nsDAModifiableBy attribute, while specific capabilities for a particular department have been defined using the Group Administrators group along with the owner attribute.

Delegated Admininstrator ACIs Explained

The following section gives a brief explanation of the actual ACIs used in iDA4.5. Explanations are grouped by type of administrator. The top level ACIs are listed first, followed by the organization specific ACI.

Top-level ACIs

The following types of ACIs are defined at the top level of the Delegated Administrator tree:

- Anonymous Access
- NDAUser Access
- Top-level Administrator Access
- Service Help Desk Administrators Access
- Group Administrator Access Control
- User Access
- Mail List access

Anonymous Access

The following ACI allows anonymous read and search access to all user entries. Anonymous access may be required by some applications to search for one or more entries prior to binding as one of them. Certain deployments may not want to expose directory data except to authenticated users with appropriate access. In such cases you may want to remove this ACI. A script (anon.ldif) is provided in the product to help do this. For more information, see “Step 9: (Optional) Disable Anonymous Access to Your User Tree” on page 64.

The following aci allows anonymous read and search access to postmaster entry. This aci is needed for the Netscape Messaging Server.

```
aci: (target=”ldap:///cn=postmaster, o=ISP”)
     (targetattr=”*”)
     (version 3.0; acl “Anonymous access to Postmaster entry”;
      allow (read,search) userdn=”ldap:///anyone”;)
```

NDAUser Access

The Authentication Administrator is a user entry, `uid=NDAUser`, stored under `ou=config` in Directory Server. Its special purpose is to act as an agent for Delegated Administrator, binding to the directory during authentication when necessary.

The following ACI grants the Authentication Administrator read and search access to the indicated attributes of users in the Delegated Administrator tree for `uid` resolution.

```
aci: (targetattr=”objectClass||uid||mail||userCertificate”)
     (targetfilter=(objectClass=nsManagedPerson))
     (version 3.0; acl “NDAUser access”; allow (read,search)
     userdn=”ldap:///uid=NDAUser, ou=config, o=ISP”;)
```

The following aci grants the NDAUser access to the relevant attributes of the root node.

```
aci: (targetattr=objectClass||o||nsNumDomains)
     (targetfilter=(objectClass=nsManagedISP))
     (version 3.0; acl NDAUser access to toplevel attributes;
     allow (read,search) userdn=ldap:///uid=NDAUser,
     ou=config, o=ISP;)
```

The following ACI grants the NDAUser read and search access to the indicated attributes of organizations in the iDA DIT.

```
aci: (targetattr=”objectClass||o||nsdaorgid||nsNumUsers
     ||nsNumDepts||nsNumMailLists||nsNumDomains
     ||nsMaxUsers||nsMaxDepts||nsMaxMailLists||nsMaxDomains”)
     (targetfilter=(objectClass=nsManagedDomain))
     (version 3.0; acl “NDAUser access to domain entries”;
     allow (read,search) userdn=”ldap:///uid=NDAUser,
     ou=config, o=ISP”;)
```

The following ACI grants the Authentication Administrator read and search access to the indicated attributes of groups in the iDA DIT.

```
aci:
(targetattr=”objectClass||cn||nsNumUsers||nsNumDepts||nsMaxUsers
||nsMaxDepts”)
     (targetfilter=(objectClass=nsManagedDept))
     (version 3.0; acl “NDAUser access to dept entries”;
     allow (read,search) userdn=”ldap:///uid=NDAUser,
     ou=config, o=ISP”;)
```

The following ACI grants the NDAUser read and search access to the indicated attributes of organization units in the iDA DIT.

```
aci: (targetattr=”objectClass”)
     (targetfilter=(objectClass=nsManagedorgUnit))
     (version 3.0; acl “NDAUser access to orgunits”;
     allow (read,search) userdn=”ldap:///uid=NDAUser,
     ou=config, o=ISP”;)
```

The following ACI grants the NDAUser read and search access to the indicated attributes of mailing lists in the iDA DIT.

```
aci: (targetattr=”objectClass||cn||nsNumUsers||nsMaxUsers”)
     (targetfilter=(objectClass=nsManagedMailList))
     (version 3.0; acl “NDAUser access to mail lists”;
     allow (read,search) userdn=”ldap:///uid=NDAUser,
     ou=config, o=ISP”;)
```

The following ACI grants the NDAUser write access to the indicated attribute of the iDA base entry.

```
aci: (targetattr=”nsNumDomains”)
     (targetfilter=(objectClass=nsManagedISP))
     (version 3.0; acl “NDAUser write access to toplevel”;
     allow (write) userdn=”ldap:///uid=NDAUser,
     ou=config, o=ISP”;)
```

The following ACI allows write access to nsNum* attributes of all domain entries.

```
aci:
(targetattr=”nsNumUsers||nsNumDepts||nsNumMailLists||nsNumDomain
s”)
     (targetfilter=(objectClass=nsManagedDomain))
     (version 3.0; acl “NDAUser write access to domains”;
     allow (write) userdn=”ldap:///uid=NDAUser,
     ou=config, o=ISP”;)
```

The following ACI grants the NDAUser write access to the indicated attributes of departments in the iDA DIT.

```
aci: (targetattr=”nsNumUsers||nsNumDepts”)
     (targetfilter=(objectClass=nsManagedDept))
     (version 3.0; acl “NDAUser write access to depts”;
     allow (write) userdn=”ldap:///uid=NDAUser,
     ou=config, o=ISP”;)
```

The following ACI grants the NDAUser write access to the indicated attributes of Mailing Lists in the iDA DIT.

```
aci: (targetattr=”nsNumUsers”)
     (targetfilter=(objectClass=nsManagedMailList))
     (version 3.0; acl “NDAUser write access to mail lists”;
     allow (write) userdn=”ldap:///uid=NDAUser,
     ou=config, o=ISP”;)
```

Top-level Administrator Access

The following ACI grants Top-level administrators read and search access to the `nsManagedISP` objects in the the base entry of the Delegated Administrator tree.

```
aci: (targetattr=”*”)
     (targetfilter=(objectClass=nsManagedISP))
     (version 3.0; acl “SA root node access”;
     allow (read,search) groupdn=”ldap:///cn=Service
     Administrators, ou=Groups, o=ISP”;)
```

The following ACI grants Service Administrators all access to all indicated objects in the NDA DIT.

```
aci: (targetattr=”*”)
     (targetfilter=(|(objectClass=nsManagedDomain)
     (objectClass=nsManagedOrgUnit)
     (objectClass=nsManagedDeptAdminGroup)
     (objectClass=nsManagedDept)
     (objectClass=nsManagedMailList)
     (objectClass=nsManagedPerson)))
     (version 3.0; acl “SA domain access”;
     allow (all) groupdn=”ldap:///cn=Service
     Administrators, ou=Groups, o=ISP”;)
```

Service Help Desk Administrators Access

The following ACI grants Top-level administrators read and search access to the Delegated Adminitrator base entry, all organizations, and all users in the Delegated Administrator tree.

```
aci: (targetattr=”*”)
     (targetfilter=(|(objectClass=nsManagedISP)
     (|(objectClass=nsManagedDomain)
     (objectClass=nsManagedPerson))))
     (version 3.0; acl “SHDA root node access”;
     allow (read,search) groupdn=”ldap:///cn=Service Help
     Desk Administrators, ou=Groups, o=ISP”;)
```

The following ACI grants Top-level Help Desk administrators complete access to Mail Lists entries.

```
aci: (targetattr=”*”)
     (targetfilter=(objectClass=nsManagedMailList))
     (version 3.0; acl “SHDA mail list access”;
     allow (all) groupdn=”ldap:///cn=Service Help
     Desk Administrators, ou=Groups, o=ISP”;)
```

The following ACI grants Top-level Help Desk administrators write access to the `userPassword` attribute of all users in the Delegated Adminitrator tree except forusers who are Top-level administrators or Top-level Help Desk Administrators. Note that the End User ACI, which grants access to attributes for self, allows Service Help Desk Administrators to modify their own passwords.

```
aci: (targetattr=”userPassword”)
     (targetfilter=(&(objectClass=nsManagedPerson)
     (&(!(memberOf=cn=Service Administrators, ou=Groups, o=ISP))
     (!(memberOf=cn=Service Help Desk Administrators,
     ou=Groups, o=ISP)))))(version 3.0; acl “SHDA user write
     access”; allow (write) groupdn=”ldap:///cn=Service Help
     Desk Administrators, ou=Groups, o=ISP”;)
```

Group Administrator Access Control

The following ACI grants Group administrators read and search access to the groups they can modify. Usually, these groups are the ones they did not create, for example Top-level groups versus subgroups.

```
aci: (targetattr=”*”)
     (targetfilter=(|(objectClass=nsManagedDept)
     (objectClass=nsManagedDeptAdminGroup)))
     (version 3.0; acl “Dept Adm dept access”;
     allow (read,search) userdn=”ldap:///o=ISP??sub?
     (memberOf=cn=Department Administrators*)” and
     groupdnattr=”ldap:///o=ISP?nsDAModifiableBy”;)
```

The following ACI allows write access to `nsNumUsers`, `nsNumDepts`, and `uniqueMember` attributes of the group entry a Group administrator can modify

```
aci: (targetattr=”nsNumUsers||nsNumDepts||uniqueMember”)
     (targetfilter=(|(objectClass=nsManagedDept)
     (objectClass=nsManagedDept)))(version 3.0; acl
     “Dept Adm dept write”; allow (write) userdn=
     “ldap:///o=ISP??sub?(memberOf=cn=Department
     Administrators*)” and groupdnattr=”ldap:///o=
     ISP?nsDAModifiableBy”;)
```

The following ACI grants Department Administrators complete access to the groups that they create or subgroups of the groups that they are owners of.

```
aci: (targetattr=”*”)
     (targetfilter=(|(objectClass=nsManagedDeptAdminGroup)
     (objectClass=nsManagedDept))) (version 3.0; acl
     “Dept Adm all access to dept”; allow (all)
     userdn=”ldap:///o=ISP??sub?(memberOf=cn=Department
     Administrators*)” and groupdnattr=”ldap:///o=ISP?owner”;)
```

The following ACI allows read, search, write and delete access to all users in dept except other administrators.

```
aci: (targetattr=”*”)
     (targetfilter=(&(objectClass=nsManagedPerson)
     (&(!(memberOf=cn=Service Administrators, ou=Groups, o=ISP))
     (&(!(memberOf=cn=Service Help Desk Administrators,
     ou=Groups, o=ISP))(&(!(memberOf=cn=Domain Administrators*))
     (!(memberOf=cn=Domain Help Desk Administrators*)
     (!(memberOf=cn=Domain Department Administrators*))))))))
     (version 3.0; acl “Dept Adm user access”; allow (read,
     search, write,delete) userdn=”ldap:///o=ISP??sub?
     (memberOf=cn=Department Administrators*)” and
     groupdnattr=”ldap:///o=ISP?owner”;)
```

The following ACI allows a Group Administrator add access to create new users.

```
aci: (targetattr=”*”)
     (targetfilter=(objectClass=nsManagedPerson))
     (version 3.0; acl “Dept Adm user create access”;
     allow (add) userdn=”ldap:///o=ISP??sub?(memberOf=
     cn=Department Administrators*)”;)
```

The following ACI allows a Group Administrator to add self to any group/subgroup that they administer.

```
aci: (targetattr=”memberOf||owner”) (version 3.0; acl
     “Dept Adm access to add self to group and subgroups”;
     allow (write) userdn=”ldap:///o=ISP??sub?(memberOf=
     cn=Department Administrators*)” and userdn=”ldap:///self”;)
```

User Access

The following ACI provides users in Delegated Administrator tree the ability to read and search their own entry.

```
aci: (targetattr=”*”)
      (targetfilter=(objectClass=nsManagedPerson))
      (version 3.0; acl “User self read,search”;
      allow (read,search) userdn=”ldap:///self”;)
```

The following ACI grants all users in the NDA DIT with the ability to update any of their attributes except for the indicated attributes.

```
aci: (targetattr!=”uid||ou||owner||nsDAModifiableBy
     ||nsDACapability ||mail||mailAlternateAddress
     ||memberOf||nsDADomain”) targetfilter=(objectClass=
     nsManagedPerson)) (version 3.0; acl “User self
     modification”; allow (write) userdn=”ldap:///self”;)
```

The following ACI denies all users in the NDA DIT the ability to delete their own entry.

```
aci: (targetfilter=(objectClass=nsManagedPerson))
     (version 3.0; acl “User self deletion”; deny (delete)
     userdn=”ldap:///self”;)
```

Mail List access

The following ACI allows all designated users to create mail lists. Users can create a mailing lists if their entries contain an attribute `nsdacapability` with a value of `mailListCreate`.

```
aci: (targetattr=”*”)
     (targetfilter=(objectClass=nsManagedMailList))
     (version 3.0; acl “Mail list create access”;
     allow (add) userdn=”ldap:///o=ISP??sub?
     (nsDACapability=mailListCreate)”;)
```

The following ACI allows an owner of a mail list to read, search, write, and delete the mail lists he or she owns, with one exception. An owner cannot change the nsMaxUsers value for the mail list once it has been created.

```
aci: (targetattr!=”nsMaxUsers”)
     (targetfilter=(objectClass=nsManagedMailList))
     (version 3.0; acl “Mail list owner access”;
     allow (read,search,write,delete) groupdnattr=
     “ldap:///o=ISP?owner”;)
```

Organization-level ACIs

The following ACIs are defined at the organization level; they exist for every organization and suborganization created. You might be able to optimize the number of ACIs required at this level based on your deployment requirements. If you must modify existing ACIs, you should create a sufficient number of ACIs to enforce the required access control, but at the same to time to keep the number to a minimum in order to ensure optimal performance.

- The following are the types of ACIs defined at the organization level:
- Organization Administrator Access Control
- Organization Help Desk Administrator Access Control
- Mailing List access control
- User access control

Organization Administrator Access Control

The following ACI allows an organization administrator read and search access to this organization and its suborganization entries.

```
aci: (targetattr=”*”)
     (targetfilter=(objectClass=nsManagedDomain))
     (version 3.0; acl “Domain Adm domain access”;
     allow (read,search) groupdn=”ldap:///cn=Domain
     Administrators, ou=Groups, o=Siroe, o=ISP”;)
```

The following ACI allows an organization administrator read and search access to the Domain Administrators group entry.

```
aci: (target=”ldap:///cn=Domain Administrators, ou=Groups,
     o=Siroe, o=ISP”) (targetattr=”*”) (targetfilter=(|
     (objectClass=nsManagedDeptAdminGroup) (objectClass=
     nsManagedDept))) (version 3.0; acl “Domain Adm dept
     access”; allow (read,search) groupdn=”ldap:///cn=Domain
     Administrators, ou=Groups, o=Siroe, o=ISP”;)
```

The following ACI allows an organization administrator read, search, and write access to the Organization Help Desk Administrators group entry.

```
aci: (target=”ldap:///cn=Domain Help Desk Administrators,
     ou=Groups, o=Siroe, o=ISP”) (targetattr=”*”)
     (targetfilter=(|(objectClass=nsManagedDeptAdminGroup)
     (objectClass=nsManagedDept))) (version 3.0; acl
     “Domain Adm dept access”; allow (read,search,write)
     groupdn=”ldap:///cn=Domain Administrators, ou=Groups,
     o=Siroe, o=ISP”;)
```

The following ACI allows read, search, and write access to the Domain Department Administrators group for Organization and Domain DeptAdmins. The Domain Department Administrator Group contains all the group administrators for groups defined at this organization level.

```
aci: (target=”ldap:///cn=Domain Department Administrators,
     ou=Groups, o=Siroe, o=ISP”) (targetattr=”*”)
     (targetfilter=(|(objectClass=nsManagedDeptAdminGroup)
     (objectClass=nsManagedDept))) (version 3.0; acl “Domain
     Adm dept access”; allow (read,search,write)
     groupdn=”ldap:///cn=Domain Administrators, ou=Groups,
     o=Siroe, o=ISP” or groupdn=”ldap:///cn=Domain Department
     Administrators, ou=Groups, o=Siroe, o=ISP”;)
```

The following ACI provides the organizational administrators with read and search access to all organizational units in the organization, Siroe.

```
aci: (target=”ldap:///ou=*, o=Siroe, o=ISP”)
     (targetattr=”*”) (targetfilter=(objectClass=
     nsManagedOrgUnit)) (version 3.0; acl “Domain Adm
     org unit access”; allow (read,search,write)
     groupdn=”ldap:///cn=Domain Administrators,
     ou=Groups, o=Siroe, o=ISP”;)
```

The following ACI provides Organizational administrators with all access to the groups, ’group administrator’ groups and mail lists in the organization, Siroe.

```
aci: (target=”ldap:///ou=*, o=Siroe, o=ISP”)
     (targetattr=”*”)
     (targetfilter=(|(objectClass=nsManagedDept)
     (objectClass=nsManagedDeptAdminGroup)
     (objectClass=nsManagedMailList)))
     (version 3.0; acl “Domain Adm dept access”;
     allow (all) groupdn=”ldap:///cn=Domain Administrators,
     ou=Groups, o=Siroe, o=ISP”;)
```

The following ACI provides the organizational administrators with read, search, and add access to all user entries in the organization and its suborganizations.

```
aci: (targetattr=”*”)(targetfilter=(objectClass=
     nsManagedPerson)) (version 3.0; acl “Domain Adm
     user access”; allow (read,search,add) groupdn=”ldap:///
     cn=Domain Administrators, ou=Groups, o=Siroe, o=ISP”;)
```

The following ACI provides the Organization administrators with write and delete access to all users in domain s/he owns except for Top-level Administrators and Top-level Help Desk Administrators.

```
 aci: (targetattr=”*”)(targetfilter=(&(objectClass=
      nsManagedPerson) (&(!(memberOf=cn=Service Administrators,
      ou=Groups, o=ISP)) (!(memberOf=cn=Service Help Desk
      Administrators, ou=Groups, o=ISP))))) (version 3.0; acl
      “Domain Adm user modify access”; allow (write,delete)
      groupdn=”ldap:///cn=Domain Administrators, ou=Groups,
      o=Siroe, o=ISP”;)
```

The following ACI provides the Organization administrators with all access to suborganizations and their users, organizational units, groups, and mail lists.

```
aci: (target=”ldap:///o=*, o=Siroe, o=ISP”)
     (targetattr=”*”)
     (targetfilter=(|(objectClass=nsManagedDomain)
     (objectClass=nsManagedDeptAdminGroup)
     (objectClass=nsManagedOrgUnit)
     (objectClass=nsManagedDept)
     (objectClass=nsManagedMailList)))
     (version 3.0; acl “Domain Adm access”;
     allow (all) groupdn=”ldap:///cn=Domain Administrators,
     ou=Groups, o=Siroe, o=ISP”;)
```

Organization Help Desk Administrator Access Control

The following ACI provides the organizational help desk administrators with read and search access to this organization, its suborganizations and all users.

```
aci: (targetattr=”*”)
     (targetfilter=(|(objectClass=nsManagedDomain)
     (objectClass=nsManagedPerson)))
     (version 3.0; acl “DHDA access”; allow (read,search)
     groupdn=”ldap:///cn=Domain Help Desk Administrators,
     ou=Groups, o=Siroe, o=ISP”;)
```

The following ACI provides the organizational help desk administrators with all access to all mail lists defined in this organizations and its suborganizations.

```
aci: (targetattr=”*”)
     (targetfilter=(objectClass=nsManagedMailList))
     (version 3.0; acl “DHDA mail list access”; allow (all)
     groupdn=”ldap:///cn=Domain Help Desk Administrators,
     ou=Groups, o=Siroe, o=ISP”;)
```

The following ACI provides the organizational help desk administrators with write access to `userPassword` attribute of all users in organization except for Top-level Administrators, Top-level Help Desk Administrators, Organization Administrators and Organization Help Desk Administrators.

```
aci: (targetattr=”userPassword”)(targetfilter=(&(objectClass=
     nsManagedPerson) (&(!(memberOf=cn=Service Administrators,
     ou=Groups, o=ISP)) (&(!(memberOf=cn=Service Help Desk
     Administrators, ou=Groups, o=ISP)) (&(!(memberOf=cn=Domain
     Administrators, ou=Groups, o=Siroe, o=ISP)) (!(memberOf=cn=
     Domain Help Desk Administrators, ou=Groups, o=Siroe,
     o=ISP))))))) (version 3.0; acl “DHDA user write access”;
     allow (write) groupdn=”ldap:///cn=Domain Help Desk
     Administrators, ou=Groups, o=Siroe, o=ISP”;)
```

Mailing List access control

The following ACI allows all users in this organization to join any mailinglist which is joinable. A mailing list is joinable if it contains an attribute `mgmanJoinability` whose value is set to `all`.

```
aci: (targetattr=”uniqueMember”)
     (targetfilter=(&(objectClass=nsManagedMailList)
     (mgmanJoinability=all))) (version 3.0; acl “User self
     subscribe access”; allow (selfwrite) userdn=”ldap:///uid=*,
     ou=People, o=Siroe, o=ISP”;)
```

The following ACI allows all users read and search access to all visible mail lists in their organization. A mailing list is visible if it contains an attribute mgmanHidden whose value is set to false.

```
aci: (targetattr!=”uniqueMember||mgrpRfc822MailMember”)
     (targetfilter=(&(objectClass=nsManagedMailList)
     (mgmanHidden=false))) (version 3.0; acl “User mail
     list access when visible”; allow (read,search)
     userdn=”ldap:///uid=*, ou=People, o=Siroe, o=ISP”;)
```

The following ACI allows all users read and search access to members of all mail lists whose members’ references are visible in their organization.

```
aci: (targetattr=”uniqueMember||mgrpRfc822MailMember”)
     (targetfilter=(&(objectClass=nsManagedMailList)
     (mgmanMemberVisibility=all))) (version 3.0; acl “User
     mail list member access”; allow (read,search) userdn=”ldap:
     ///uid=*, ou=People, o=Siroe, o=ISP”;)
```

The following ACI allows all members of a restricted mailing list read and search access to all other members of the restricted mailing lists.

```
aci: (targetattr=”uniqueMember||mgrpRfc822MailMember”)
     (targetfilter=(&(objectClass=nsManagedMailList)(mgmanMember
     Visibility=restricted))) (version 3.0; acl “User mail list
     access - group”; allow (read,search) groupdnattr=”ldap:///o=
     ISP?mgmanMemberVisibilityGroup”;)
```

The following ACI allows authenticated or unauthenticated users read and search access to the mailing lists with public access.

```
aci: (targetattr=”uniqueMember||mgrpRfc822MailMember”)
     (targetfilter=(&(objectClass=nsManagedMailList)
     (mgmanMemberVisibility=anyone))) (version 3.0; acl
     “User mail list access - public”; allow (read,search)
     userdn=”ldap:///anyone”;)
```

User access control

The following ACI provides all authenticated users of an organization with read and search access to all attributes except the `userPassword` of other users in the organization .

```
aci: (targetattr!=”userPassword”)(targetfilter=
     (objectClass=nsManagedPerson)) (version 3.0; acl
     “User access to all users in domain”; allow (read,search)
     userdn=”ldap:///uid=*, ou=People, o=Siroe, o=ISP”;)
```

Tips on Customizing Delegated Administrator ACIs

It may be necessary to customize the ACI for your deployment. Since the ACIs are completely externalized from the servlets, the only places where changes need to go are in the appropriate Directory entries. The number of changes that need to be made would depend upon the level at which the ACI changes are being affected.

Adding, removing or modifying ACIs at the top level or the root node are the easiest to do. The changes just need to be made in the Directory entry of the root node.

However, if you make modify ACIs at the organization level, and if the changes must be applied to all organizations that are subsequently created, then you may need to affect these changes in more than one place. For example, when you create a new organization, the default ACIs are picked up from the appropriate node in the appropriate organization configuration subtree. By default, Delegated Administrator uses a default configuration that can be found under the following entry:

```
dn: cn=domainConfiguration, ou=config, o=ISP
```

Once you’ve located the domain configuration subtree, locate the following entry in the subtree:

```
dn: cn=Domain, cn=objects, cn=servletsconf, <domain configuration
subtree DN>
```

Make the necessary ACI modifications using the same ACI form as other ACI-related attributes in this entry.

In order for the ACI changes to take effect, you must do one of the following:

- Restart the Web server.
- Use the Configuration tab in Delegated Administrator to reload the appropriate configuration as a Top level administrator. See Chapter 14, “Customizing Configuration in the Directory” for more information.

Index