Administrator's Guide

Sun^{TM} ONE Directory Proxy Server

Version 5.2

June 2003
816-6391-10

Contents

List of Figures

About This Guide

The *Administrator's Guide* presents various deployment scenarios for Sun™ Open Net Environment (Sun ONE) Directory Proxy Server and explains how to configure and maintain it.

This preface has the following sections:

- Audience for This Guide (page 3)
- What's in This Guide (page 4)
- Conventions Used in This Guide (page 4)
- Related Information (page 5)
- Accessibility Features (page 6)

Audience for This Guide

The Directory Proxy Server Administrator's Guide is written for administrators who will configure and operate one or more servers. This guide assumes that you have the following background:

- A general understanding of the Internet and LDAP.
- A general understanding of Sun ONE Directory Server 5.x and its administration. You should be able to read and modify directory data.

What’s in This Guide

The guide is organized into three parts:

- Part 1, “Introduction to Sun ONE Directory Proxy Server”
- Part 2, “Console Based Administration”
- Part 3, “Appendixes”

Conventions Used in This Guide

This section explains the conventions used in this book.

`Monospaced font`—This typeface is used for any text that appears on the computer screen or text that you should type. It is also used for filenames, functions, and examples.

NOTE	Notes and Cautions mark important information. Make sure you read the information before continuing with a task.

The greater than symbol (>) is used as a separator for successive menu selections. For example, Object > New > User means that you should pull down the Object menu, drag the mouse down to highlight New, and drag the mouse across to the New submenu in which you must select User.

Throughout this book you will see path references of the form:

```
<server-root>/dps-<hostname>/...
```

where `<server-root>` is the default installation directory and `<hostname>` is the name of the host machine in which Directory Proxy Server is installed. For example, if the installation directory is `/usr/sunone/servers` and the hostname of the machine is `testmachine`, the actual path would be:

```
/usr/sunone/servers/dps-testmachine/. . .
```

All paths specified in this manual are in UNIX format. If you are using a Windows NT-based directory server, you should assume the NT equivalent file paths whenever UNIX file paths are shown in this guide.

Related Information

In addition to this guide, the Directory Proxy Server documentation set includes the following:

- **Sun ONE Directory Proxy Server Release Notes.** The release notes contain important information available at the time of the release of Directory Proxy Server. New features and enhancements, known problems, and other late-breaking issues are addressed here. Read this document before you begin using Directory Proxy Server.
- **Sun ONE Directory Proxy Server Installation Guide.** This guide contains procedures for installing Directory Proxy Server plus requirements and tuning information.

Other useful Sun ONE information can be found at the following Internet locations:

- Product documentation on line—`http://docs.sun.com`
- Product support and status—`http://www.sun.com/service/support/software/`
- Sun Enterprise Services for Solaris patches and support—`http://www.sun.com/service/`
- Developer information—`http://www.sun.com/developers/`
- Support and Training—`http://www.sun.com/supportraining`
- Product data sheets—`http://www.sun.com/software/`

Accessibility Features

Based on the the Java^{TM} Foundation Classes (JFC), the Sun ONE Directory Proxy Server console provides support for the assistive software and technologies that make software accessible to users with disabilities. This appendix describes the accessibility features of the Sun ONE Directory Proxy Server console, and the improvements that have been made to the document set to make it more accessible.

Console Accessibility Features

Most of the accessibility features described in the following section are provided automatically through the use of JFC/Swing! components.

Accessible names and descriptions

All objects have accessible names (succinct explanations of the object's purpose). These names can be used by assistive technologies to present the objects to the user. Accessible descriptions are more verbose explanations that provide additional information on objects, where this is necessary.

Customizable fonts

The style and size of fonts in text panes, menus, labels, and information messages, can be customized.

Although color coding is used to convey information, it is not the only means of doing so.

Dynamic GUI layout

The dynamic layout allows users to specify the size and position of Directory Server windows, or for this to be determined by the user's settings.

Keyboard traversable components

This accessibility feature caters for users who have difficulty using a mouse. Pressing the tab key moves the input focus from component to component and shift-tab moves the focus in the opposite direction. The arrow keys allow users to navigate trees without using the mouse.

The focus is programmatically exposed so that assistive software can track focus and focus changes.

Text equivalents for non-text elements

When an image represents a program element, the information conveyed by the image is also available in the text.

Equivalent command-line interface

Most of the functionality of the console can be achieved at the command-line. This command-line interface is comprehensively documented.

Documentation Accessibility Features

The Sun ONE Directory Proxy Server 5.2 document set is delivered in both PDF and HTML format. This section describes accessibility features in the HTML version of the documentation.

Text equivalents for non-text elements

Alternative text labels are assigned to links or graphics. Where graphics provide detailed descriptions, text versions of these descriptions are provided either within the surrounding text, or in a separate file.

Tables that can be interpreted by assistive technology

All tables now include descriptive headers. A brief description of the table contents is also provided in the surrounding text.

Part 1

Introduction to Sun ONE Directory Proxy Server

Chapter 1

Overview of Sun ONE Directory Proxy Server

This chapter introduces you to Sun ONE Directory Proxy Server. The chapter consists of the following sections:

- Introduction (page 11)
- Directory Proxy Server Feature Set (page 13)

Introduction

Sun ONE Directory Proxy Server is an essential component of any mission-critical directory service for e-commerce solutions. Directory Proxy Server is an LDAP application layer protocol gateway that offers enhanced directory access control, schema compatibility, and high availability using application layer load balancing and fail over.

Functionally, Directory Proxy Server is an “LDAP access router” located between LDAP clients and LDAP directory servers. Requests from LDAP clients can be filtered and routed to LDAP directory servers based on rules defined in the Directory Proxy Server configuration. Results from the directory server can be filtered and passed back to clients, again based on rules defined in the Directory Proxy Server configuration. This process is totally transparent to the LDAP clients, which connect to Directory Proxy Server just as they would to any LDAP directory server.

Directory Proxy Server is a unique product that provides high availability, security, and client compatibility features for both extranet and intranet directory infrastructures, including:

- Automatic load balancing

- Transparent server failover and failback
- Automatic referral following
- Extranet/intranet access control groups
- Secure client and server authentication
- Dynamic query and response filtering
- Dynamic schema mapping
- Directory-based or file-based configuration
- Configurable logging

Directory Proxy Server coexists with and complements new and existing LDAP directory infrastructures and integrates seamlessly with directory-enabled applications already deployed in enterprise extranets and intranets. It can be deployed to leverage the existing investment in a customer's directory infrastructure. Directory Proxy Server will inter-operate with any LDAP compliant directory server. Directory Proxy Server will work with any LDAP enabled and conformant directory, whether it's a native LDAP directory, an LDAP enabled X.500 directory, or an LDAP enabled relational database.

Directory Proxy Server implements the LDAPv3 Internet specification and also supports the older and less functional LDAPv2 specification for compatibility with already deployed directory-enabled client applications that use LDAPv2. Directory Proxy Server runs as a separate system server process on UNIX and Windows NT platforms. The server is multi-threaded and can handle thousands of LDAP client requests while applying access control rules and protocol filtering rules to each request.

Directory Proxy Server can help organizations protect their private directory information from unauthorized access, while making it safe for these organizations to publish their public information. Directory Proxy Server can be used to configure a fine-grained, access control policy on LDAP directories, such as controlling who can perform different types of operations on different parts of the Directory Information Tree (DIT). Directory Proxy Server can also be configured to disallow certain kinds of operations typically performed by web trawlers and robots to collect information.

Unlike a web proxy server, Directory Proxy Server operates in a reverse proxy mode. It does not forward connections to arbitrary servers on the Internet from clients inside the firewall. Neither does it cache search results. The predominant reason for this is the problem of applying access controls to the data. This is currently done only in the LDAP directory server where the access controls are maintained. Directory Proxy Server has no knowledge of the directory server access controls.

Directory Proxy Server Feature Set

The Directory Proxy Server feature set provides distinct functions: high availability, load balancing, fail over, firewall-like security, and client-server compatibility.

High Availability

Directory Proxy Server is designed to support high availability directory deployments by providing both automatic load balancing and automatic fail over and fail back among a set of replicated LDAP directory servers. For extranet and intranet environments it is often necessary to ensure that mission-critical directory-enabled clients and applications have 24x7 access to directory data. Directory Proxy Server maintains connection state information for all directory servers that it knows about, and is able to dynamically perform proportional load balancing of LDAP operations across a set of configured directory servers. Should one or more directory servers become unavailable, the load is proportionally redistributed among the remaining servers. When a directory server comes back on line, the load is proportionally reallocated dynamically.

For example, suppose directory server A is configured to receive 40 percent of the LDAP client load, server B 20 percent, server C 20 percent and server D 20 percent. If directory server B fails, Directory Proxy Server will recognize that server A is configured to carry twice the load of servers C and D, and will redistribute the 20 percent load from server B such that server A now receives 50 percent, server C 25 percent and server D 25 percent. When directory server B is recovered, Directory Proxy Server will automatically detect this and revert back to the original load percentages configured across all four servers.

Network layer IP load balancing devices don’t have access to the LDAP protocol layer. However, Directory Proxy Server integrates load balancing with access control, query filtering, and query routing, and can make intelligent application layer access control and LDAP routing decisions.

Load Balancing

Load balancing must be configured in Directory Proxy Server using the load balancing property described in “ids-proxy-sch-LoadBalanceProperty Object Class,” on page 222, or in Chapter 7, “Defining and Managing Property Objects.” Each back-end directory server that Directory Proxy Server can communicate with is configured to receive a percentage of total client load. Directory Proxy Server then automatically distributes client queries to different back-end servers to meet the load criteria defined in the configuration. If a server becomes unavailable, Directory Proxy Server distributes the load percentage of that server proportionally among the available servers based on their load percentage. Directory Proxy Server starts rejecting client queries if all back-end LDAP servers become unavailable.

Load balancing in Directory Proxy Server is session-based. This means that the decision function that chooses a particular server to which a client’s queries will be directed is applied once per client session; in particular, at the start of the client session. All subsequent client queries in that session are directed to the server that was chosen at the beginning of the session.

The number of back-end LDAP servers that Directory Proxy Server can load balance depends on several factors, such as the size of the host running Directory Proxy Server, the network bandwidth available, the query mix that Directory Proxy Server receives, the length of client sessions, and Directory Proxy Server’s configuration. In general, Directory Proxy Server can support fewer servers if most sessions are short lived and queries are computationally intensive. Computationally intensive queries are those that require the inspection of the entire message such as when the attribute renaming feature described in “Attribute Renaming Property,” on page 100 is used.

Directory Proxy Server uses a monitor process to make health checks on its backend servers including those that communicate only through SSL. This feature is automatically enabled if load balancing is used. Directory Proxy Server makes an anonymous search operation for the Root DSE every 10 seconds for each of its backend directory servers. If one of them becomes unavailable or unresponsive, Directory Proxy Server removes it for the active load balanced server set. When the server becomes available again, it is reintroduced in the set.

Failover

Directory Proxy Server detects when a server becomes unavailable either when a connection attempt is returned with a connection refused error or when it times out. Since both these cases occur at the initial stages of the session, and no operations have yet been processed for that session, Directory Proxy Server fails over to another server, provided one is available transparently. In the connect attempt timeout case, the client can experience significant delay in getting a response. If a connection between Directory Proxy Server and a back-end server is abruptly lost, Directory Proxy Server returns LDAP_BUSY error for all outstanding operations to the affected client. Subsequently, Directory Proxy Server fails over that client session to another directory server.

In order to avoid Directory Proxy Server becoming the single point of failure for your directory deployment, we recommend you use at least two Directory Proxy Servers with an IP appliance in front of it.

Security

Directory Proxy Server provides flexible external directory access control facilities that enhance the basic access control provided by a directory server. The access control mechanisms allow different users and communities of users to be associated with specific access groups to which administrator-defined security restrictions and query filters will be applied. The administrator can control access to entries based on LDAP authentication information, IP address, domain name, and other criteria.

A significant security feature that Directory Proxy Server provides is the protection of the number of connections established between LDAP clients and the LDAP directory server. You can protect your LDAP directory server from connection attacks by configuring Directory Proxy Server to monitor a number of specific metrics: the number of simultaneous client operations, the number of operations a client can request per connection, and the number of connections for a particular client group. It also has the ability to time out inactive clients.

You can configure Directory Proxy Server with specific threshold limits not to be exceeded for the given metrics. Directory Proxy Server will monitor these metrics and ensure that the thresholds are not exceeded. Directory Proxy Server keeps several metrics, such as the number of connections open from a particular host, the number of operations performed on a particular session, etc., to limit possible trawling of the directory and denial of service attacks. A detailed description of the configuration of these parameters are in “Creating System Configuration Instances,” on page 57.

Directory Proxy Server also limits trawling by disallowing certain kind of generic filter such as (cn=A*) or (cn>A). More details on how to configure filtering of filters is in Chapter 6, “Creating and Managing Groups.”

Directory Proxy Server allows an authenticated client to change its access control to the directory service. This allows authenticated clients to have greater access to the directory information even if they are outside the secure network.

Directory Proxy Server provides data protection by supporting Secure Socket Layer (SSL) transport protocol. You can, for example, configure Directory Proxy Server so that all clients that access your directory services from outside the protected network are required to establish an SSL session. Details on configuring SSL in Directory Proxy Server is given in “Configuring Security,” on page 149.

These features can help prevent “denial of service” attacks and “flood attacks” that are so commonplace in the industry today. If Directory Proxy Server detects that a threshold has been reached, it will then start refusing connections to the directory server and prevent the directory server from being attacked and overwhelmed.

Client-Server Compatibility

Directory Proxy Server makes query routing decisions based on LDAP Distinguished Names (DNs) and group access rights, including identifying mobile users based on authentication credentials. Directory Proxy Server automatically follows LDAP referrals that may be returned by a directory server, in support of highly distributed and scalable directory services. Automatic referral following is a significant advantage for large-scale directory deployments where you must physically distribute directory information among a set of directory servers, but have the distributed directory appear to users as one logical directory. Directory Proxy Server supports this type of deployment scenario by providing the ability to logically unify otherwise distributed directory data in support of scalable distributed directory services.

Directory Proxy Server supports any compliant LDAPv2 or LDAPv3 client application. Support is provided for schema rewriting to accommodate client applications with fixed schemas that do not always match the directory server’s schema. For example, the Microsoft Outlook™ email client has a fixed schema that expects the directory server to implement Microsoft-defined attributes that may not match an enterprise’s more general schema requirements. The schema rewriting capability allows the directory system administrator to implement a general purpose enterprise schema, and then map specific elements of that schema dynamically into the set of attribute types that are required by the less functional client application. Directory Proxy Server is otherwise schema agnostic and accepts any attribute types and object classes defined by a large set of standard and *ad hoc* industry schema definitions, including RFC1274, X.520, X.521, LIPS, PKIX, inetOrgPerson, and DEN.

Chapter 2

Sun ONE Directory Proxy Server Deployment Scenarios

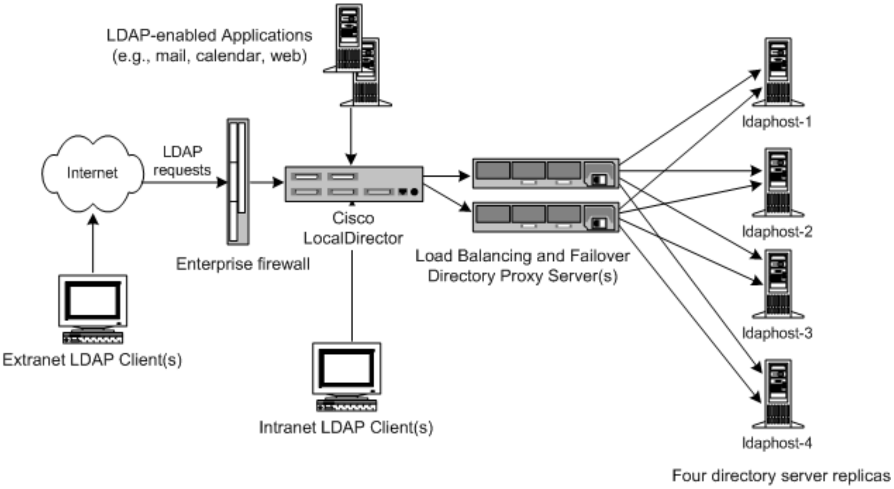
There are several ways you may want to deploy Sun ONE Directory Proxy Server, depending on your computing environment. This chapter describes and illustrates typical deployments, including:

- An Internal High Availability Configuration (page 19)
- A Distributed LDAP Directory Infrastructure (page 20)
- A Centralized LDAP Directory Infrastructure (page 23)
- Deploying Directory Proxy Server with a Single Firewall (page 26)
- Deploying Directory Proxy Server with Two Firewalls (page 28)

An Internal High Availability Configuration

In the configuration shown in Figure 2-1, the customer has deployed an LDAP infrastructure for internal enterprise use only. There is no requirement for external network access to any of the enterprise LDAP services. The customer has deployed an enterprise firewall that will reject any access to internal LDAP services originating from outside the firewall. All client LDAP requests initiated internally must still go through Directory Proxy Server via the Cisco LocalDirector (for high availability), which is shown here only as an example of IP packet switching that ensures clients have access to at least one Directory Proxy Server. The customer prevents direct access to the directory servers by everyone except the hosts running Sun ONE Directory Proxy Servers; this can be achieved by using firewalls to protect the hosts running the directory server and Directory Proxy Server.

Figure 2-1 Internal High Availability Configuration



A Distributed LDAP Directory Infrastructure

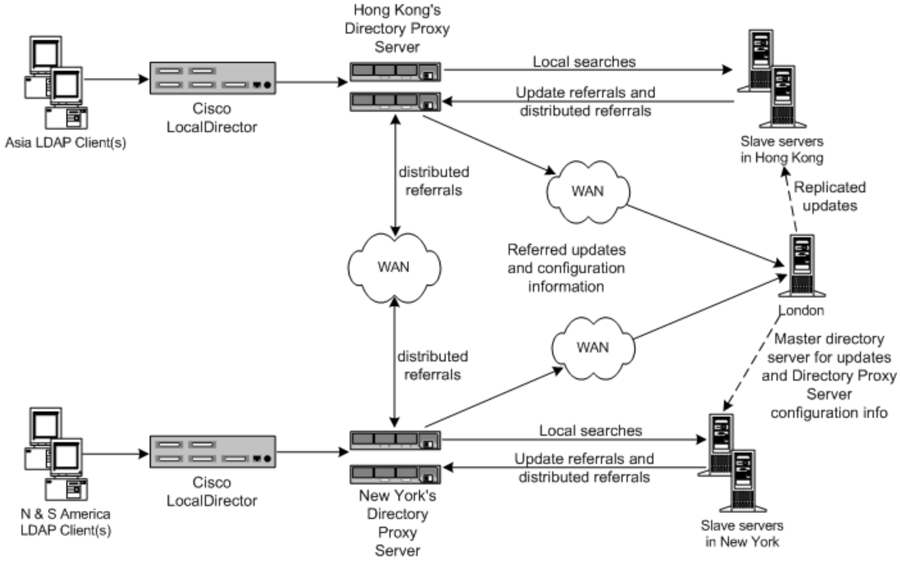
The following sections explain the role of Directory Proxy Server in a distributed LDAP directory infrastructure:

- Customer Scenario
- Customer Deployment
- LDAP Request Flow

Customer Scenario

In the configuration shown in Figure 2-2, a large financial institution is headquartered in London with data centers in London, New York, and Hong Kong. Currently, the vast majority of the data available to employees resides centrally in legacy RDBMS repositories in London. All access to this data from the financial institution’s client community is via the Wide Area Network (WAN). The financial institution is experiencing scalability and performance problems with this centralized model and has decided to move to a distributed data model. The financial institution has also decided to deploy an LDAP directory infrastructure at the same time. The data in question is considered “mission critical” and should therefore be deployed in a highly available, fault tolerant infrastructure. An analysis of client application profiles has revealed that 95 percent of data accessed by a geographical client community is specific to that community since the data is customer based. It is rare for a client in Asia to access data for a customer in North America but it does happen infrequently. The client community also has a need to update customer information from time to time.

Figure 2-2 A Distributed LDAP Directory Infrastructure


Hong Kong's Directory Proxy Server
Asia LDAP Client(s)
Cisco LocalDirector
Local searches
Update referrals and distributed referrals
Slave servers in Hong Kong
distributed referrals
WAN
Replicated updates
WAN
Referred updates and configuration information
London
WAN
distributed referrals
Master directory server for updates and Directory Proxy Server configuration info
N & S America LDAP Client(s)
Cisco LocalDirector
Local searches
Update referrals and distributed referrals
New York's Directory Proxy Server
Slave servers in New York

Customer Deployment

Given the profile of 95 percent local data access, the financial institution decided to distribute its LDAP directory infrastructure geographically. It deployed multiple directory consumer servers in each geographical location (i.e., Hong Kong, New York, and London; London consumer servers are not shown in the diagram). Each of these consumer servers is configured to hold the customer data specific to the location. Data for European and Middle East customers is held in the London consumer servers, data for North and South American customers is held in the New York consumer servers, and data for Asian and Pacific Rim customers is held in the Hong Kong consumer servers. With this deployment, the overwhelming data requirement of the local client community is located in the community. This provides significant performance improvements over the centralized model since client requests are processed locally, thereby reducing the network overhead; the local directory servers are effectively partitioning the directory infrastructure, thereby providing increased directory server performance and scalability. Each set of consumer directory servers is configured to return referrals if a client submits an update request or if a client submits a search request for data located elsewhere.

LDAP Request Flow

Client LDAP requests are sent to the Sun ONE Directory Proxy Server via the Cisco LocalDirector. The LocalDirector product is shown here only as an example of IP packet switching that ensures clients always have access to at least one Directory Proxy Server. The locally deployed Directory Proxy Server initially routes all requests to the array of local directory servers holding the local customer data. The instances of Directory Proxy Server are configured to load balance across the array of directory servers, thereby providing automatic failover and failback. Client search requests for local customer information are satisfied by a local directory and appropriate responses returned to the client via Directory Proxy Server. Client search requests for geographically “foreign” customer information are initially satisfied by the local directory server by returning a referral back to Directory Proxy Server.

This referral contains an LDAP URL that points to the appropriate geographically distributed Directory Proxy Server instance. The local Directory Proxy Server processes the referral on behalf of the local client and sends the search request to the appropriate distributed instance of Directory Proxy Server. The distributed Directory Proxy Server forwards the search request on to the distributed directory server and receives the appropriate response. This response is then returned to the local client via the distributed and the local instances of Directory Proxy Server.

Update requests received by the local Directory Proxy Server are also satisfied initially by a referral returned by the local directory server. Again, Directory Proxy Server follows the referral on behalf of the local client but this time forwards the update request onto the supplier directory server located in London. The supplier directory server applies the update to the supplier database and sends a response back to the local client via the local Directory Proxy Server. Subsequently, the supplier directory server will propagate the update down to the appropriate consumer directory servers.

All the Sun ONE Directory Proxy Servers are configured to start up and look for their configuration in the supplier directory server. This allows you to distribute multiple instances of Directory Proxy Server geographically but manage their configurations centrally.

A Centralized LDAP Directory Infrastructure

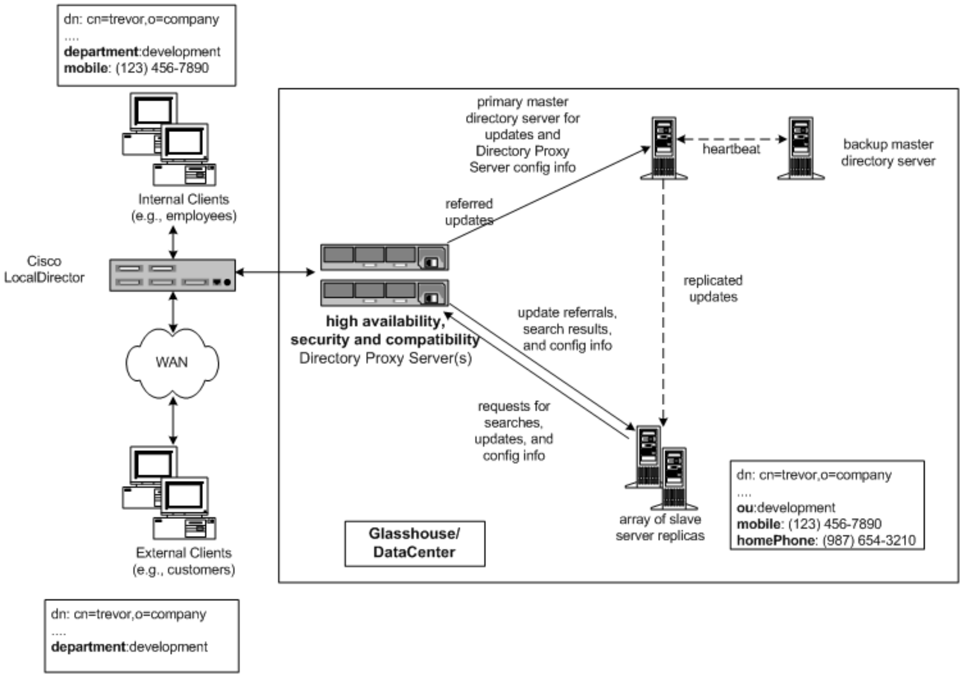
The following sections explain the role of Directory Proxy Server in a centralized LDAP directory infrastructure:

- Customer Scenario
- Customer Deployment
- LDAP Request Flow

Customer Scenario

Figure 2-3 depicts a large global enterprise, with customers and employees distributed throughout the world, that wanted to deploy a corporate white and yellow pages (electronic phone book) to reduce the cost of printing a paper phone book, to increase the accuracy of the corporate information, and to reduce the use of environmental resources. The white and yellow pages information had to be available to both customers and employees with appropriate access controls. They also had to be available 24x7 and were classified as mission critical due to customers and employees being distributed throughout the world across all time zones.

Figure 2-3 A Centralized LDAP Directory Infrastructure



Customer Deployment

The global enterprise decided to deploy a centralized LDAP directory infrastructure to support the deployment of the white and yellow pages. A centralized deployment was chosen in this instance because the white and yellow pages are for corporate employee information only. This was not to be a customer database although the intent was for customers to have access to some of the information. It was decided that the projected size of the directory database (~200,000 entries) was not sufficient to require a more complex distributed deployment model since neither scalability nor performance were anticipated to be a problem.

Since there was a high availability requirement, the enterprise decided to deploy multiple consumer directory server replicas supplied by a single supplier directory server. To remove the single point of failure introduced by a single supplier directory server, the enterprise deployed a backup supplier directory server.

Sun ONE Directory Proxy Servers were deployed for three different reasons. First, to provide the load balancing and automatic failover and failback between all LDAP clients and the array of directory server replicas. Second, to be able to differentiate between external and internal clients and to set appropriate access controls accordingly. Third, to provide compatibility between the LDAP clients using the white and yellow pages and the directory servers themselves. In addition to utilizing a custom-built white and yellow pages application, the LDAP clients also used a number of off-the-shelf LDAP enabled applications that came with fixed schema requirements. These schema requirements did not always match the directory schema designed by the enterprise, therefore requiring some basic schema attribute mapping. In addition, not all the LDAP enabled applications used by the clients were capable of processing referrals received from the directory servers correctly. The Sun ONE Directory Proxy Servers were configured to follow these referrals on behalf of the clients.

LDAP Request Flow

All client requests, whether from internal or external clients and whether search requests or update requests, are sent to instances of Directory Proxy Server via the Cisco LocalDirector. The LocalDirector product is shown here only as an example of IP packet switching that ensures clients always have access to at least one Directory Proxy Server. Multiple instances of Directory Proxy Server are deployed to ensure there is no single point of failure. The instances of Directory Proxy Server load balance all the requests received from the clients across all the consumer directory servers in the array. Directory Proxy Server will also detect the failure of any of the consumer servers and failover to the available consumer servers in the array.

Since consumer servers are read-only replicas, they are configured to return an LDAP referral when an update request is received from a client. This referral contains an LDAP URL pointing to the supplier directory server. When the directory server returns the referral, the Directory Proxy Server recognizes it and follows the referral on behalf of the client. It binds to the supplier directory server and sends the update request to it. The supplier directory server applies the update to the supplier database and sends a response back to the client via Directory Proxy Server. Subsequently, the supplier directory server will propagate the update down to the appropriate consumer directory servers.

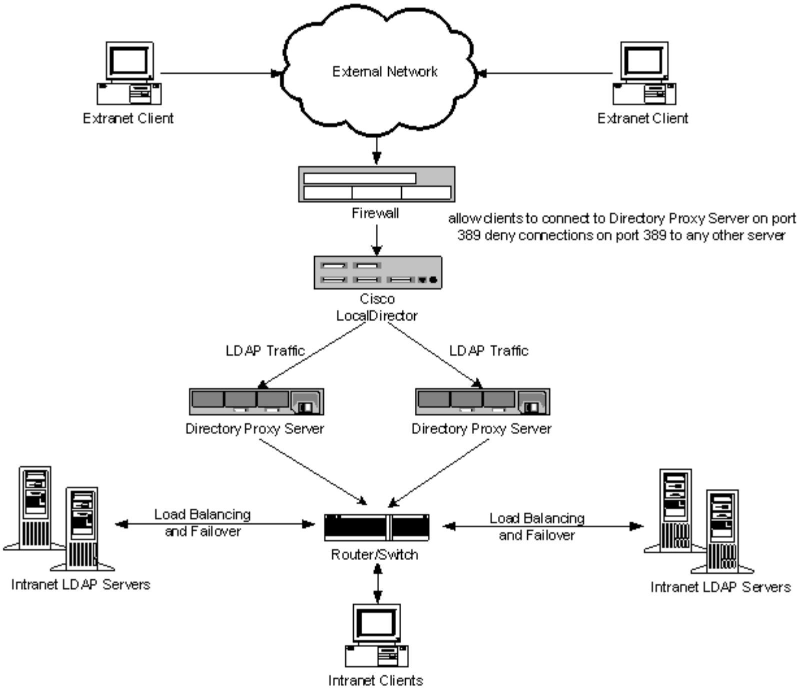
Search requests sent by clients get routed via the Directory Proxy Servers to the array of consumer directory server replicas. Sun ONE Directory Proxy Servers can be configured to “inspect” these search requests before sending them on to the directory servers and filter out any requests that don’t meet the access control and security rules configured for a particular client group and perform any necessary mappings. Directory Proxy Server can also be configured to “inspect” the search result returned by the directory server and again perform appropriate filtering and mapping. In the example shown in Figure 2-3, both internal and external clients have requested a search for the entry belonging to “Trevor.” These inbound requests are treated identically by Directory Proxy Server irrespective of the client type. The directory server executes the request successfully and returns the entry for “Trevor” back to the Directory Proxy Server. Directory Proxy Server has been configured to manipulate the search result differently depending on whether the original request came from an internal or external client. In the case of the external client, both the mobile phone number and the home phone number fields in the entry are filtered out since they are deemed to be data inappropriate for customers. Note also that the ou: development attribute/value pair has been mapped to department: development. This is necessary because one of the applications the client is using to access the directory (e.g., Outlook, Outlook Express) has fixed schema elements that do not match the schema elements deployed in the enterprise directory servers. In the case of the internal client it was determined that the mobile phone number was an important data element to share among employees whereas the home phone number was not. So for internal clients, Directory Proxy Server is configured to filter out only the home phone number and to permit the client to see the mobile phone number. Note the same mapping of the ou attribute to the department attribute is also performed.

All Sun ONE Directory Proxy Servers are configured to start up and look for their configuration in the supplier directory server. This allows for the management of multiple Directory Proxy Server configurations centrally from a directory.

Deploying Directory Proxy Server with a Single Firewall

Your organization’s firewall must be configured like that shown in Figure 2-4 to allow only LDAP clients to access the machine and port on which the Directory Proxy Server is running. Typically, LDAP clients will connect on TCP port 389. This will protect the host running Directory Proxy Server from clients who may try to gain unauthorized access to it. Also, placing the host running the proxy server on its own LAN, by using the router switch, will protect your internal network from denial of service attacks such as flooding your network with unnecessary traffic. The firewall should also disallow LDAP access to the machine(s) and port(s) on which the LDAP Directory Server(s) are “hiding,” thereby protecting the LDAP directory database(s).

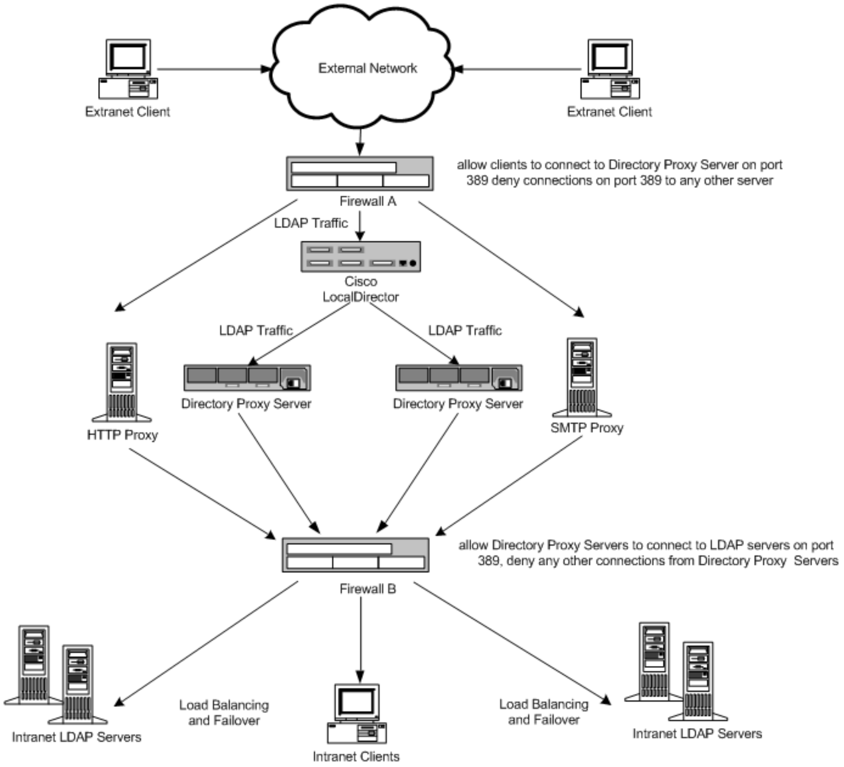
Figure 2-4 Directory Proxy Server Setup with One Firewall



Deploying Directory Proxy Server with Two Firewalls

The configuration shown in Figure 2-5 has all the benefits of the configuration shown in Figure 2-4 with some additional security. Installing two firewalls creates a zone of control around the "proxies," allowing the site administrator to rate limit traffic from the external networks. It also ensures that a compromise of one of the "proxy" servers cannot be used directly to attack other machines in the interior network. Firewall A would be configured to allow only incoming packets if the destination IP address is that of the proxy handling that TCP or UDP protocol. Firewall B would be configured to allow only packets from the proxy machines that are appropriate to the servers that the proxy needs to access.

Figure 2-5 Directory Proxy Server Setup with Two Firewalls


External Network
Extranet Client
Extranet Client
allow clients to connect to Directory Proxy Server on port 389 deny connections on port 389 to any other server
Firewall A
LDAP Traffic
Cisco LocalDirector
LDAP Traffic
LDAP Traffic
HTTP Proxy
Directory Proxy Server
Directory Proxy Server
SMTP Proxy
allow Directory Proxy Servers to connect to LDAP servers on port 389, deny any other connections from Directory Proxy Servers
Firewall B
Intranet LDAP Servers
Load Balancing and Failover
Intranet Clients
Load Balancing and Failover
Intranet LDAP Servers

Part 2

Console Based Administration

Chapter 3

Introducing Directory Proxy Server Consoles

After installing Sun ONE Directory Proxy Server, you first configure it to function with your directory deployment, and then on, closely monitor its activities. In administering Directory Proxy Server, you perform server-specific tasks such as starting, stopping, and restarting the server; creating groups; setting up the server to identify certain events and execute appropriate actions; changing configuration; performing any routine server maintenance tasks; and monitoring logs.

To enable you to accomplish these server-specific tasks quickly and easily, Directory Proxy Server provides GUI-based administration tools, called the *Directory Proxy Server Server Console* and *Directory Proxy Server Configuration Editor Console*, both of which are accessible from within the Console. This chapter provides an overview of both Sun ONE and Directory Proxy Server consoles.

The chapter has the following sections:

- Getting Started with Sun ONE Console (page 32)
- Accessing the Directory Proxy Server Consoles (page 36)

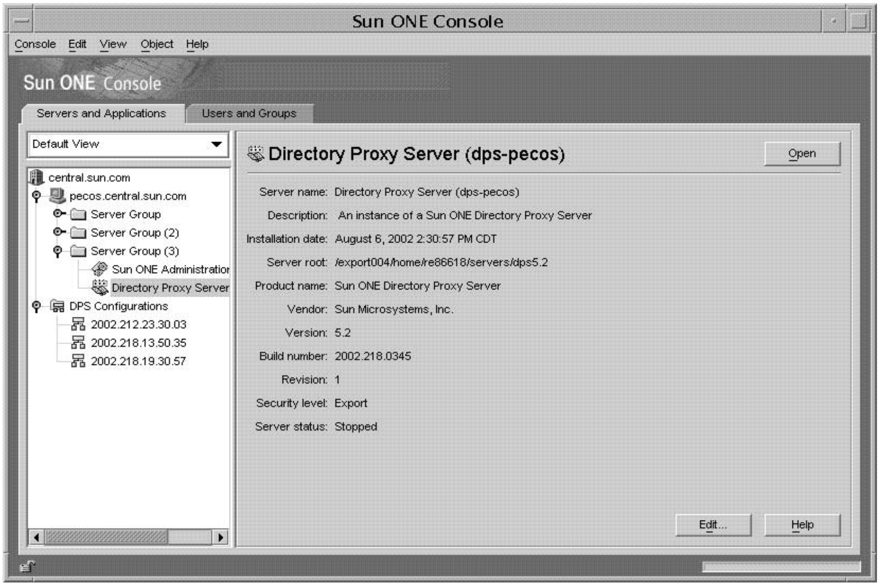
NOTE	You can use the Sun ONE Console for managing various network resources. However, this chapter's focus is on using the Sun ONE Console for Directory Proxy Server administration only. For complete information about the Sun ONE Console, see *Managing Servers with Sun ONE Console*, which is included with the Directory Proxy Server documentation. You can also get a copy of this book from this site: `http://docs.sun.com/`

Getting Started with Sun ONE Console

The Sun ONE Console is a stand-alone Java application that provides a GUI-based front end to all network resources registered in an organization's *configuration directory*. This unified administration interface simplifies network administration by supplying access points to all Sun ONE version 5.x server instances installed across a network. Similarly, it simplifies basic user and group management by providing a unified administration interface to the user directory.

Figure 3-1 shows the "Servers and Applications" tab of the Sun ONE Console with an Directory Proxy Server instance selected.

Figure 3-1 Sun ONE Console: Servers and Applications Tab



Directory Proxy Server (dps-pecos)

Server name: Directory Proxy Server (dps-pecos)
Description: An instance of a Sun ONE Directory Proxy Server
Installation date: August 6, 2002 2:30:57 PM CDT
Server root: /export004/home/re86618/servers/dps5.2
Product name: Sun ONE Directory Proxy Server
Vendor: Sun Microsystems, Inc.
Version: 5.2
Build number: 2002.218.0345
Revision: 1
Security level: Export
Server status: Stopped

Servers and Applications Tab

For any given instance of the Sun ONE Console, the limits of the network it can administer are defined by the set of resources whose configuration information is stored in the same configuration directory—that is, the maximum set of hosts and servers that can be monitored from the Sun ONE Console. The *superadministrator* (the person who manages the configuration directory) can set access permissions on all network resources registered in the configuration directory. Thus, for a given administrator using the Sun ONE Console, the actual number of visible hosts and servers may be fewer, depending on the access permissions set by the superadministrator.

The “Servers and Applications” tab displays all servers registered in a particular configuration directory, giving you a consolidated view of all the server software and resources under your control. What you control is determined by the access permissions the superadministrator has set up for you.

From this view, you can perform tasks across arbitrary groups or a cluster of servers in a single operation. In other words, you can use the “Servers and Applications” tab to manage a single server or multiple servers that are installed on different ports on one machine. Also, you can access individual server consoles (or administration interfaces) by double-clicking the icons for the corresponding server instance entries (SIEs).

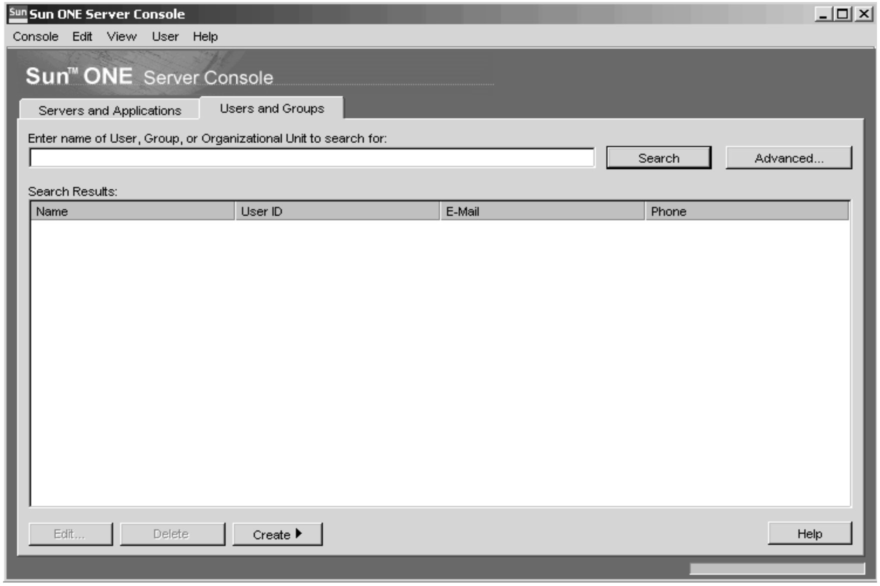
You can accomplish various Directory Proxy Server-specific tasks from the “Servers and Applications” tab:

- Launch the Directory Proxy Server Server Console.
- Launch the Directory Proxy Server Configuration Editor Console (so that you can configure a group of Directory Proxy Servers).
- Set access permissions for Directory Proxy Server.
- Launch the Administration Server Console (so that you can configure an Administration Server instance for administering Directory Proxy Server).

Users and Groups Tab

The “Users and Groups” tab (shown in Figure 3-2) manages user accounts, group lists, and access control information for individual users and groups. All applications registered within the Sun ONE Console framework share core user and group information in the user directory, which typically is a global directory for corporate wide user data.

Figure 3-2 Sun ONE Console: Users and Groups Tab



From this tab, you can accomplish various user- and group-specific tasks, such as these:

- Add, modify, and delete user and group information in the user directory.
- Search for specific user and group entries in the user directory.

Sun ONE Administration Server

Sun ONE Administration Server is a web-based (HTTP) server that enables you to configure all your Sun ONE servers, including Directory Proxy Server, via the Sun ONE Console. Administration Server (and the configuration directory) must be running before you can configure any of these servers. Administration Server is included with all the Sun ONE servers and is installed when you install your first server in a *server group*. A server group refers to servers that are installed in a server root directory and that are managed by a single instance of Administration Server.

You access Administration Server by entering its URL in the Sun ONE Console login screen; see "Step 1. Log In to the Sun ONE Console," on page 36. This URL is based on the computer hostname and the port number you chose when you installed Directory Proxy Server. The format for the URL looks like this: `http://<machine_name>.<your_domain>.<domain>:<port>`

Whenever you try to gain access to Administration Server, you will be prompted to authenticate yourself to the configuration directory by entering your user ID and password. These are the *administrator* user name and password that you specified when you installed Directory Proxy Server (or the first server in the server group) and Administration Server on your computer. Once Administration Server is running, you can use the Sun ONE Console to administer all servers in that group, including Directory Proxy Server.

For complete details about Administration Server, see *Managing Servers with Sun ONE Console*. To locate an online version of this book in your Directory Proxy Server installation, open this file: `<server-root>/manual/en/admin/ag/contents.htm`

You can also get the latest version of this book from this site:

`http://docs.Sun ONE.com/docs/manuals/console.html`

Starting Administration Server

The Directory Proxy Server installation program automatically starts the instance of Administration Server that you identified during installation for monitoring Directory Proxy Server. If you stopped Administration Server after Directory Proxy Server installation, you must start it before you can administer Directory Proxy Server from the Directory Proxy Server Console.

You can start Administration Server from the command line or from the Windows NT Services panel.

- To start Administration Server from the command line:

  At the prompt, enter the following line: `<server-root>/start-admin`

- Administration Server runs as a service in a Windows NT system. You can use the Windows NT Services panel to start the service directly.

All the above-mentioned methods start Administration Server at the port number you specified during installation. Once the server is running, you can use the Sun ONE Console to access Directory Proxy Server.

Stopping Administration Server

It is good security practice to shut down Administration Server when you are not using it. This minimizes the chances of someone else changing your configuration. You can shut down the server from the Sun ONE Console, the command line, or the Windows NT Services panel.

- To shut down Administration Server from the Sun ONE Console:

  a. Log in to the Sun ONE Console (see “Step 1. Log In to the Sun ONE Console” on page 36).

  b. In the “Servers and Applications” tab, locate the Administration Server instance that you want to shut down, and double-click the corresponding entry.

  The Administration Server Console appears.

  a. In the Tasks tab, click Stop the Server.

- To shut down Administration Server from the command line:

  At the prompt, enter the following line: `<server-root>/stop-admin`

- Administration Server runs as a service in a Windows NT system; you can use the Windows NT Services panel to stop the service directly.

Accessing the Directory Proxy Server Consoles

To perform any of the Directory Proxy Server-administration tasks from the Directory Proxy Server consoles, you need to open it first.

- Step 1. Log In to the Sun ONE Console
- Step 2. Open the Appropriate Directory Proxy Server Console

Step 1. Log In to the Sun ONE Console

You can launch and use the Sun ONE Console only when the corresponding configuration directory and Administration Server are running. If the servers are not running, go to the command line and start them. For information on starting Administration Server from the command line, see “Starting Administration Server,” on page 35. For information on starting the configuration directory, check the Sun ONE Directory Server documentation.

When you launch the Sun ONE Console, it displays a login window. You are required to authenticate to the configuration directory by entering your administrator's ID, your password, and the URL (including the port number) of the Administration Server representing a server group to which you have access. You cannot use the Sun ONE Console without having access privileges to at least one server group on your network.

1. Open the Sun ONE Console application by using the appropriate option:
    - For local access on a UNIX machine, at the command-line prompt, enter the following line: `<server-root>/start-console`
    - For local access on a Windows NT machine, double-click the Sun ONE Console icon on your desktop; this icon was created when you installed your first Sun ONE server.

    The Sun ONE Console Login window appears.

2. Authenticate yourself to the configuration directory.

    User ID. Type the *administrator ID* you specified when you installed Administration Server on your machine. You installed Administration Server either when you installed your first Sun ONE server or as a part of Directory Proxy Server installation.

    Password. Type the *administrator* password that you specified when you installed Administration Server on your computer during Directory Proxy Server installation.

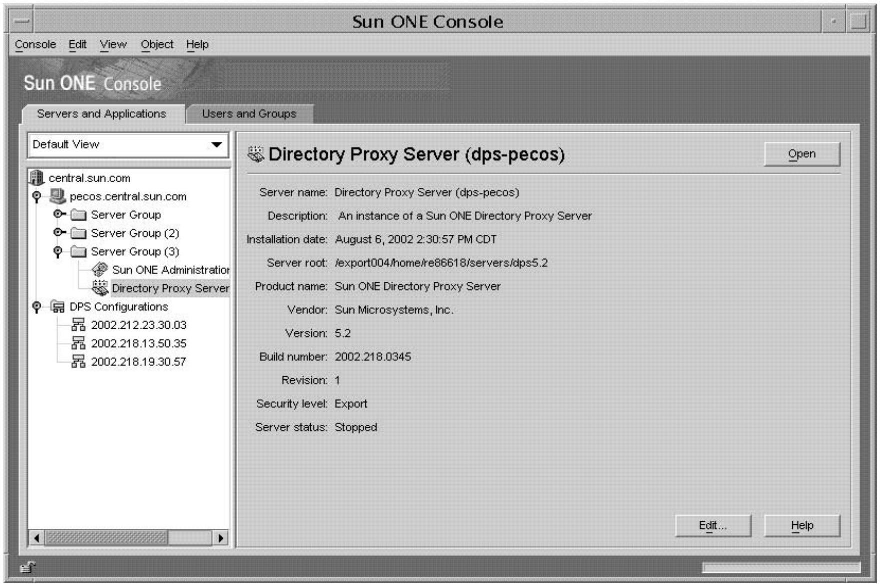
    Administration URL. This field should show the URL to Administration Server. If it doesn't or if it doesn't have the URL of Administration Server that you want, type the URL in this field. The URL is based on the computer host name and the Administration Server port number you chose when you installed Directory Proxy Server. Use this format:

    ```
    http://<machine_name>.<your_domain>.<domain>:<port_number>
    ```

    For example, if your domain name is `sun` and you installed Administration Server on a host machine called `myHost` and specified port number `12345`, the URL would look like this: `http://myHost.sun.com:12345`

3. Click OK.

    The Sun ONE Console appears with a list of all the servers and resources under your control.



Directory Proxy Server (dps-pecos)

Server name: Directory Proxy Server (dps-pecos)
Description: An instance of a Sun ONE Directory Proxy Server
Installation date: August 6, 2002 2:30:57 PM CDT
Server root: /export004/home/re86618/servers/dps5.2
Product name: Sun ONE Directory Proxy Server
Vendor: Sun Microsystems, Inc.
Version: 5.2
Build number: 2002.218.0345
Revision: 1
Security level: Export
Server status: Stopped

Step 2. Open the Appropriate Directory Proxy Server Console

In the Sun ONE Console, you will notice that there are two entries for Directory Proxy Server, one for the Directory Proxy Server instance node and another for the Directory Proxy Server Configurations node. The Directory Proxy Server instance node corresponds to the Directory Proxy Server server instance and the Directory Proxy Server Configurations node corresponds to the configuration shared by multiple Directory Proxy Server instances.

Each node is associated with a GUI-based administration interface:

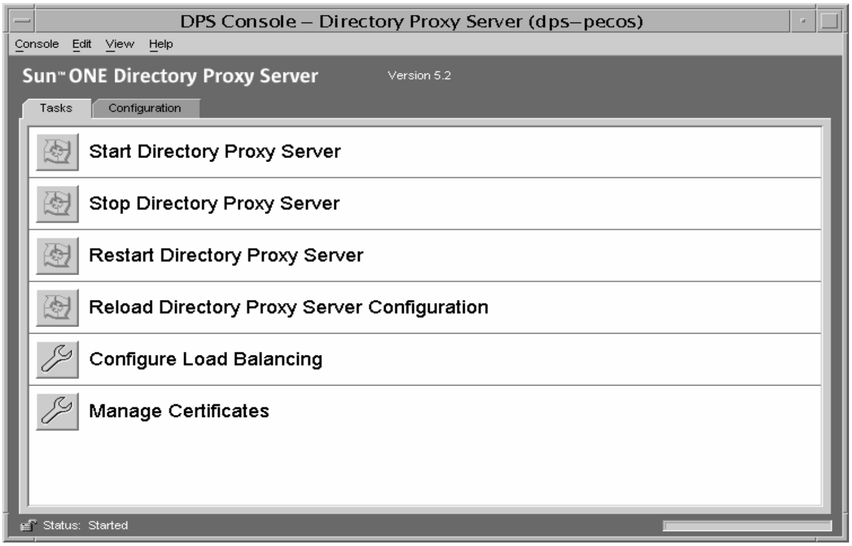
- Directory Proxy Server Console—This administration interface enables you to create, configure and manage an Directory Proxy Server instance, for example to start it, to stop it, to specify configuration, to monitor logs, and so on. You can use the Directory Proxy Server Server Console to access the server locally or remotely. Directory Proxy Server instances created and configured with the Directory Proxy Server Server Console affect all Directory Proxy Server instances that use the configuration.

- Directory Proxy Server Configuration Editor Console—The logic and system configurations can be shared by multiple Directory Proxy Server instances. The ability of Directory Proxy Server instances to share configuration information simplifies the task of managing a cluster of Directory Proxy Servers. The Directory Proxy Server Configuration Editor Console is an administration interface that enables you to configure and manage a cluster of Directory Proxy Servers. Edits made via this interface affect all Directory Proxy Server instances that use the edited configuration.

Opening the Directory Proxy Server Server Console

Once you have logged in to the Sun ONE Console, you can open the Directory Proxy Server Server Console: in the navigation tree of the Sun ONE Console, expand the hostname that contains the server group to which the Directory Proxy Server instance belongs, expand the Server Group node, select the entry that corresponds to the Directory Proxy Server instance of your interest, and click Open. The Directory Proxy Server Console opens (Figure 3-3).

Figure 3-3 Directory Proxy Server Server Console: Tasks Tab

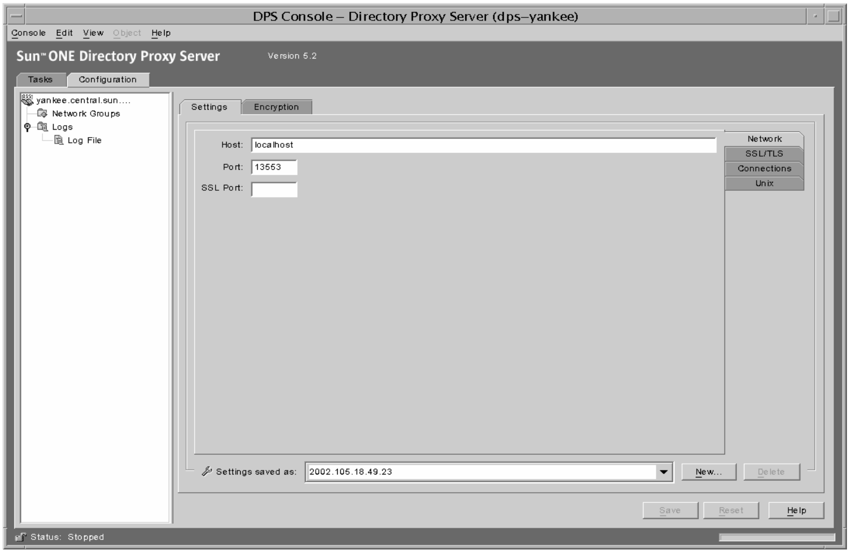

DPS Console – Directory Proxy Server (dps–pecos)
Console
Edit
View
Help
Sun™ ONE Directory Proxy Server
Version 5.2
Tasks
Configuration
Start Directory Proxy Server
Stop Directory Proxy Server
Restart Directory Proxy Server
Reload Directory Proxy Server Configuration
Configure Load Balancing
Manage Certificates
Status: Started

The Directory Proxy Server Console to has two tabs—Tasks and Configuration—each addressing specific administrative areas.

The Tasks tab enables you to perform common tasks such as starting, stopping, restarting, and reloading the server, distributing or balancing load among various LDAP directories and manage certificates. For details about starting, stopping, and restarting Directory Proxy Server, see Chapter 4, “Starting, Restarting, and Stopping Directory Proxy Server.” For details about load balancing, see Chapter 7, “Defining and Managing Property Objects.” For details about Managing certificates, see Chapter 11, “Configuring Security.”

The Configuration tab (Figure 3-4) enables you to view and modify the configuration for a particular instance.

Figure 3-4 Directory Proxy Server Server Console: Configuration Tab Settings Tab



Host: localhost

Port: 13553

SSL Port:

Settings saved as: 2002.105.18.49.23

Status: Stopped

The Settings and Encryptions tabs are related to how this specific instance of Directory Proxy Server is configured.

The Settings Tab (Figure 3-4) allows you to configure the following parameters:

Network. Displays the Host Name, Port, and SSL Port for this instance of Directory Proxy Server.

SSL/TLS. Displays the currently selected configuration from which Directory Proxy Server sends to and requires from SSL certificates from servers and clients. It also identifies the SSL / TLS versions for client to Directory Proxy Server and Directory Proxy Server to backend communication.

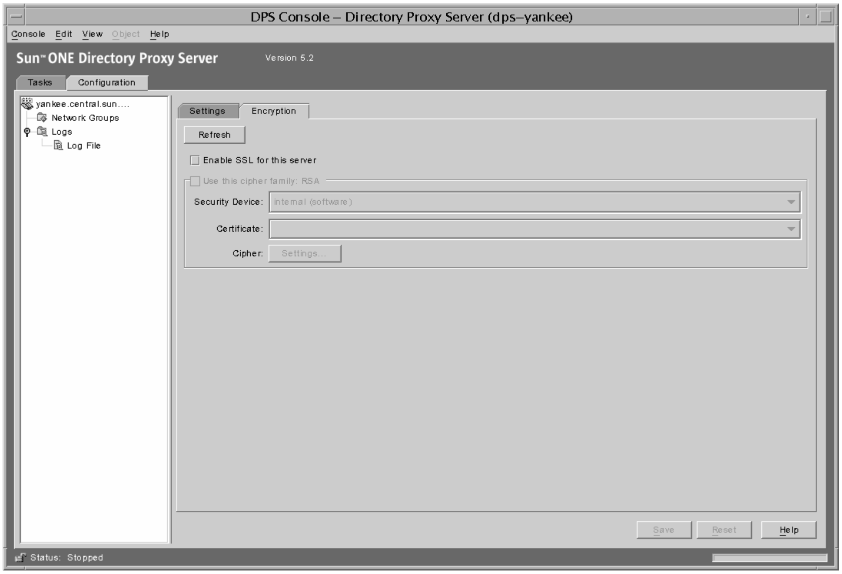
Connections. Displays the Directory Proxy Server connection backlog value, allows you to specify a maximum number of connections, and set connection pool timeout values.

Unix. Displays the UNIX user ID and working directory for this instance of Directory Proxy Server.

Settings saved as. Allows you to specify a Directory Proxy Server name value for the editing session currently displayed in the list box. You may also create a new or delete an old Directory Proxy Server configuration.

The Configuration tab encryption tab (Figure 3-5) enables you to view and modify the encryption settings.

Figure 3-5 Directory Proxy Server Server Console: Configuration Tab Encryption Tab



☐ Enable SSL for this server

☐ Use this cipher family: RSA

Security Device: Internal (software)

Certificate:

Status: Stopped

The Encryption Tab allows you to configure the following parameters:

Refresh. Allows you to refresh the current screen values to see newly added certificates.

Enable SSL for this server. Enables SSL encryption for this instance of Directory Proxy Server.

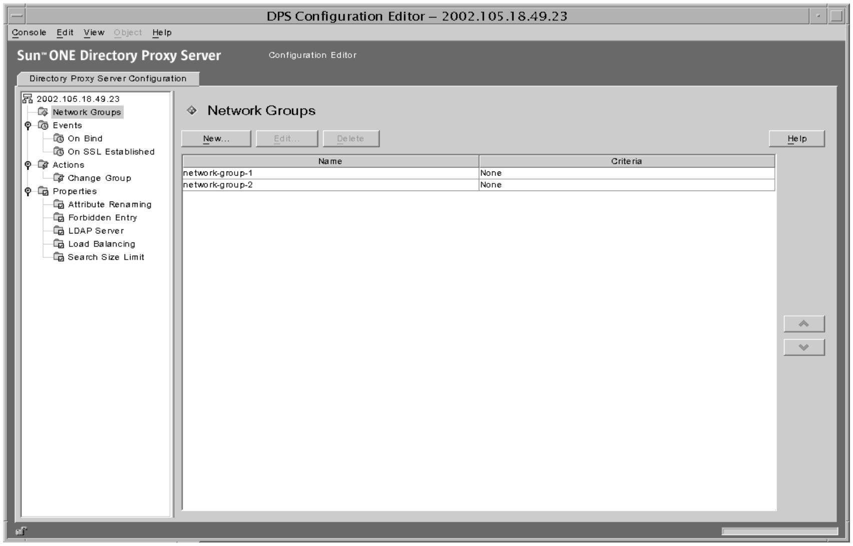
Use the cipher family RSA. Enables you to set the Security Device, Certificate, and cipher settings for this instance of Directory Proxy Server.

See “Creating System Configuration Instances,” on page 57 for more information on setting encryption for your system.

Opening the Directory Proxy Server Configuration Editor Console

Once you have logged in to the Console, you can open the Directory Proxy Server Configuration Editor Console. In the navigation tree of the Console, expand the Directory Proxy Server Configurations node, select the entry, and click Open. The Directory Proxy Server Configuration Editor Console opens (Figure 3-6).

Figure 3-6 Directory Proxy Server Configuration Editor Console



Name	Criteria
network-group-1	None
network-group-2	None

The navigation tree on the left side contains nodes for each of Directory Proxy Server’s basic configuration objects. Expanding one of the main nodes shows tree nodes for each of object subtype. Clicking a tree node displays a table on the right side containing all current objects of the type indicated by the selected tree node. Object tables whose ordering is important, for example, Network Groups, have a set of up and down buttons that allow individual objects to be raised or lowered in precedence.

Table 3-1 lists the configuration object types shown in the navigation tree.

Table 3-1 Configuration Objects in the Directory Proxy Server Configuration Editor Console

Configuration Object Type	Description
Network Groups	Each Network Group object identifies a specific client community, and specifies the restrictions to enforce on clients that match that group. For details, see Chapter 6, “Creating and Managing Groups.”
Events	Event objects are used to specify conditions that occur at predetermined states. Conditions can be attached to certain events, on which, if satisfied, Directory Proxy Server can take certain actions. For details, see Chapter 8, “Creating and Managing Event Objects.”
Actions	Actions are used to specify actions to take when an event occurs. For details, see Chapter 9, “Creating and Managing Action Objects.”
Properties	Properties are used to describe more specialized restrictions on the client. Each group object may include a set of properties defined by property objects. For details, see Chapter 7, “Defining and Managing Property Objects.”

Chapter 4

Starting, Restarting, and Stopping Directory Proxy Server

This chapter describes how to start, stop, and restart Sun ONE Directory Proxy Server and how to check its current status.

The chapter has the following sections:

- Starting and Stopping Directory Proxy Server (page 45)
- Restarting Directory Proxy Server (page 50)
- Checking Directory Proxy Server System Status (page 52)

NOTE	You can use the Directory Proxy Server consoles only when the appropriate Directory Server (identified as the *configuration* directory) and Administration Server are running. Be sure to start Administration Server at the port you specified during Directory Proxy Server installation. To minimize security risks, shut down Administration Server when you have finished using the Sun ONE Console. For instructions on starting and shutting down Administration Server, see “Sun ONE Administration Server,” on page 34.

Starting and Stopping Directory Proxy Server

Once Directory Proxy Server is installed, it runs constantly, listening for and accepting requests; it runs as a UNIX daemon process or a Windows NT service normally started during system boot time.

You can start and stop Directory Proxy Server in several ways:

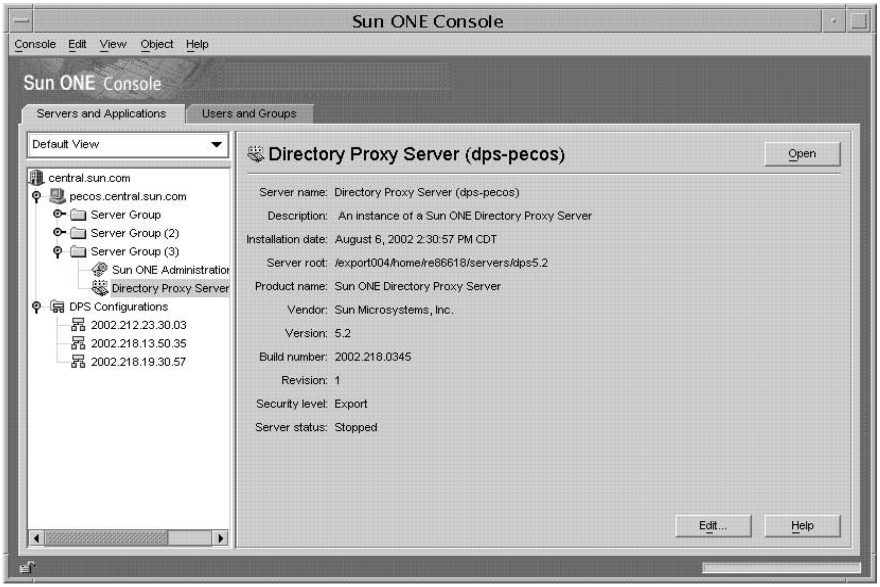
- From the Sun ONE Console (locally and remotely)
- From the command line (locally only)
- On a Windows NT system, from the Windows NT Services panel

Note that stopping Directory Proxy Server shuts down all its components completely, interrupting service until the server is started again. If the host machine crashes or is taken off line, the server stops, and any requests it was servicing are lost. You need to start the server again to restore the service.

Starting and Stopping Directory Proxy Server From Sun ONE Console

You can use the Sun ONE Console to start and stop Directory Proxy Server installed on a local or remote host. To start or stop Directory Proxy Server:

1. Log in to the Sun ONE Console (see "Step 1. Log In to the Sun ONE Console," on page 36).
2. In the "Servers and Applications" tab, expand the hostname and then the Server Group that contains the Directory Proxy Server instance you want to start.
3. In the navigation tree, locate the Directory Proxy Server instance you want to start or stop, select the corresponding entry, and click Open.

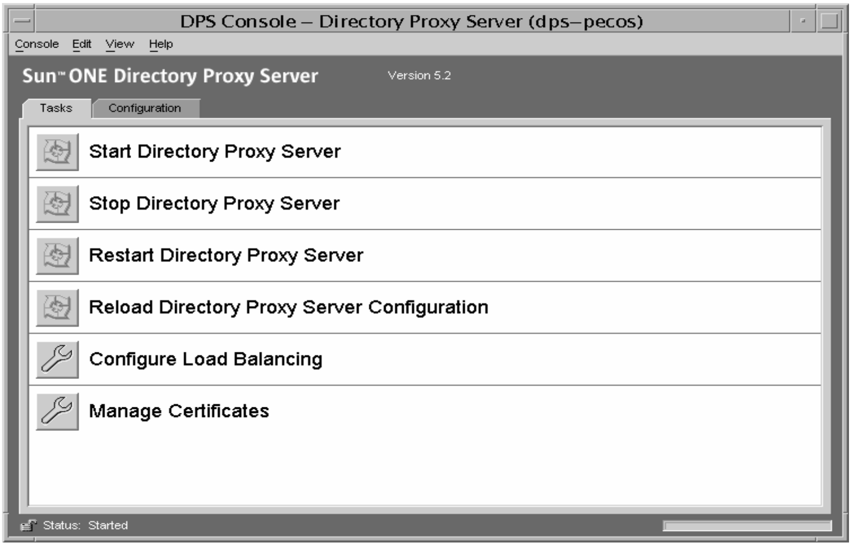


Directory Proxy Server (dps-pecos)

Server name: Directory Proxy Server (dps-pecos)
Description: An instance of a Sun ONE Directory Proxy Server
Installation date: August 6, 2002 2:30:57 PM CDT
Server root: /export004/home/re86618/servers/dps5.2
Product name: Sun ONE Directory Proxy Server
Vendor: Sun Microsystems, Inc.
Version: 5.2
Build number: 2002.218.0345
Revision: 1
Security level: Export
Server status: Stopped

The Directory Proxy Server Server Console opens.

4. In the Tasks tab, click Start Directory Access Router to start the server or Stop Directory Access Router to stop the server.


DPS Console – Directory Proxy Server (dps–pecos)
Console
Edit
View
Help
Sun™ ONE Directory Proxy Server
Version 5.2
Tasks
Configuration
Start Directory Proxy Server
Stop Directory Proxy Server
Restart Directory Proxy Server
Reload Directory Proxy Server Configuration
Configure Load Balancing
Manage Certificates
Status: Started

Starting and Stopping Directory Proxy Server From Command Line

To start or stop Directory Proxy Server from the command line:

1. Open a terminal window to your server.
2. In a UNIX system, log in as `root` if the server runs on ports less than 1024; otherwise, log in either as `root` or with the server's user account. (By default, if Directory Proxy Server is run by `root`, it changes its user ID to `nobody`.)
3. At the command-line prompt, enter either of the following lines:

   To start Directory Proxy Server:
   ```
   <server-root>/dps-<hostname>/start-dps[.exe]
   ```

   To stop Directory Proxy Server:
   ```
   <server-root>/dps-<hostname>/stop-dps[.exe]
   ```

   `<server-root>` is the directory where the Directory Proxy Server binaries are kept. You first specified this directory during installation.

   `<hostname>` is the name of the host on which this instance of Directory Proxy Server is installed.

`.exe` specifies the file extension; this is required only when running the utility on a Windows NT system.

NOTE If Directory Proxy Server is already running, the start-up command fails. Stop the server first using the `stop-dps` command, then use the `start-dps` command.

Starting and Stopping Directory Proxy Server From Windows NT Services Panel

If you have installed Directory Proxy Server on a Windows NT system, you can start and stop the server (as a service) from the Windows NT Services panel. The Directory Proxy Server service has the following name: `Sun ONE Directory Proxy Server`.

To start or stop Directory Proxy Server from the Windows NT Services panel:

1. On your desktop, select Start > Settings > Control Panel.
2. In the Control Panel window that appears, double-click Services.
3. Scroll through the list of services, and locate the service that corresponds to the Directory Proxy Server instance.
4. To start the service, select the Directory Proxy Server instance, and click Start. To stop the service, select the Directory Proxy Server instance, and click Stop.

Restarting Directory Proxy Server

Whenever you change the Directory Proxy Server configuration, you must save your changes for them to be stored in the configuration directory. All configuration changes require that you restart Directory Proxy Server after you save the changes. If restarting is required, the console prompts you accordingly.

During restart, Directory Proxy Server re-reads its configuration and uses the new configuration for future connections. Client connections that are already established continue to use the old configuration until the clients disconnect. The restart function is only available on UNIX platforms. On Windows NT, restarting Directory Proxy Server is equivalent to stopping and starting Directory Proxy Server.

You can restart Directory Proxy Server in two ways:

- From the Directory Proxy Server Server Console (locally and remotely)
- From the command line (locally only)

Restarting Directory Proxy Server From Command Line

To restart Directory Proxy Server from the command line:

1. Open a terminal window to your server.
2. In a UNIX system, log in either as `root` or using the server’s user account (if that is how you started the server).
3. At the command-line prompt, enter the following line:

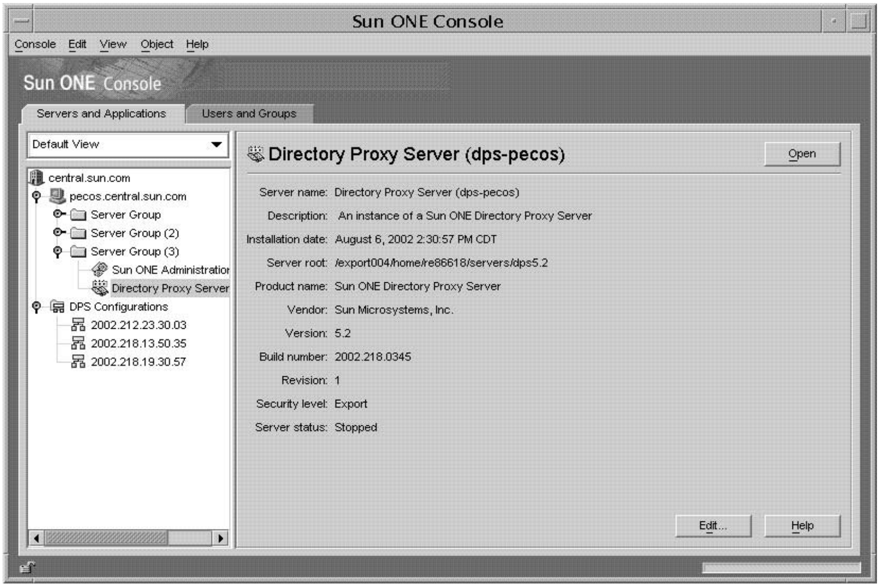
```
<server-root>/dps-<hostname>/restart-dps[.exe]
```

Reloading Directory Proxy Server From Sun ONE Console on UNIX Platforms

On UNIX platforms you can use the Directory Proxy Server Server Console to reload a Directory Proxy Server configuration installed on a local or remote host. Whenever you change the Directory Proxy Server configuration on UNIX platforms reloading the Directory Proxy Server configuration causes the changes to take effect. On NT platforms you must restart the Directory Proxy Server configuration.

To reload Directory Proxy Server from the Directory Proxy Server Console:

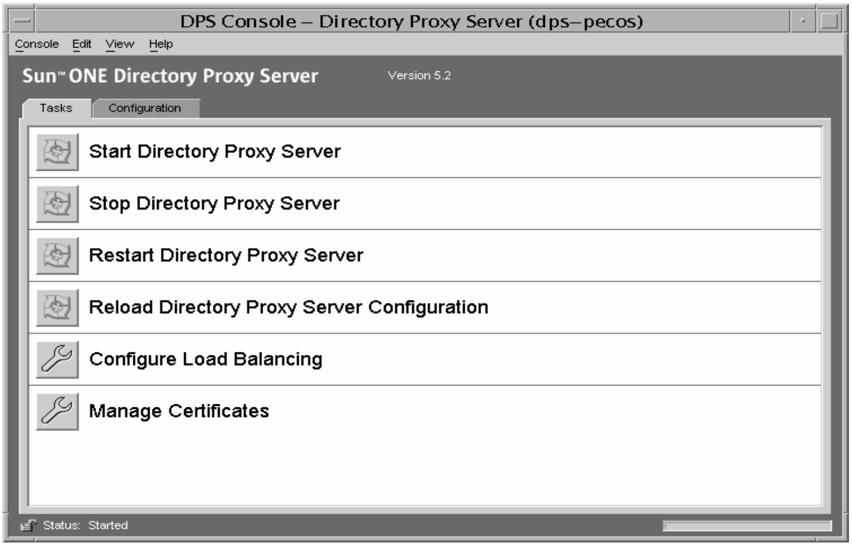
1. If you're not already viewing the Directory Proxy Server Server Console, log in to the Sun ONE Console (see "Step 1. Log In to the Sun ONE Console," on page 36).
2. In the "Servers and Applications" tab, expand the hostname and then the Server Group that contains the Directory Proxy Server instance you want to restart.
3. In the navigation tree, locate the Directory Proxy Server instance you want to start or stop, select the corresponding entry, and click Open.



Server name: Directory Proxy Server (dps-pecos)
Description: An instance of a Sun ONE Directory Proxy Server
Installation date: August 6, 2002 2:30:57 PM CDT
Server root: /export004/home/re86618/servers/dps5.2
Product name: Sun ONE Directory Proxy Server
Vendor: Sun Microsystems, Inc.
Version: 5.2
Build number: 2002.218.0345
Revision: 1
Security level: Export
Server status: Stopped

The Directory Proxy Server Server Console opens.

4. In the Tasks tab, click Reload Router Configuration to reload the server.


DPS Console – Directory Proxy Server (dps–pecos)
Console Edit View Help
Sun™ ONE Directory Proxy Server
Version 5.2
Tasks
Configuration
Start Directory Proxy Server
Stop Directory Proxy Server
Restart Directory Proxy Server
Reload Directory Proxy Server Configuration
Configure Load Balancing
Manage Certificates
Status: Started

Checking Directory Proxy Server System Status

You can check whether a particular instance of Directory Proxy Server is started or stopped in two ways:

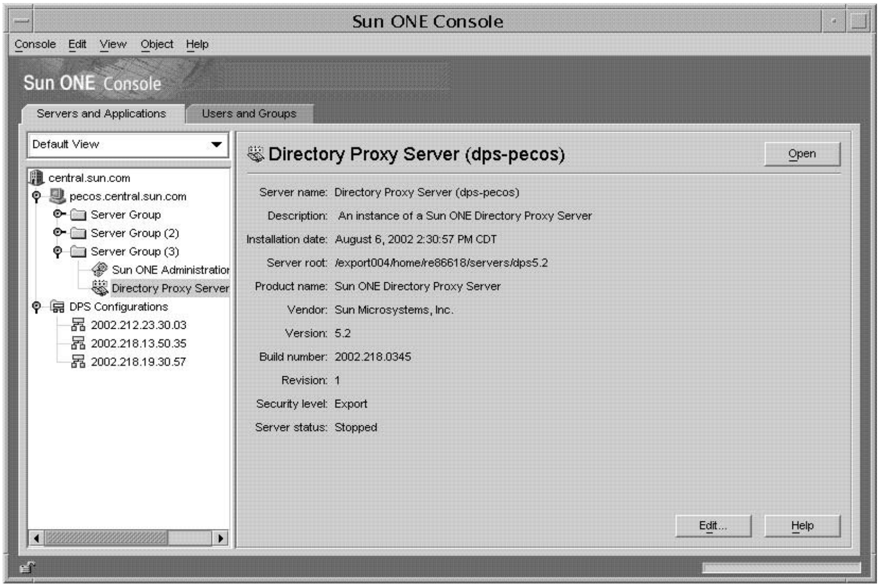
- From the Sun ONE Console (locally and remotely)
- From the command line (locally only)

Checking Directory Proxy Server Status From Sun ONE Console

You can use the Sun ONE Console to find out whether a particular Directory Proxy Server instance is running.

1. Log in to the Sun ONE Console (see “Step 1. Log In to the Sun ONE Console,” on page 36).

2. In the Servers and Applications tab, select the entry that corresponds to the Directory Proxy Server instance you want to check.



Directory Proxy Server (dps-pecos)

Server name: Directory Proxy Server (dps-pecos)
Description: An instance of a Sun ONE Directory Proxy Server
Installation date: August 6, 2002 2:30:57 PM CDT
Server root: /export004/home/re86618/servers/dps5.2
Product name: Sun ONE Directory Proxy Server
Vendor: Sun Microsystems, Inc.
Version: 5.2
Build number: 2002.218.0345
Revision: 1
Security level: Export
Server status: Stopped

3. In the right pane, check the Server Status field.

If the selected instance of Directory Proxy Server is running, the status will be *Started*. Otherwise it will be *Alert*, *Stopped*, or *Unknown*. Server status of stopped is also indicated when the SIE name is in italics.

Checking Directory Proxy Server Status From Command Line

To find out whether a particular Directory Proxy Server instance is running from the command line:

1. Open a terminal window to your server.
2. In a UNIX system, log in either as `root` or using the server's user account (if that is how you started the server).
3. At the command-line prompt, enter the following line:

```
<server-root>/dps-<hostname>/status-dps[.exe]
```

Starting and Stopping Directory Proxy Server From the Command Line

Directory Proxy Server program runs as a UNIX daemon process or an NT service normally started during system boot time.

On all platforms, Directory Proxy Server's start program resides at:

```
<server-root>/dps-<hostname>/start-dps
```

The startup configuration file resides at:

```
<server-root>/dps-<hostname>/etc/tailor.txt
```

Directory Proxy Server may be started and stopped via the scripts found at:

```
<server-root>/dps-<hostname>
```

The Windows NT Service Manager should be used to start and stop Directory Proxy Server on Windows NT. On platforms other than Windows NT, Directory Proxy Server will produce only a `core` image in case of a crash if its effective user ID is same as its real user ID. Therefore, if you want Directory Proxy Server to produce a core, then you must set the `ids-proxy-con-userid` attribute in object class `ids-proxy-sch-GlobalConfiguration` to the same user who starts the Directory Proxy Server process. By default, if Directory Proxy Server is run by `root`, it changes its userid to `nobody`.

Supported Flags

The flags supported by the start and stop scripts are described in Table 4-1.

Table 4-1 Flags Supported By the Start and Stop Scripts

Flag	Description
`-d`	When this flag is present, Directory Proxy Server will handle only a single incoming connection at a time, and will send more detailed internal tracing information to the log file. This flag should not be used during normal operation, because it will prevent the Directory Proxy Server daemon from detaching from the controlling terminal.

Table 4-1 Flags Supported By the Start and Stop Scripts *(Continued)*

Flag	Description
`-D`	This flag tells Directory Proxy Server to send more detailed tracing information to the log file. Directory Proxy Server will still handle multiple client connections and run as a daemon. The `-d` and `-D` flags should be treated as mutually exclusive.
`-t <startup configuration file>`	This option can be used to specify an alternate startup configuration file. You Must specify the absolute path to the configuration file.
`-s`	This option tells Directory Proxy Server to send the initial log messages to the `syslogd` using the `LOG_DAEMON` facility. This flag is ignored on Windows NT. This is the default if the environment variable `dps_ROOT` is not defined.
`-M`	If this flag is specified, Directory Proxy Server will spawn another process to monitor itself. In the case where Directory Proxy Server exits ungracefully, the monitor process restarts Directory Proxy Server after waiting for 30 seconds. This is not available on Windows NT.
-r	This flag is used to append a value is joined to the tail of a hard coded registry path. The resulting registry path points a Directory Proxy Server service to its configuration information such as the root or instance root name. On Windows systems only one instance of Directory Proxy Server can be installed on a host.
`-v`	This flag prints the version information for Directory Proxy Server. On Windows NT, this flag should be used from the command line only.

Restarting Directory Proxy Server

On UNIX platforms, Directory Proxy Server can be sent a `SIGHUP` signal to make it re-read its configuration. If the configuration is re-read successfully, Directory Proxy Server will use this new configuration for future connections. Client connections that are already established will continue to use the old configuration until the clients disconnect.

To signal Directory Proxy Server to re-read its configuration, use the `hup-dps` command found at `<server-root>/dps-<hostname>`.

Some attribute values cannot be changed using the `HUP` signal facility. For changes to the following configuration parameters, Directory Proxy Server will have to be shut down and started again. These attributes include:

```
ids-proxy-con-listen-port
ids-proxy-con-listen-host
ids-proxy-con-ldaps-port
ids-proxy-con-foreground
ids-proxy-con-listen-backlog
ids-proxy-con-ssl-cert
ids-proxy-con-ssl-key
```

Also, the logging properties `ids-proxy-sch-LogProperty` cannot be changed using this facility.

On all platforms, a `restart-dps` command is found at `<server-root>/dps-<hostname>`. The restart command simply invokes the `stop-dps` and `start-dps` commands found in the aforementioned directory.

Chapter 5

Creating System Configuration Instances

System parameters are those that affect the functional behavior of Sun ONE Directory Proxy Server. This chapter explains how to specify and save system configuration.

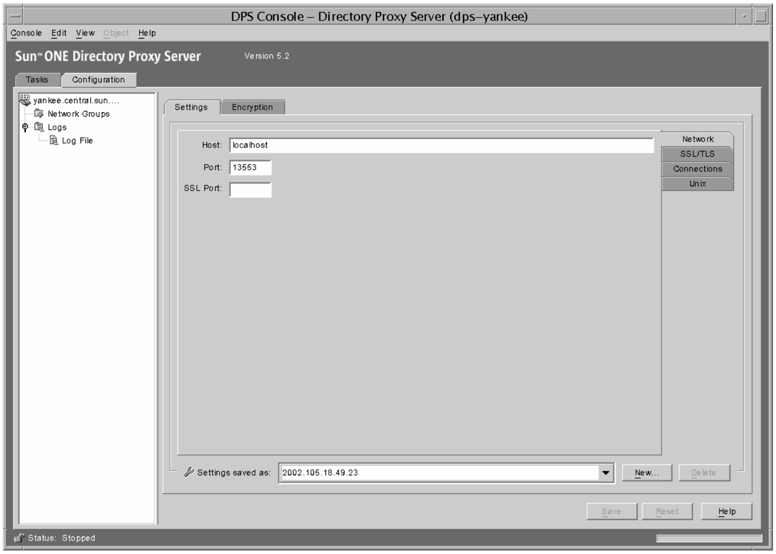
The chapter contains the following sections:

Creating System Configuration Instances

This section explains how to configure system-specific parameters of a Directory Proxy Server instance. To create an object for system configuration:

1. Access the Directory Proxy Server Console; see "Accessing the Directory Proxy Server Consoles," on page 36.
2. In the navigation tree, select the appropriate Directory Proxy Server instance and press Open.

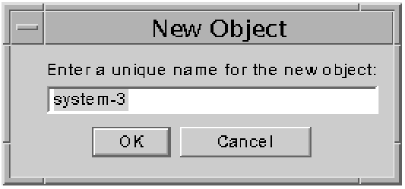
   At the Directory Proxy Server Console press the Configuration tab.



Host: localhost
Port: 13553
SSL Port:
Settings saved as: 2002.105.18.49.23

3. Click New.

   The New Object window appears.



Enter a unique name for the new object: system-3

4. In the Name field, type a name for the system configuration. The name must be a unique alphanumeric string. Press OK.

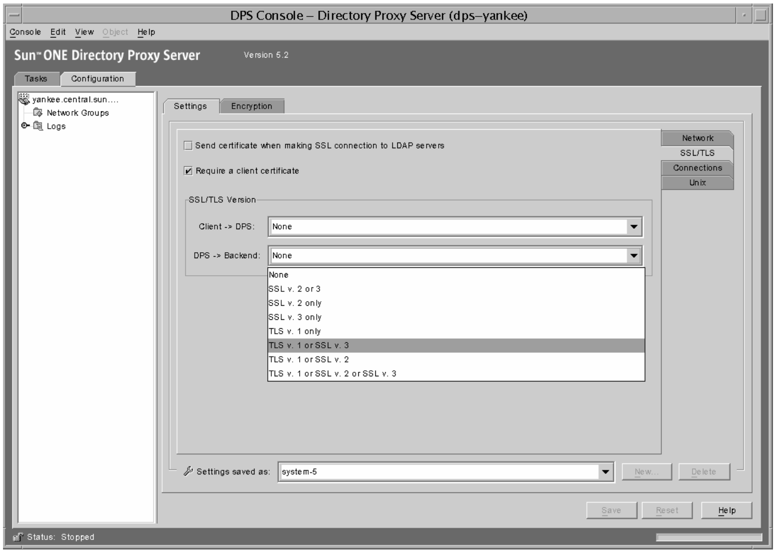
5. In the Network tab, specify general settings for this system configuration:

   Host. Enter the name of the host interface on which Directory Proxy Server will listen for connections. This attribute is needed only if there are multiple network interfaces on the host running Directory Proxy Server. By default, the hostname is set to “localhost,” meaning Directory Proxy Server will listen on all available network interfaces. Specifying “localhost” will permit shared system properties.

Port. Enter the port number on which Directory Proxy Server will listen for incoming connections. Legal values for this field are 1 through 65535. By default, the value is set to 389, as specified for LDAP. This port number must be different from that used by any other LDAP server running on the same host. On UNIX platforms the server must be started as root to listen on a port number below 1024.

SSL port. Enter a value representing the port number on which to listen for LDAPS (LDAP over SSL) connections. By default, Directory Proxy Server does not listen for connections from LDAPS clients. This value must be present to enable LDAPS connections from clients using this nonstandard function, with a value such as 636. This value must be different from the Host value. This option also requires TLS / SSL configuration, found on the Encryption tab.

6. Press the SSL / TLS tab.



☐ Send certificate when making SSL connection to LDAP servers

☑ Require a client certificate

SSL/TLS Version

Client -> DPS: None

DPS -> Backend: None

None
SSL v. 2 or 3
SSL v. 2 only
SSL v. 3 only
TLS v. 1 only
TLS v. 1 or SSL v. 3
TLS v. 1 or SSL v. 2
TLS v. 1 or SSL v. 2 or SSL v. 3

Settings saved as: system-5

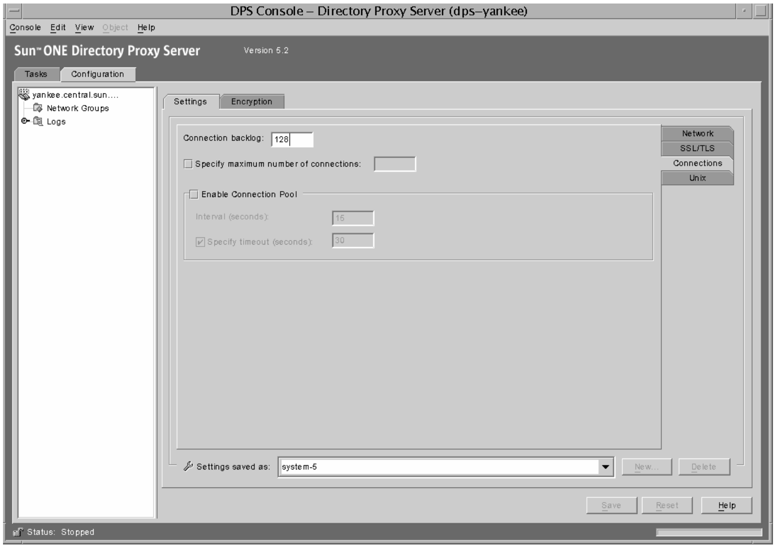
This displays the default configuration from which Directory Proxy Server sends to and requires from SSL certificates from servers and clients. Select entries for:

Send certificate when making SSL connection to LDAP sever. Enable this setting if you want Directory Proxy Server to send its certificate to the backend LDAP directory server when making a TLS connection. By default this setting is disabled.

Require a client certificate. Enable this setting to specify that Directory Proxy Server will require all clients that establish an SSL session to submit a certificate chain. Directory Proxy Server will close the connection if a certificate chain is not submitted. Note that this option does not effect SSL sessions between Directory Proxy Server and the backend servers. By default this setting is disabled.

SSL/TLS Version. Select the drop-down windows next to Client > Directory Proxy Server and Directory Proxy Server > Backend to select the appropriate SSL / TLS version for each case. You must specify a version if SSL is enabled for the system.

7. Press the Connections tab and specify how Directory Proxy Server should maintain its connections.



Connection backlog: 128

☐ Specify maximum number of connections:

☐ Enable Connection Pool

Interval (seconds): 15

☑ Specify timeout (seconds): 30

Settings saved as: system-5

Status: Stopped

This displays the Directory Proxy Server connection backlog value, allows you to specify a maximum number of connections, and set connection pool timeout values. Select entries for:

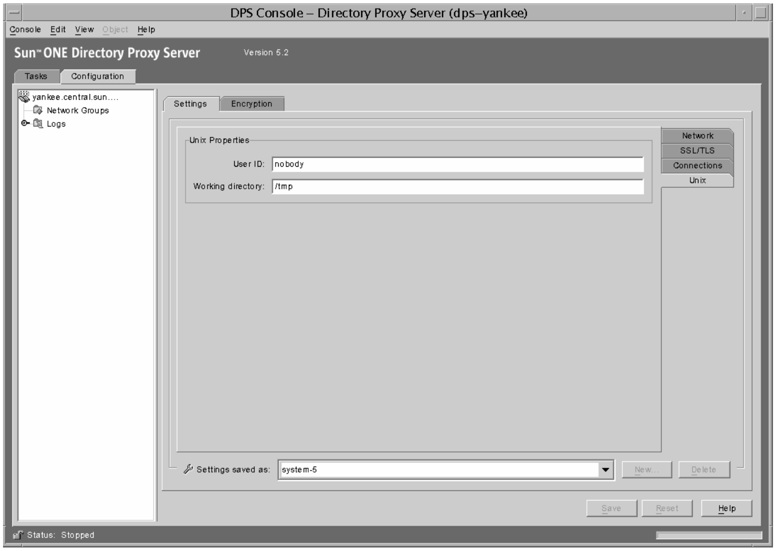
Connection backlog. Enter a value greater than zero specifying the maximum number of outstanding connections in the listening socket's queue. The default is 128 connections. The maximum value depends on the underlying operating system configuration.

Specify maximum number of connections. Select the option and enter a value (greater than zero) specifying the maximum number of simultaneous client connections that Directory Proxy Server will accept. To allow an unlimited number of simultaneous connections, do not select this option.

Enable Connection Pool. Enables the connection pool module with which Directory Proxy Server will preconnect to the directory servers. The default for the setting is disabled. If the connection pool is enabled, Directory Proxy Server will try to reuse existing connections to the backend LDAP servers. Switching on this option can give significant performance gain if the backend server is on a Wide Area Network (WAN). Enter the following values:

> **Interval.** Enter the number of seconds (greater or equal to one) specifying the interval in seconds at which Directory Proxy Server will sample the incoming requests to anticipate future activity. The default is 15.
>
> **Specify timeout.** Select the option and enter the number of seconds (greater or equal to zero) specifying the period of time in seconds after which an idle connection to an LDAP server will be terminated. If the checkbox is unchecked, no timeout will be applied. The default is 30. This value should be less than the idle connection timeout value of the backend LDAP server.

8. Press the UNIX Tab.



User ID: nobody

Working directory: /tmp

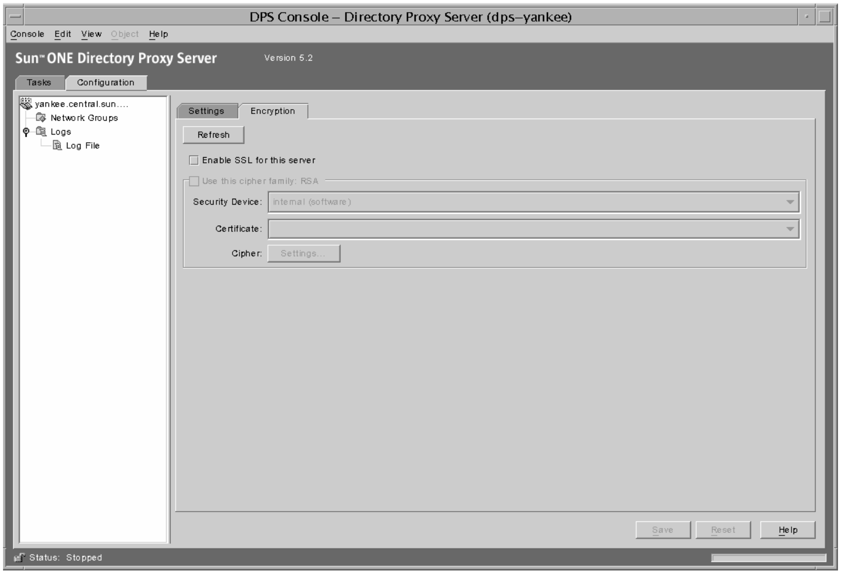
Settings saved as: system-5

This panel contains attributes that pertain to Directory Proxy Server servers in a UNIX environment only.

User ID. Enter the user ID under which Directory Proxy Server will run. If Directory Proxy Server was run as *root* then it will change its uid to the one specified here. The default is to switch to *nobody*. This option is not applicable on Windows NT.

Working directory. Enter the directory from which Directory Proxy Server should run. Directory Proxy Server will change its working directory to the directory specified as value for this attribute on startup. The default is `/tmp`. This attribute only takes effect on platforms other than Windows NT.

9. Select the Encryption tab and configure Directory Proxy Server for SSL-enabled communication. For information on configuring the server for SSL communication see Configuring Security.



☐ Enable SSL for this server

☐ Use this cipher family: RSA

Security Device: internal (software)

Certificate:

Status: Stopped

The Encryption Tab allows you to configure the following parameters:

Refresh. Click to refresh the current screen values. Refresh the screen to see newly created certificates.

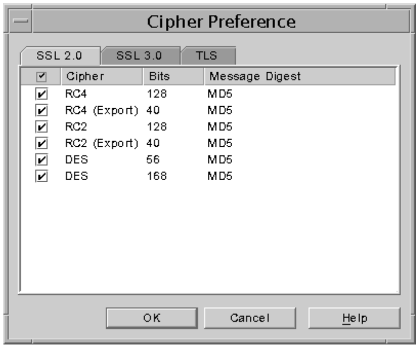
Enable SSL for this server. Select this box to enable SSL / TLS information needed by Directory Proxy Server to listen over a secure connection. If an SSL port is specified, you must enable this setting in order to save this configuration.

Use this cipher family RSA. Select this box to set the Security Device, Certificate, and Cipher Settings for this instance of Directory Proxy Server

Security Device. Click the drop-down window to select from available options. The default is internal (software).

Certificate. Click the drop-down window to select from available options.

Cipher. Select Settings to set SSL 2.0, SSL 3.0, and TLS Cipher Preferences. Press the SSL 2.0, SSL 3.0, and TLS tabs and select the box next to desired Ciphers for each.



☑	Cipher	Bits	Message Digest
☑	RC4	128	MD5
☑	RC4 (Export)	40	MD5
☑	RC2	128	MD5
☑	RC2 (Export)	40	MD5
☑	DES	56	MD5
☑	DES	168	MD5

10. Click Save to save the object.

The Directory Proxy Server configuration is modified, and you are prompted to restart the servers that rely on this configuration. Don’t restart the servers yet. You can do this after you’ve completed all the configuration changes.

11. Repeat Step 3 through Step 10 to create any additional objects.

12. Restart the servers; see “Restarting Directory Proxy Server,” on page 50.

NOTE Changes to Host, Port, and “SSL port” fields in the Settings tab require stopping and starting Directory Proxy Server.

For instructions to stop and start Directory Proxy Server, see “Starting and Stopping Directory Proxy Server,” on page 45.

Saving Configurations

The utility `dpsconfig2ldif` is used to download Directory Proxy Server configuration and save it in an LDIF file. The utility is found at the following location:

```
<Install Root>/bin/dps_utilities/dpsconfig2ldif
```

The utility requires two arguments:

Argument	**Meaning**
-t *filename*	*Filename* is the path to the startup configuration file. This will usually be the tailor.txt file in the etc directory.
-o *filename*	The name of the file in which to output the configuration.

Chapter 6

Creating and Managing Groups

When an LDAP client requests a service from an LDAP directory, it connects to Sun ONE Directory Proxy Server, which identifies the client's access rights from the client profile, determines whether the client is allowed to request the service from the directory, imposes configured restrictions, and then forwards the request to the appropriate directory. This chapter explains how to configure Directory Proxy Server to identify clients and impose any restrictions using the Directory Proxy Server Configuration Editor Console.

The chapter has the following sections.

Overview of Groups

Directory Proxy Server network groups are key to understanding how Directory Proxy Server works—they define how Directory Proxy Server should identify an LDAP client and what restrictions Directory Proxy Server should enforce on clients that match that group. It's important that you understand Directory Proxy Server groups clearly in order to use them to effectively control directory access by LDAP clients.

You use network groups to identify the following:

- A client
- A set of LDAP directories to which Directory Proxy Server can forward requests from a client.

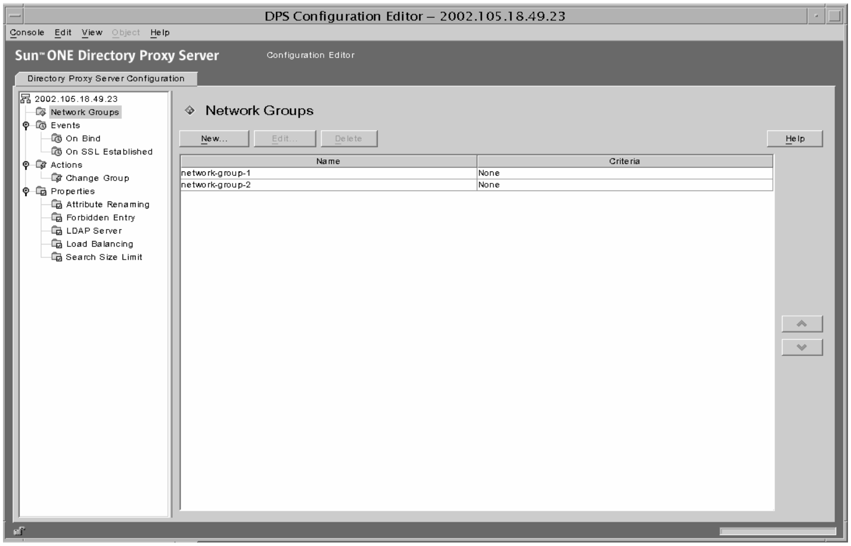
- A set of operations a client can perform while interacting with its set of directories.
- The data accessible to a client while interacting with its set of directories. (Because Directory Proxy Server enables you to hide certain entries and rename attributes in a directory, you can effectively control which data contained within a directory is viewable by a client.)

Directory Proxy Server determines the group membership for a client by attempting to match the connection's origination attributes with a group's criteria. The server checks currently-configured groups in the descending order of priority, from the highest to the lowest priority. The first network group criteria to match the connection's origination attributes receives the connection. For this reason, it's important to create separate groups for generic and specific criteria, and prioritize the groups from most specific to most general.

If no groups are found to match a client, the client's request is rejected and the connection is closed. For this reason, there must be at least one group entry in the Directory Proxy Server configuration.

The order of priority for groups is specified by their placement in the Network Groups window of the Directory Proxy Server Configuration Editor Console (see Figure 6-1). In this window, groups on the bottom of the list have less priority than those towards the top. The order of evaluation of groups with equal priority is undefined.

Figure 6-1 Directory Proxy Server Configuration Editor Console: Network Groups Window

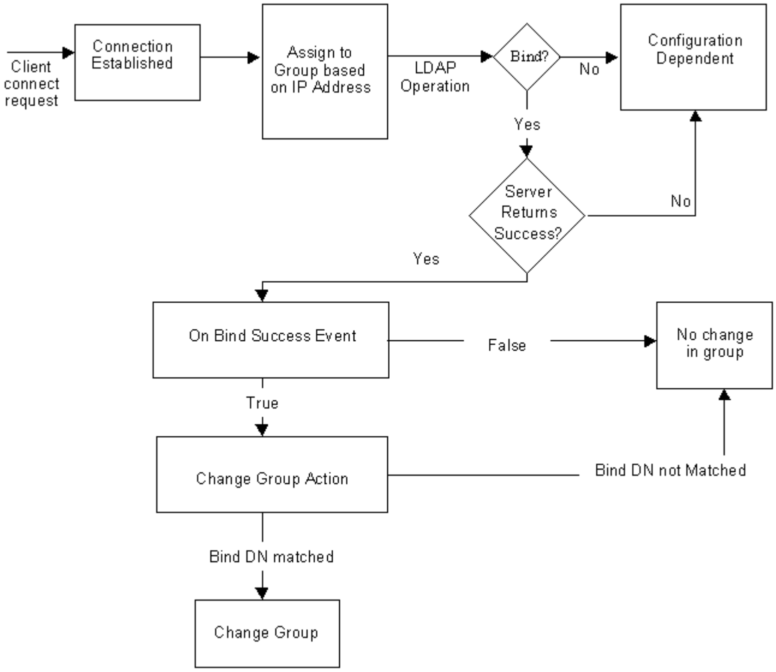


Name	Criteria
network-group-1	None
network-group-2	None

Note that clients are initially identified into a group based on the network address they connect from, for example, their IP address and/or domain name. They may change their group after a successful bind; for details, see Chapter 8, “Creating and Managing Event Objects.” Once a client obtains membership in a group, it implies that all the properties of the group apply to the client.

Figure 6-2 illustrates how groups are evaluated by Directory Proxy Server in response to a client query.

Figure 6-2 Directory Proxy Server Decision Tree for Determining Group Membership



Network criteria for groups can be based on the following:

- IP address or network mask of the hosts
  - Single IP address (for example, `129.153.129.14`)
  - IP quad/match bits (for example, `129.153.129.0/24`)
  - IP quad/match quad (for example, `129.153.129.0/255.255.255.128`)
- Domain name of the hosts
  - Full name (for example, `box.eng.sun.com`)
  - Suffix name (for example, `.eng.sun.com`)

Note that if the domain name suffix rule is used to identify clients, make sure that DNS is set up to return fully qualified names to the DNS queries. this feature will not work if short names are returned.

- Special
  - `ALL` (This is to be used for “catch-all” groups.)

- `0.0.0.0` (This is to be used for groups to which initial membership is not considered, for example, if a group is only used for clients to switch to when they bind.)

To further understand how Directory Proxy Server evaluates groups, take a look at the sample groups listed in Table 6-1. It shows five groups, created with specific to generic network criteria, and listed in the descending order of priority.

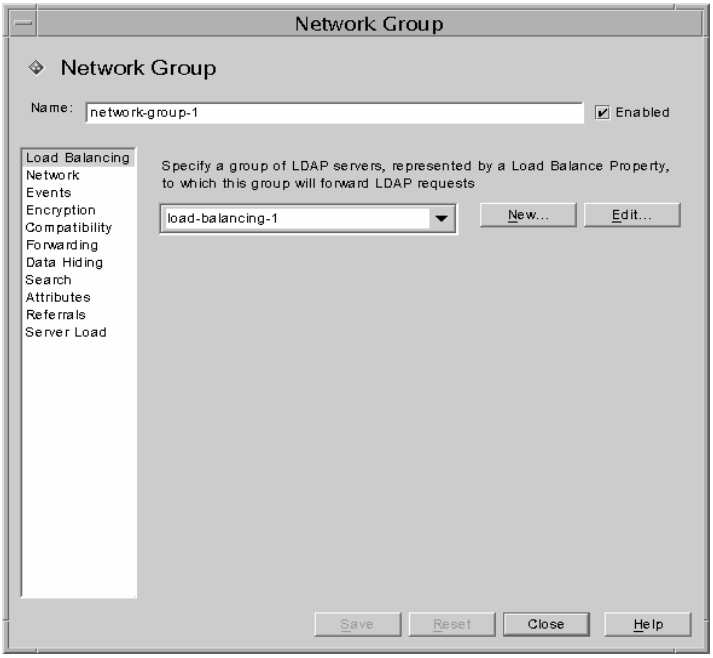
Table 6-1 Sample Groups

Priority	Group Name	Network Criteria
5	Admin-machine	129.153.129.72
4	IT-management-subnet	129.153.120.0/24
3	Operations	.ops.sun.com
2	Catch-all	ALL
1	Trusted	0.0.0.0

When an LDAP client requests a service from an LDAP directory, Directory Proxy Server checks whether the request is from IP address `129.153.129.72`. If it isn't, Directory Proxy Server checks whether the request matches `129.153.129.0/24`. If it does not, Directory Proxy Server checks whether the request originated from `.ops.sun.com`. If it didn't, Directory Proxy Server places the connection in a `catch-all` group, and then moves to the next step in the decision tree (see Figure 6-2).

Figure 6-3 shows that part of the Directory Proxy Server Configuration Editor Console where you are able to create groups.

Figure 6-3 Directory Proxy Server Network Group Definition



Name: network-group-1

☑ Enabled

Specify a group of LDAP servers, represented by a Load Balance Property, to which this group will forward LDAP requests

load-balancing-1

Notice that when creating a network group, you're given the opportunity to specify a combination of criteria. Table 6-2 summarizes them.

Table 6-2 List of Available Criteria for Network Groups

Criteria	Description
Load Balancing	Enables you to specify a group of LDAP servers represented by a load balance property to which this group forwards LDAP requests. "Load Balancing Property," on page 113.
Network	Enables you to specify connection details and other network criteria for clients so that their requests get sorted or filtered into the appropriate groups.
Events	Enables you to specify which events, if any, to associate with a group, so that clients in the group can effectively change group after binding successfully to a specified directory. Shows the list of existing objects for events; for details, see "Creating Groups," on page 72.

Table 6-2 List of Available Criteria for Network Groups *(Continued)*

Criteria	Description
Encryption	Enables you to specify encryption criteria for the group (for example, to specify whether clients can request an SSL session).
Compatibility	The LDAP v2 specification (RFC 1777) does not allow a client to bind multiple times in one session. However, some clients expect this functionality. This option can be set to interoperate with these clients.
Forwarding	Enables you to specify the criteria for passing the bind, compare, and other LDAP requests to the server.
Data Hiding	Enables you to specify which subtree, entries, or attributes of the entries in a directory are to be hidden from a group. Shows the list of existing objects for the Forbidden Entry property; for details, see "Forbidden Entry Property," on page 103.
Search	Enables you to specify the scope and size limit of searches for a group. Shows the list of existing objects for the Search Size Limit property; for details, see "Search Size Limit Property," on page 117.
Attributes	Enables you to specify rules for preventing certain kinds of search and compare operations from reaching the LDAP server. Shows the list of existing objects for the Attribute Renaming property; for details, see "Attribute Renaming Property," on page 100.
Referrals	Enables you to specify whether a group should forward, follow, or discard referrals returned by the server. Note that a client that does not implement LDAPv3 will not understand forwarded referrals. This setting applies to all referrals except for the search-continuation referrals.
Server Load	Enables you to specify details such as the total number of connections to a group, simultaneous and total operations per connection, simultaneous operations per IP address, and so on.

Creating Groups

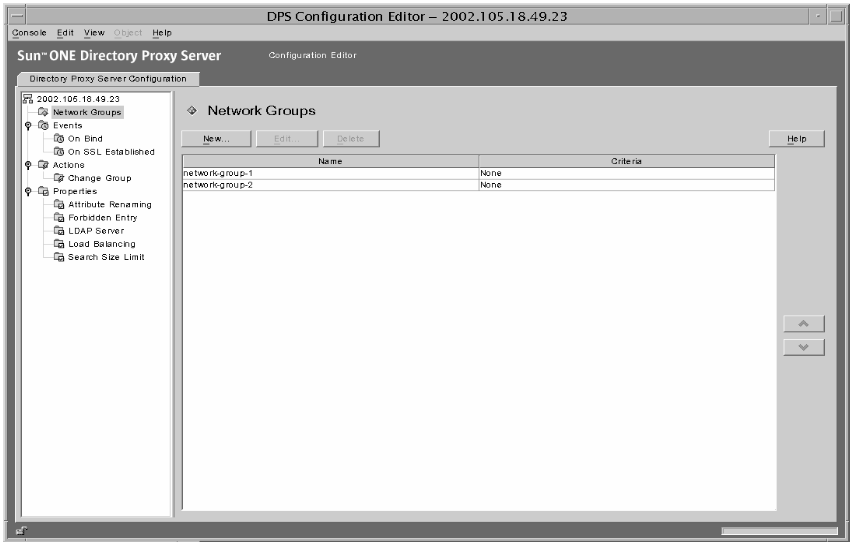
This section explains how to create groups using the Directory Proxy Server Configuration Editor Console. Before you start creating a group, be sure to read section “Overview of Groups,” on page 65 and understand the significance of Directory Proxy Server groups. After you create the required groups and prioritize them, be sure to test the configuration to see if the groups filter client requests as desired.

Notice that when creating a network group, you’re given the opportunity to specify a variety of criteria. The instructions provided in this section present all these criteria in the order in which they appear on the UI, and rely on your judgement to set the appropriate criteria for a group.

To create a network group in Directory Proxy Server, follow these steps:

1. Access the Directory Proxy Server Configuration Editor Console; see “Accessing the Directory Proxy Server Consoles,” on page 36.
2. In the navigation tree, select Network Groups.

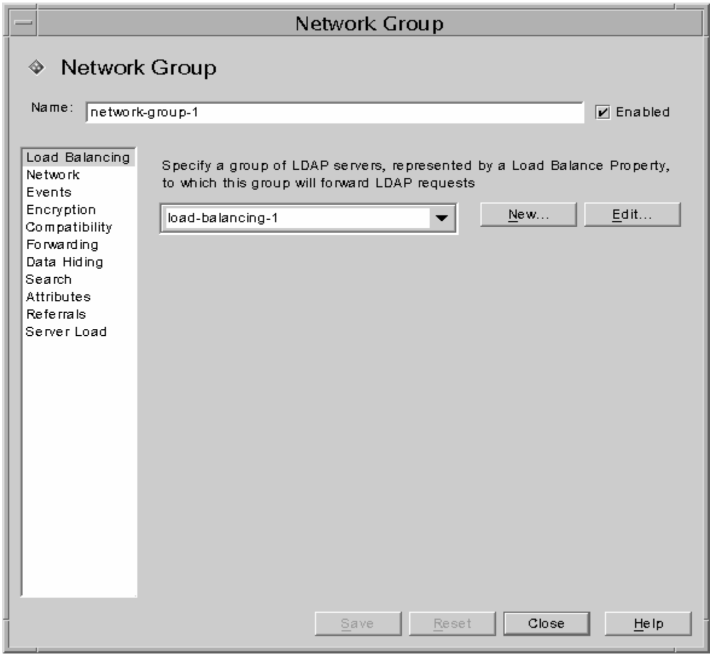
   The right pane shows the list of existing groups.



Name	Criteria
network-group-1	None
network-group-2	None

3. Click New.

   The Network Group window appears.



Name: network-group-1

Specify a group of LDAP servers, represented by a Load Balance Property, to which this group will forward LDAP requests

load-balancing-1

4. In the Name field, type a name for the group. The name must be a unique alphanumeric string.

5. Make sure that the Enabled option is selected; by default, it is selected. For a group to be part of an Directory Proxy Server configuration, this option must be selected. Deselect the option to disable the group in a configuration.

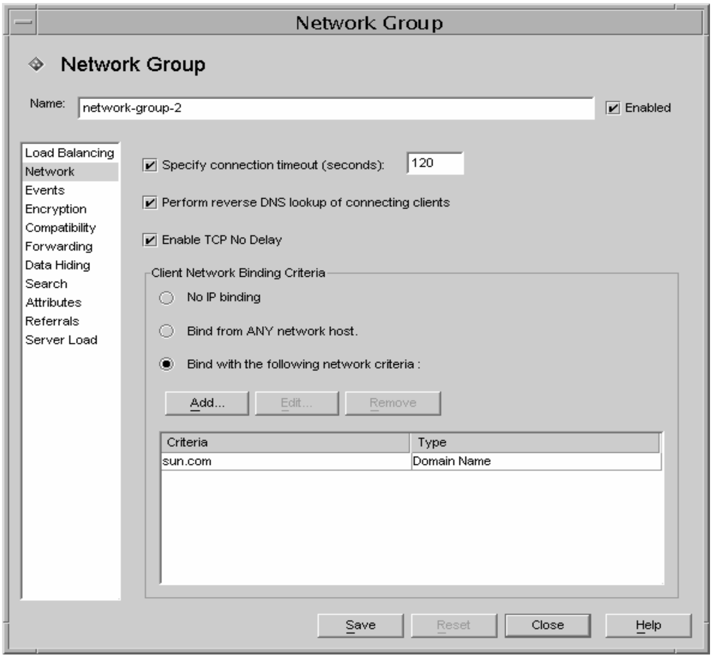
6. If desired, specify a load balancing property from the drop-down menu. This property identifies a group of LDAP servers to which this group will forward LDAP requests to use a Load Balance property to handle requests from clients. The associated drop-down list shows existing objects for the Load Balance property; see “Load Balancing Property,” on page 113. Select an appropriate object. By default, no (<NONE>) objects are selected. If there isn’t an object, you can create one on the fly by clicking on the New button.

   New. Displays a dialog to create a new Load Balance property.

   Edit. Displays a dialog to edit an existing Load Balance property.

7. To specify network criteria for the group to sort or filter requests, select Network on the left frame. Then specify the appropriate network values as follows referring to the on-screen elements description:

- Specify a connector timeout value. By default, no value is present, which also means to not timeout connections.
- Enable reverse DNS lookup for connecting clients.
- Select Enable TCP no delay.
- Define the Client Network Binding Criteria.



Name: network-group-2 ☑ Enabled

☑ Specify connection timeout (seconds): 120

☑ Perform reverse DNS lookup of connecting clients

☑ Enable TCP No Delay

Client Network Binding Criteria

○ No IP binding

○ Bind from ANY network host.

● Bind with the following network criteria :

Criteria	Type
sun.com	Domain Name

The description of the on-screen elements is as follows:

Specify connection timeout. Select this box if you want to enter a period of client inactivity after which Directory Proxy Server may close the connection to the client. The value must be a number in seconds, typically 120 or more. By default, no value is present, which also means to not timeout connections. Note that if TCP keepalives are not enabled, this attribute must be present to keep Directory Proxy Server from being clogged by lost client connections.

Perform reverse DNS lookup of connecting clients. By default, this option is enabled. If Reverse DNS lookup is disabled, Directory Proxy Server will not perform a reverse DNS lookup to find the domain name of the connecting client. Disabling Reverse DNS lookup can sometimes significantly improve Directory Proxy Server performance. If you have used a domain name or a domain name suffix as a value in the "Client Network Binding Criteria," you must not disable Reverse DNS lookup, otherwise Directory Proxy Server will not function properly. DNS must be configured to return full host names to lookup queries.

Enable TCP no delay. By default, this option is enabled. If the option is disabled, then Directory Proxy Server will disable the Nagle Algorithm for connections between itself and clients that fall into this group. "TCP no delay" should be disabled only if the network bandwidth between Directory Proxy Server and clients is small; however, it may create substantial performance degradation.

Client Network Binding Criteria. Use this section to specify which clients are able to bind in this network group.

No IP binding. Select this option if clients are to switch only when they bind to the group. By default, this option is selected. De-select the option if the group is only used for clients to switch to when they bind.

Bind from ANY network host. Select this option if all hosts are allowed to bind with this network group.

Bind with the following criteria. Select this option to specify the domain names or IP addresses of the hosts that match the network group; in this case, the group must specify the domain name or IP address of the host that will bind to it.

Add. Displays a dialog to add a network criteria. There are four options: "Domain Name," "IP address," "IP address and bits," and "IP address and quad."

Edit. Displays a dialog to edit a network criteria.

Remove. Displays a dialog to remove a network criteria.

Domain name dialog. Specify the domain name suffix or the full name of the client that can bind to a network group, for example, `foo.sun.com`. Note that Directory Proxy Server does not assume any domain suffix by default; hence, complete domain names must be provided. A domain name suffix with a leading period, for example, `.sun.com` will cause all hosts with domain names that end in that suffix to match.

Also note that if the domain name suffix rule is used to identify clients, make sure that DNS is set up to return fully qualified names to the DNS queries. this feature will not work if short names are returned.

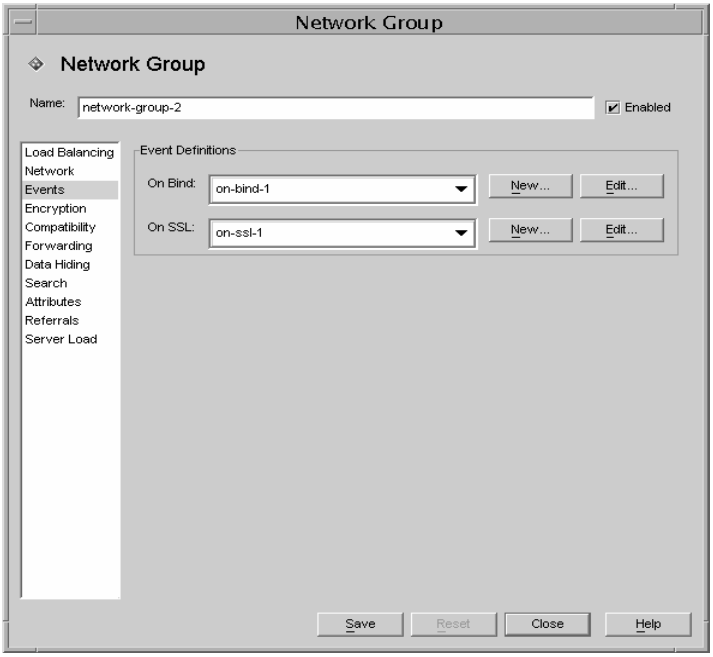
IP address. Specify a single IP address in dotted decimal form, for example, `198.214.11.1`.

IP address and bits. Specify an IP network mask, in the form of `<network number>/<mask bits>`, for example, `198.241.11.0/24`. The first half is the network number and the second half indicates the number of bits of the network number necessary for matching.

IP address and quad. Specify an IP network mask, in the form of a pair of dotted decimal quads, for example, `198.241.11.0/255.255.255.128`. The first half is a network number, the second half indicates the bits of the network number necessary for matching. For example, `198.214.11.0/255.255.255.128` will match a host with IP address `198.214.11.63` but not the one with IP address `198.214.11.191`.

Note that use of domain names or domain name suffixes requires “Perform reverse DNS lookup of connecting client” to be enabled.

8. If you want to associate an event-driven action with the group (for example, to change clients from one group to another), select Events on the left frame and specify the appropriate values on the right frame.



Network Group

Name: network-group-2

☑ Enabled

Event Definitions

On Bind: on-bind-1

On SSL: on-ssl-1

The description of the on-screen elements is as follows:

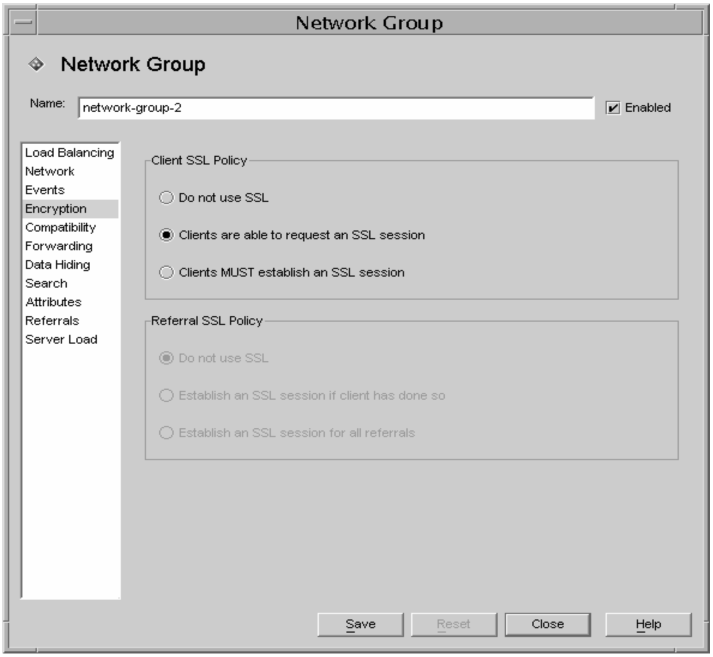
On bind. The drop-down list shows existing objects for OnBindSuccess events; see “Creating OnBindSuccess Event Objects,” on page 124. Select the name of an object that will be performed when a client successfully completes a bind operation. By default, no (<NONE>) objects are selected. If there isn’t an object, you can create one on the fly by clicking on the New button.

On SSL. The drop-down list shows existing objects for OnSSLEstablished events; see “Creating OnSSLEstablished Event Objects,” on page 127. Select the name of an object that will be performed when a client successfully establishes an SSL session. If there isn’t an object, you can create one on the fly by clicking on the New button.

Edit. Displays a dialog box for editing the behavior of an event.

New. Displays a dialog box for creating a new event.

9. If you want to specify encryption criteria for the group (for example, to specify whether clients can request an SSL session), select Encryption on the left frame and specify the appropriate values on the right frame.



Name: network-group-2 ☑ Enabled

Client SSL Policy

○ Do not use SSL

● Clients are able to request an SSL session

○ Clients MUST establish an SSL session

Referral SSL Policy

● Do not use SSL

○ Establish an SSL session if client has done so

○ Establish an SSL session for all referrals

The description of the on-screen elements is as follows:

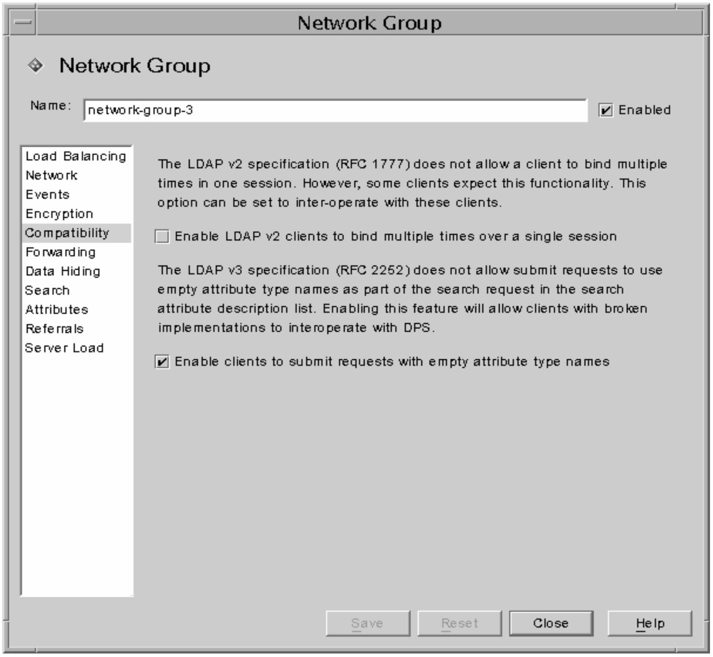
Client SSL Policy. Configure the client SSL policy.

- **Do not use SSL.** Select this option if you do not wish to use SSL encryption.
- **Clients are able to request an SSL session.** Select this option if the clients in the group will establish an SSL session requesting SSL.
- **Clients MUST establish an SSL session.** Select this option if the clients in the group must establish an SSL session before performing any operation.

Referral SSL policy. Configure the SSL policy while following referrals.

- **Do not use SSL.** Select this option if you do not wish to use SSL encryption.
- **Establish an SSL session if client has done so.** If this option is enabled, Directory Proxy Server will only initiate SSL for clients in that group if the client already has an SSL session established with Directory Proxy Server.
- **Establish an SSL session for all referrals.** Enable this option, if, upon a referral, Directory Proxy Server will initiate an SSL session before the operation is forwarded.

10. If you want to specify compatibility criteria for the group (for example, to allow a client to bind multiple times in one session), select Compatibility on the left frame and specify the appropriate values on the right frame.



Name: network-group-3 ☑ Enabled

The LDAP v2 specification (RFC 1777) does not allow a client to bind multiple times in one session. However, some clients expect this functionality. This option can be set to inter-operate with these clients.

☐ Enable LDAP v2 clients to bind multiple times over a single session

The LDAP v3 specification (RFC 2252) does not allow submit requests to use empty attribute type names as part of the search request in the search attribute description list. Enabling this feature will allow clients with broken implementations to interoperate with DPS.

☑ Enable clients to submit requests with empty attribute type names

The description of the on-screen element is as follows:

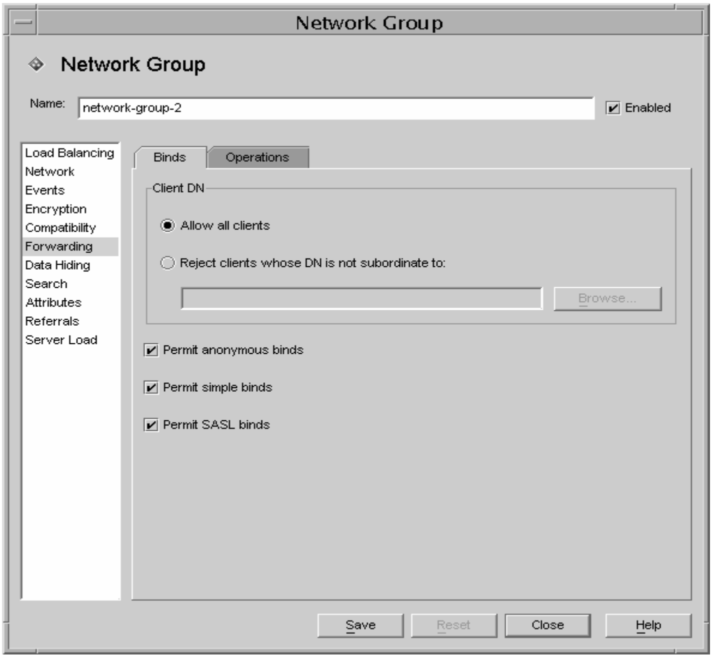
Enable LDAP v2 clients to bind multiple times over a single session. The LDAP v2 specification (RFC 1777) does not allow a client to bind multiple times in one session. However, some clients expect this functionality. Select this if you want this group to allow clients to submit search request with one or more attributes in the attribute request list as NULL. This compatibility feature allows Directory Proxy Server to interoperate with some broken JAVA based clients. Note that NULL attribute names in attribute request list is in violation of the LDAP protocol. By default this option is set to TRUE.

Enable clients to submit requests with empty attribute type names. Select this if you want the group to allow a client to submit requests even if they do not identify their attribute type name.

11. If you want to specify request-forwarding criteria for the group, select Forwarding on the left frame and specify the appropriate values on the right frame.

Once Directory Proxy Server has accepted a connection from the client and matched a group, it will wait for the client to send the LDAP operation. Directory Proxy Server uses the “Client DN,” “Permit Anonymous binds,” “Permit simple binds,” and “Permit SASL binds” to determine whether to pass the bind request to the server, or reject the bind request and close the client’s connection.

If the client’s bind passes enabled tests, Directory Proxy Server will forward it to the server. If the server accepts the bind, the connection is established. If, however, the server returns an error indication for the bind request, Directory Proxy Server will forward the error indication to the client, and then close the connection to the client, if the client was using LDAPv2.



Name: network-group-2

☑ Enabled

● Allow all clients

○ Reject clients whose DN is not subordinate to:

☑ Permit anonymous binds

☑ Permit simple binds

☑ Permit SASL binds

The description of the elements in the Binds tab is as follows:

Allow all clients. By default, this option is enabled, which permits access by all clients.

Reject clients whose DN is not subordinate to. Select this option if you want the group to check for a distinguished name (DN). Any client that provides a distinguished name in its bind that is not subordinate to a the specified DN will be rejected. Use the Browse button to browse an LDAP directory in order to construct a DN.

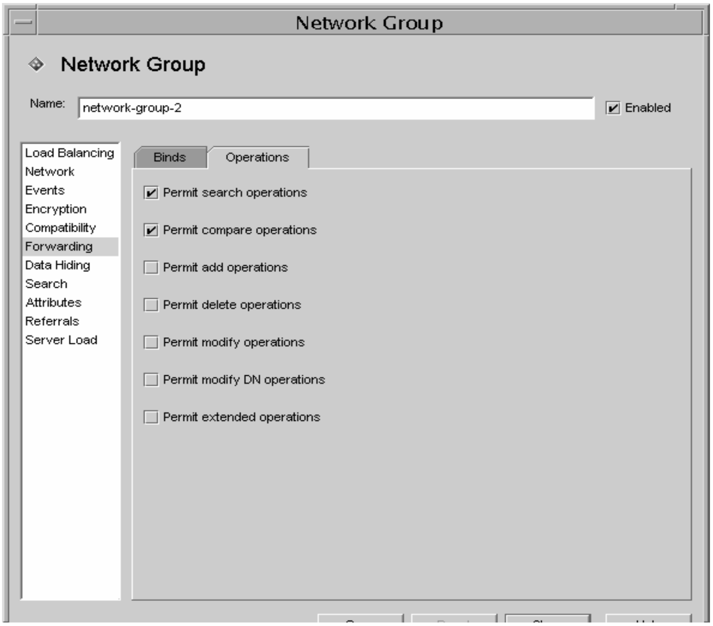
Permit anonymous binds. By default, this option is enabled, which permits a bind even if a client has not supplied a password. Disable the option to forbid anonymous binds.

Permit simple binds. By default, this option is enabled, which permits a client to supply a password in the clear. Disable the option to forbid clear text password authenticated bind requests.

Permit SASL binds. By default, this option is enabled, which specifies that SASL binds are permitted. Disable the option to forbid SASL authentication.

12. Select the Operations tab and specify which operations are to be forwarded.

Directory Proxy Server by default forwards search and compare requests. Directory Proxy Server also recognizes an unbind request and closes the connection to the LDAP server.



Name: network-group-2 ☑ Enabled

☑ Permit search operations

☑ Permit compare operations

☐ Permit add operations

☐ Permit delete operations

☐ Permit modify operations

☐ Permit modify DN operations

☐ Permit extended operations

The description of the elements in the Operations tab is as follows:

Permit search operations. By default, this option is enabled. Disable the option to prevent Directory Proxy Server from forwarding search requests to the server.

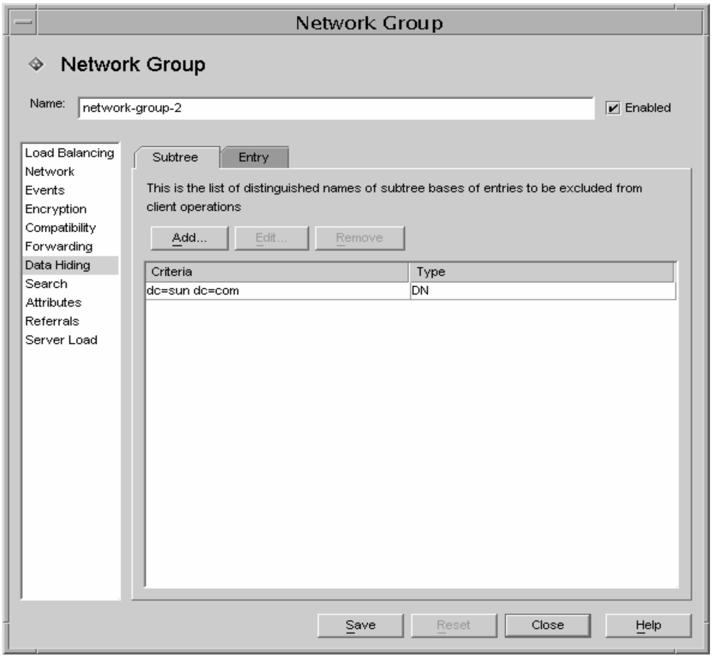
Permit compare operations. By default, this option is enabled. Disable the option to prevent Directory Proxy Server from forwarding compare requests to the server.

Permit add, delete, modify, modify DN, and extended operations. By default, Directory Proxy Server does not forward add, modify, delete, modify DN, or extended operations requests. To permit forwarding of these operations, enable the appropriate operation to be allowed.

Note that you must enable "Permit extended operations" if you want your clients to be able to negotiate Start TLS.

13. If you want to specify data hiding criteria for the group, select Data Hiding on the left frame and specify the appropriate values on the right frame.

    Use the Subtree tab to specify which part of the directory tree is to be hidden and Entry tab to specify entries or attributes to be hidden.



Name: network-group-2

☑ Enabled

This is the list of distinguished names of subtree bases of entries to be excluded from client operations

Criteria	Type
dc=sun dc=com	DN

The description of the elements in the Subtree tab is as follows:

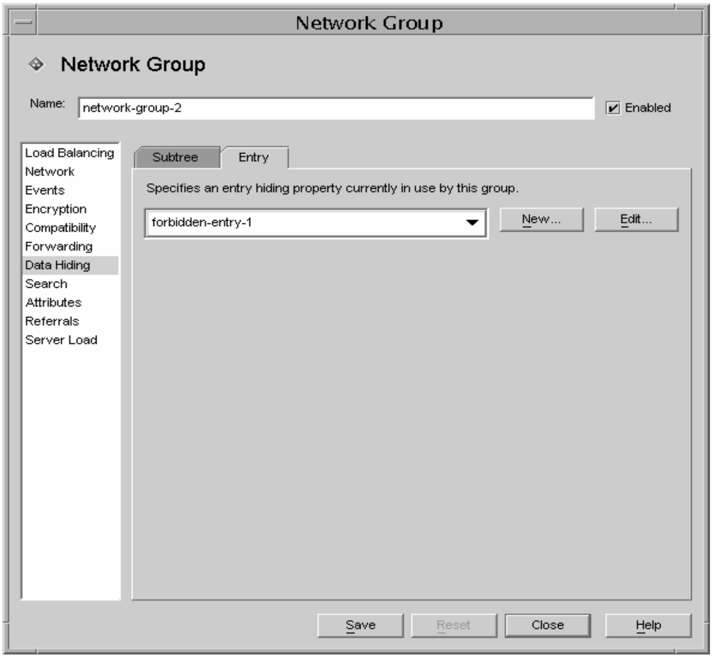
Hiding a subtree of entries. Operations that request entries at or below a forbidden subtree will be rejected with an insufficient access error. Entries that match a search filter and are inside a forbidden subtree are dropped. Note that this option does not remove DN syntax attributes whose values fall under the subtree from entries that are being returned as part of the result.

Add. Displays a dialog box to add a distinguished name to a list of the base of a subtree of entries to be excluded. The default, if distinguished names are not present in a network group, is to allow access to all entries in the directory. An entry in the list has dn syntax.

Edit. Displays a dialog box to edit a distinguished name.

Remove. Removes a distinguished name from the list.

14. Select the Entry tab and specify which entries or attributes are to be hidden.



Network Group

Network Group

Name: network-group-2

☑ Enabled

Specifies an entry hiding property currently in use by this group.

forbidden-entry-1

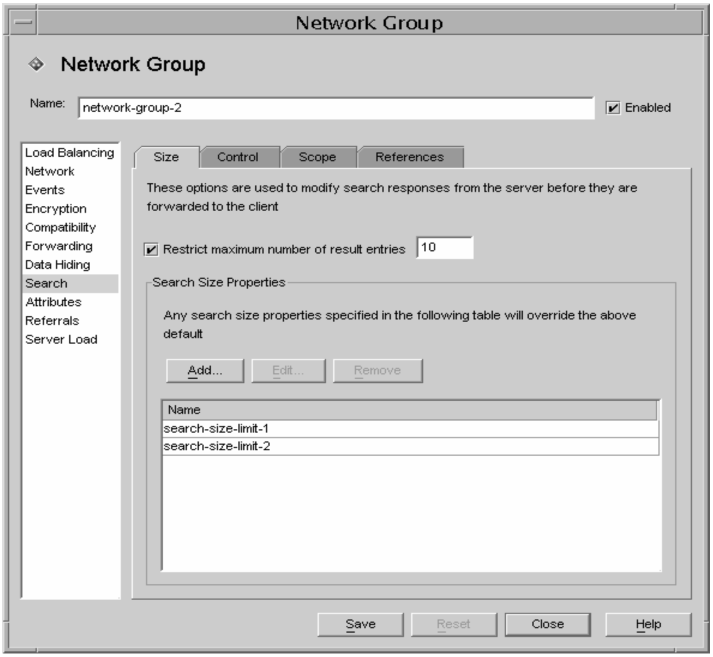
The description of the elements in the Entry tab is as follows:

Specifies an entry hiding property currently in use by this group. The drop-down list shows existing objects for the Forbidden Entry property; see "Forbidden Entry Property," on page 103. Select the name of an object. By default, no (<NONE>) objects are selected. If there isn't an object, you can create one on the fly by clicking on the New button.

New. Displays a dialog to create a new Forbidden Entry property.

Edit. Displays a dialog to edit an existing Forbidden Entry property.

15. If you want to specify search attributes for the group, select Search on the left frame and specify the appropriate values on the right frame.



Network Group

Name: network-group-2

☑ Enabled

These options are used to modify search responses from the server before they are forwarded to the client

☑ Restrict maximum number of result entries 10

Search Size Properties

Any search size properties specified in the following table will override the above default

Name
search-size-limit-1
search-size-limit-2

The description of the elements in the Size tab is as follows:

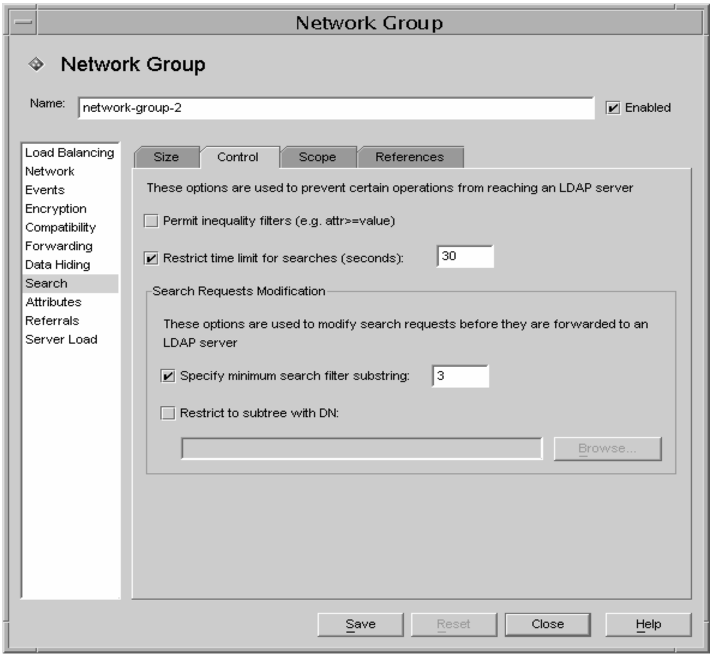
Restrict maximum number of result entries. Enable this option to specify the maximum number of result entries that may be returned to a client at one time from a single search operation. The value may be any number greater than zero, and if reached, will cause an `administrativeLimitExceeded` error to be indicated to the client and subsequent entries will be discarded. The default, if this property is disabled, is to not discard entries.

Add. Displays a dialog to add a Search Size Limit property. For details, see "Search Size Limit Property," on page 117.

Edit. Displays a dialog to edit a Search Size Limit property.

Remove. Displays a dialog to remove a Search Size Limit property. (This action removes the property from the group without displaying a dialog.)

16. Select the Control tab and specify the criteria for controlling search filters.



Name: network-group-2

☑ Enabled

These options are used to prevent certain operations from reaching an LDAP server

☐ Permit inequality filters (e.g. attr>=value)

☑ Restrict time limit for searches (seconds): 30

Search Requests Modification

These options are used to modify search requests before they are forwarded to an LDAP server

☑ Specify minimum search filter substring: 3

☐ Restrict to subtree with DN:

The description of the elements in the Control tab is as follows:

Permit inequality filters. By default, this option is enabled. Permit inequality filters specifies whether clients are permitted to request searches that contain inequality filters (`attr>=value`) and (`attr<=value`). Disable this option if a network group does not permit inequality searches to be performed.

Restrict time limit for searches. Enable this option and enter a value in seconds for a network group to specify a maximum time limit in seconds for search operations. If the client specifies a time limit that is larger than the value given in this option, the value specified for this network group will override the client’s request. By default, this option is disabled and a network group will allow the client to set any time limit, including no limit.

Specify minimum search filter substring. Enable this option and enter a value to specify the minimum permissible length of a substring in a search filter. The value is a number greater than one. The default, if this option is disabled, is to allow any size of substring in a search filter. This option should be enabled in the network group if you wish to restrict the kinds of searches that may be performed by web robots. For example, a value of 2 will block searches like (`cn=A*`).

NOTE This attribute does not affect presence filters (attrname=*). To disallow certain presence filters use the forbidden compare configuration.

Restrict to subtree with DN. Enable this option and specify the base of a subtree for all operations. This option has dn syntax. If this option is disabled, then there is no restriction to a minimum base.

Operations whose target entry is at or below the minimum base entry are not affected by this option. If the target entry is superior to the minimum base entry, and the operation is a subtree search, then the query will be rewritten before being sent to the server, to change the target entry to be the minimum base. If the target entry is not below the minimum base or a superior of it, the request will be rejected with a no such object error.

For example, if the “Restrict to subtree with DN” is set as:

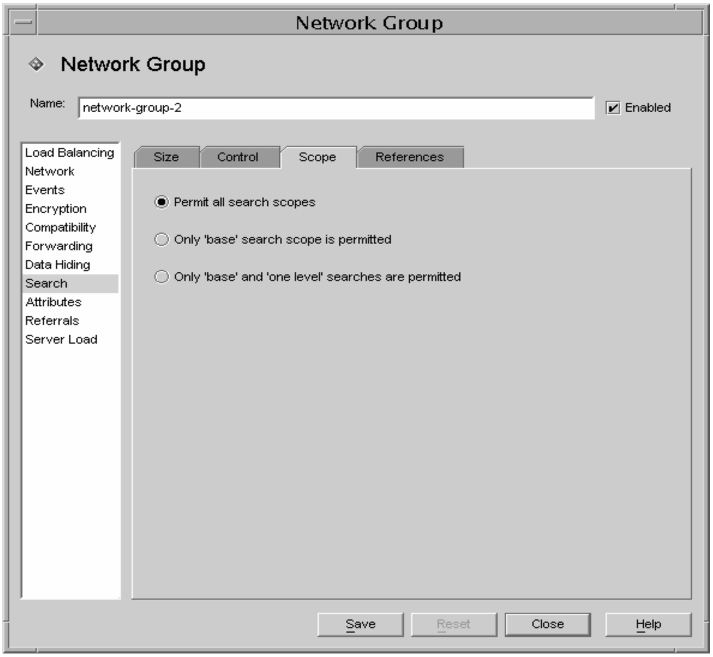
```
o=sun, st=California, c=US
```

and a subtree search of `st=California, c=US` is received, the search will be rewritten such that the server performs a subtree search of

```
o=sun, st=California, c=US
```

Browse. Displays a dialog to aid in constructing a valid DN.

17. Select the Scope tab and specify the search scope (that a client may specify in a search request).



Name: network-group-2

☑ Enabled

● Permit all search scopes

○ Only 'base' search scope is permitted

○ Only 'base' and 'one level' searches are permitted

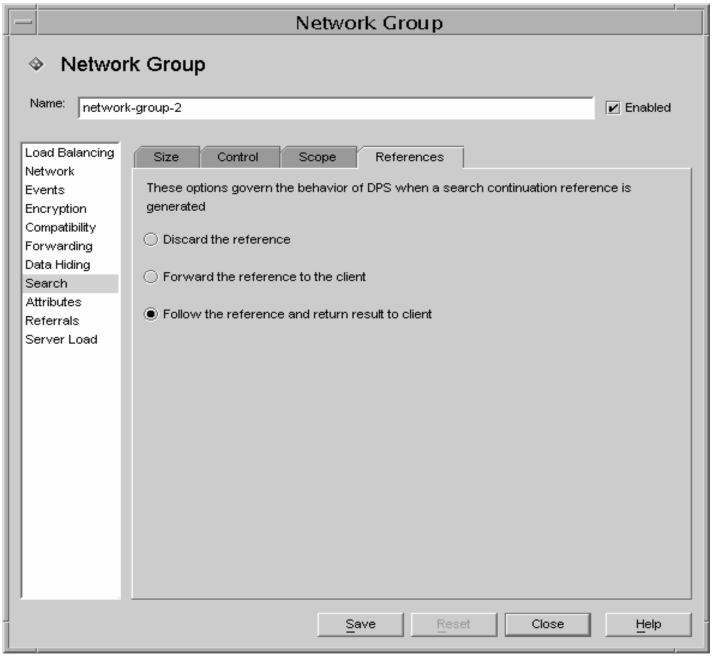
The description of the elements in the Scope tab are as follows:

Permit all search scopes. By default, this option is enabled, permitting all search scopes by a client.

Only 'base' search scope is permitted. Enable this option to permit only base search scope.

Only 'base' and 'one level' searches are permitted. Enable this option to permit only base and one level searches.

18. Select the References tab and specify what to do if a search-continuation reference is generated during a search.



Network Group

Name: network-group-2 ☑ Enabled

These options govern the behavior of DPS when a search continuation reference is generated

○ Discard the reference

○ Forward the reference to the client

● Follow the reference and return result to client

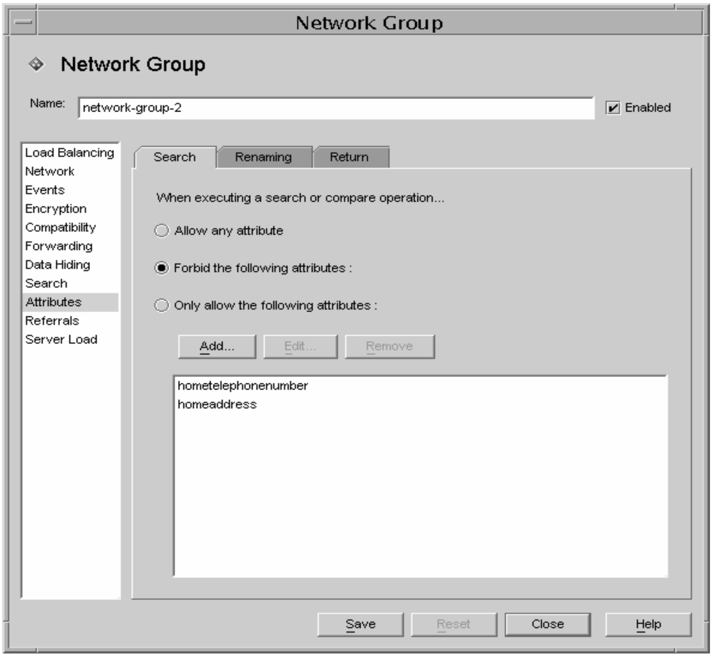
The description of the elements in the References tab is as follows:

Discard the reference. By default, this option is enabled, which will discard a reference if it is generated during a search.

Forward the reference to the client. Enable this option only to forward a search continuation reference.

Follow the reference and return result to client. Enable this option to follow and return the result for a search continuation reference. A search continuation referral is a special case of a referral whereby part of the query has been satisfied by the original directory server queried but that directory server has a reference to another directory server with more data satisfying the query. This option can be used to hide the part of your Directory Information Tree whose naming context is mastered by another LDAP server. It also prevents clients from finding out the network address and port on which this server runs.

19. If you want to specify attribute criteria for the group, select Attributes on the left frame and specify the appropriate values on the right frame.



Name: network-group-2 ☑ Enabled

When executing a search or compare operation...

○ Allow any attribute

● Forbid the following attributes :

○ Only allow the following attributes :

hometelephonenumber
homeaddress

The description of the elements in the Search tab is as follows:

This tab is used to prevent certain kinds of search and compare operations from reaching the LDAP server. If the client's request falls under this restriction, Directory Proxy Server will return an insufficient access error to the client.

Allow any attribute. By default, this option is enabled to permit all attributes to be used for search filters and comparisons.

Forbid the following attributes. Enable this option to specify the name of an attribute or attributes that cannot be used by a client in a search filter or compare request.

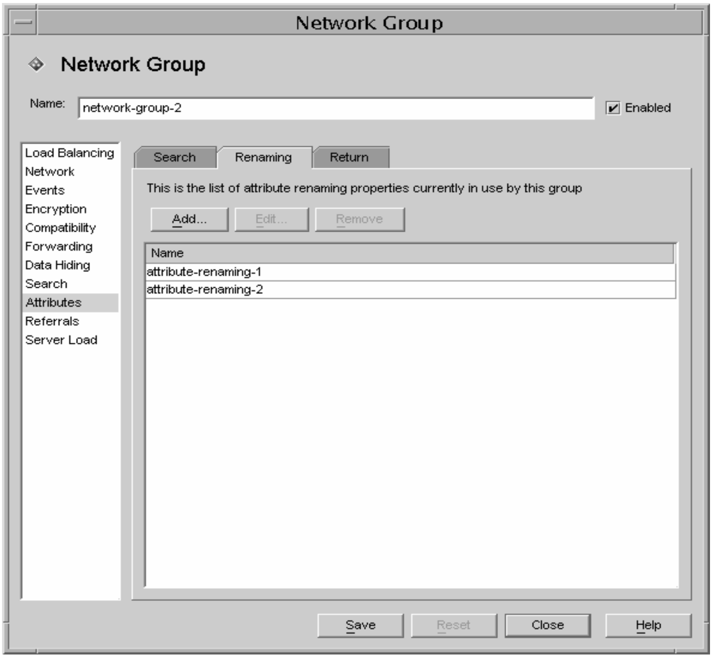
Only allow the following attributes. Enable this option to specify the name of an attribute or attributes that may be used in a search filter or compare request. If there is one or more attributes values present in a network group table and a compare does not match one of these, the request will be rejected by Directory Proxy Server. If there are no attributes present in a network group table, and an attribute does not match any attributes, then it may be used by clients. For example, if you want only the cn, dn, and mail attributes to be searchable by the client, add these attributes to the table.

Add. Displays a dialog box that allows an attribute to be added to the table. You must specify whether these attributes are to be forbidden or permitted.

Edit. Displays a dialog box to edit a selected attribute in the table.

Remove. Removes an attribute from the table.

20. Select the Renaming tab and specify the rules for renaming of attributes.



Name: network-group-2

☑ Enabled

This is the list of attribute renaming properties currently in use by this group

Name
attribute-renaming-1
attribute-renaming-2

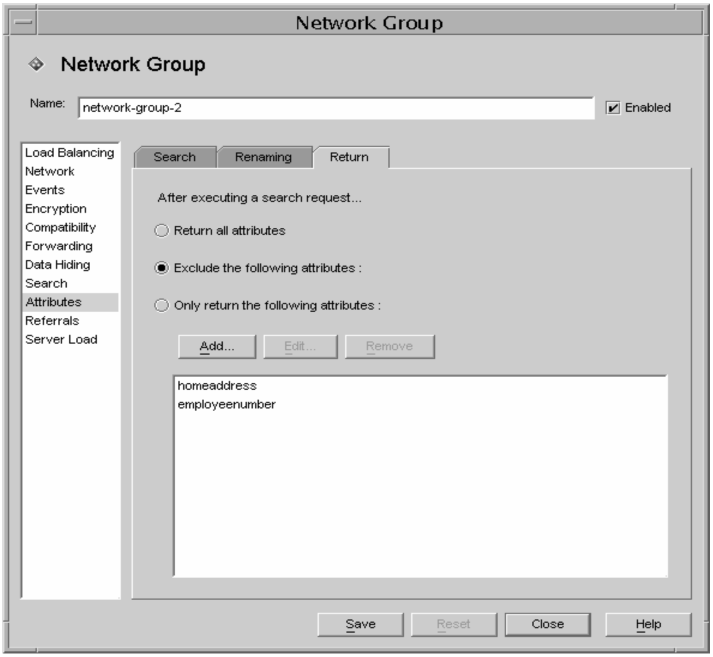
The description of the elements in the Renaming tab is as follows:

Add. Displays a dialog box to add one or more existing attribute renaming properties to the following table that will be used by this network group. (See “Attribute Renaming Property,” on page 100.)

Edit. Displays a dialog box to edit a selected attribute renaming property.

Remove. Remove an attribute renaming property from the table.

21. Select the Return tab and specify restrictions that are to be applied to search results being returned by the server, before they are forwarded to the client.



Name: network-group-2

☑ Enabled

After executing a search request...

○ Return all attributes

● Exclude the following attributes :

○ Only return the following attributes :

homeaddress
employeenumber

The description of the elements in the Return tab is as follows:

Return all attributes. This option is enabled by default, and it will permit all attributes to be returned.

Exclude the following attributes. Enable this option to specify the name of the attributes that are to be excluded from search result entries.

Only return the following attributes. Enable this option to specify the name of attributes that may be returned from a search result, if present.

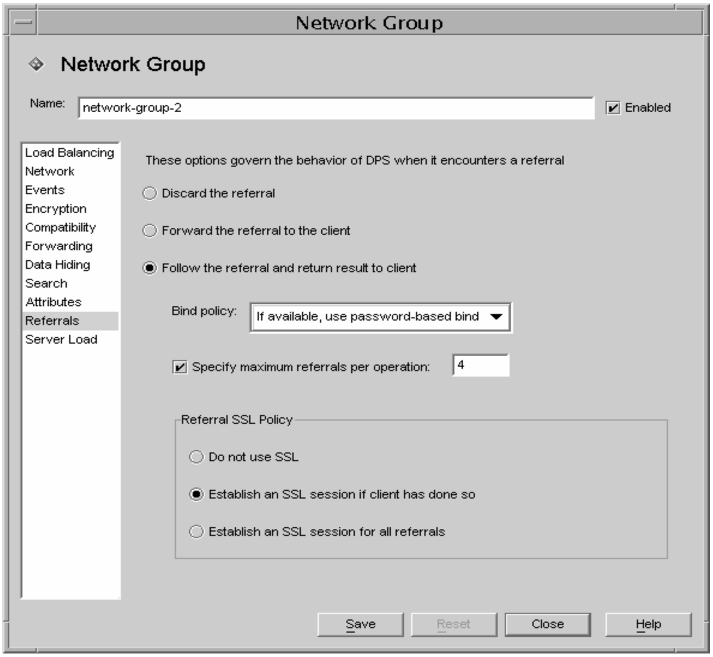
If attributes returned as part of a search result are not present in the “Only return the following attributes” table, they are not returned. If the table is empty and they are not in the “exclude the following attributes” table, they are returned.

Add. Displays a dialog box that allows an attribute to be added to the table. You must specify above whether these attributes are to be forbidden or permitted.

Edit. Displays a dialog box to edit a selected attribute in the table.

Remove. Removes an attribute from the table.

22. If you want to specify referrals for the group (for example, whether the group will forward, follow, or discard referrals returned by the server), select Referrals on the left frame and specify the appropriate values on the right frame.



Network Group

Name: network-group-2

☑ Enabled

These options govern the behavior of DPS when it encounters a referral

○ Discard the referral

○ Forward the referral to the client

● Follow the referral and return result to client

Bind policy: If available, use password-based bind

☑ Specify maximum referrals per operation: 4

Referral SSL Policy

○ Do not use SSL

● Establish an SSL session if client has done so

○ Establish an SSL session for all referrals

The description of the on-screen elements is as follows:

Discard the referral. Enable this option if a network group will discard all referrals returned by the server.

Forward the referral to the client. By default, this option is enabled, which will forward referrals returned by the server.

Follow the referral and return result to client. Enable this option if a network group will forward referrals returned by the server and return results to the client.

Bind policy. This option controls the bind policy when an operation is referred and the referral is being followed.

Note that Directory Proxy Server cannot replay binds for clients bound using a SASL mechanism. Thus the referral operation will be rejected if “Required” is specified and the client used a SASL mechanism to bind.

Always. Select this option if Directory Proxy Server should always bind anonymous while following a referral for a client connected to this network group.

Any. Select this option if a network group should use simple bind if the client had used password-based bind, else bind as anonymous. This is the default.

Required. Select this option if a network group should reject the referred operation if the client is not password-based bound.

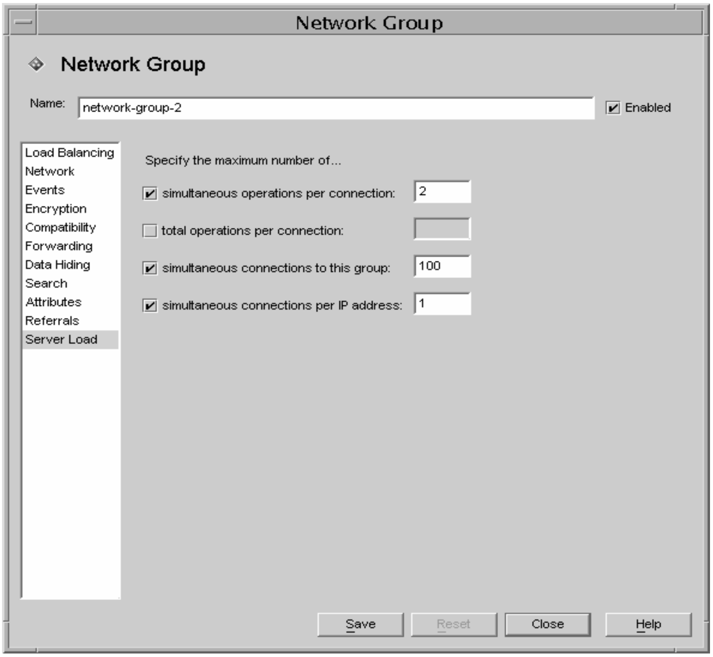
Maximum referrals per operation. Enter an integer value greater or equal to zero. This will limit the maximum number of references that will be followed for a single operation. The default is 15. A value of zero indicates that no limit will be applied.

Referral SSL Policy. In order to enable the Referral SSL Policy Panel, "SSL is available" option must be enabled on the encryption view.

If client has an SSL session established. Enable this option if a network group will only initiate SSL if the client already has SSL session established with Directory Proxy Server. This is the default.

For all referrals. Enable "For all referrals" if, upon a referral, a group will initiate an SSL session before the operation is forwarded.

23. If you want to specify server load criteria for the group, select Server Load on the left frame and specify the appropriate values on the right frame.



Name: network-group-2 ☑ Enabled

Specify the maximum number of...

☑ simultaneous operations per connection: 2

☐ total operations per connection:

☑ simultaneous connections to this group: 100

☑ simultaneous connections per IP address: 1

The description of the on-screen elements is as follows:

Simultaneous operations per connection. Select this option to limit the number of simultaneous operations Directory Proxy Server will process per connection in that group. The value is an integer greater than zero. If this attribute is not present, then no limit is enforced. For example, if you set this value to 1, all the clients in that group will be forced to perform synchronous LDAP operations. Additional simultaneous requests, except for requests to abandon an operation, will fail with Server Busy error.

Total operations per connection. Select this option to limit the total number of operations that Directory Proxy Server will allow per connection in a group. The value is an integer greater than zero. If a client exceeds the maximum number of operations allowed for its group on one connection, then that connection will be closed by Directory Proxy Server. If this attribute is not present, then no limit is set.

Connections to this group. Select this option to limit the number of simultaneous connections to this network group, and specify the number.

Simultaneous connections per IP address. Select this option to restrict the number of simultaneous connections clients can make from a single IP address. By default, any number of connections are allowed.

24. Click Save to create the group.

    The Directory Proxy Server configuration is modified, and you are prompted to restart the servers that rely on this configuration. Don’t restart the servers yet. You can do this after you’ve completed all the configuration changes.

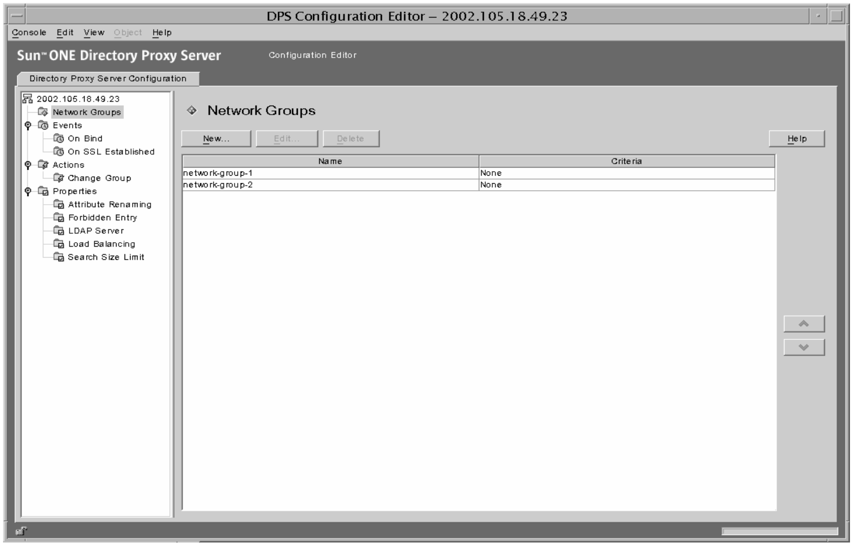
25. Repeat Step 3 through Step 24 to create any additional groups.
26. Go to the Network Groups window (see Step 2) and prioritize the groups appropriately.
27. Restart the servers; see “Restarting Directory Proxy Server,” on page 50.

Modifying Groups

To modify a group:

1. Access the Directory Proxy Server Configuration Editor Console; see “Accessing the Directory Proxy Server Consoles,” on page 36.
2. In the navigation tree, select Network Groups.

   The right pane shows the list of existing groups.



Name	Criteria
network-group-1	None
network-group-2	None

3. In the list, select the group you want to modify and click Edit.
4. Make the required modifications.

5. Click Save to save your changes.

   The Directory Proxy Server configuration is modified, and you are prompted to restart the servers that rely on this configuration. Don't restart the servers yet. You can do this after you've completed all the configuration changes.

6. Repeat Step 3 through Step 5 to modify any additional groups.

7. Restart the servers; see "Restarting Directory Proxy Server," on page 50.

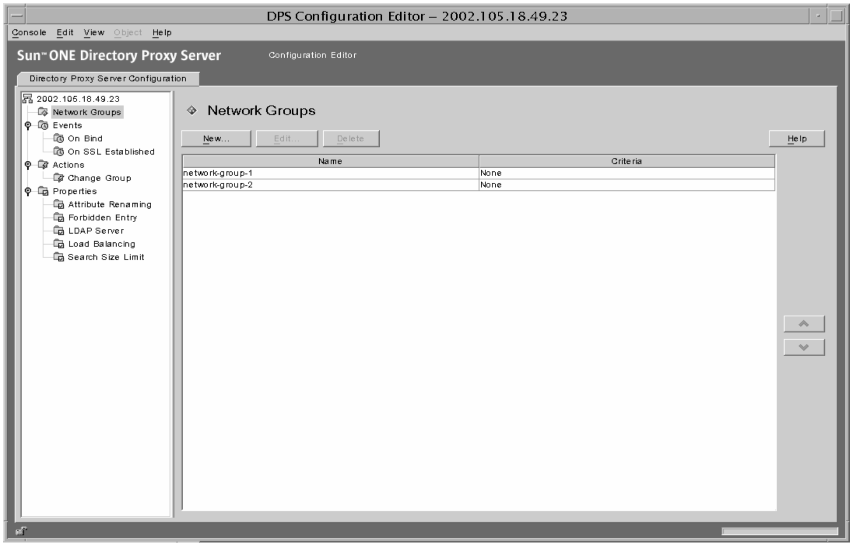
Deleting Groups

You can delete any unwanted network groups from the Directory Proxy Server configuration. To delete a group:

1. Access the Directory Proxy Server Configuration Editor Console; see "Accessing the Directory Proxy Server Consoles," on page 36.

2. In the navigation tree, select Network Groups.

   The right pane shows the list of existing groups.



Name	Criteria
network-group-1	None
network-group-2	None

3. In the list, select the group you want to delete and click Delete.

4. Confirm your action.

   The name of the group you deleted is now removed from the list. The Directory Proxy Server configuration is modified, and you are prompted to restart the servers that rely on this configuration. Don't restart the servers yet. You can do this after you've completed all the configuration changes.

5. Repeat Step 3 and Step 4 to delete any additional groups.

6. Restart the servers; see "Restarting Directory Proxy Server," on page 50.

Chapter 7

Defining and Managing Property Objects

As explained in the deployment chapter of this book, Sun ONE Directory Proxy Server can function as an *LDAP access router*, helping you protect your private directory information from unauthorized access, while making it safe for you to publish your public information. The server can handle thousands of LDAP client requests and can apply fine-grained access control rules and protocol filtering rules to each request before routing it to a directory server.

Property objects in Directory Proxy Server enable you to specify specialized restrictions that the LDAP clients must follow. These properties can then be included in other entries where the restrictions need to be applied. This chapter provides an overview of each of the properties and explains how to create property objects using the Directory Proxy Server Configuration Editor Console.

The chapter has the following sections:

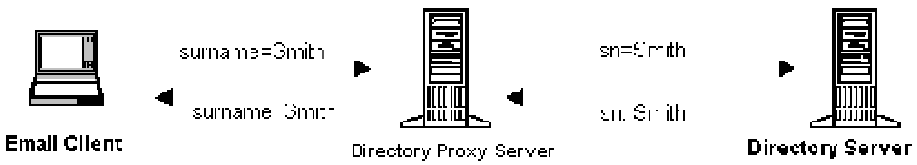
Attribute Renaming Property

Typically, an LDAP directory contains information about entities such as people in your organization and your network resources. For each entity, there would be an entry in the directory. Each entry in a directory is identified by its distinguished name (DN) and is represented by a set of attributes and their values. Each entry has an object class attribute that specifies the kind of object the entry describes and defines the set of additional attributes it contains. Each attribute describes a particular trait or characteristic of an entry. For example, an entry might be of an object class `organizationalPerson`, indicating that the entry represents a person within a particular organization. This object class allows the `givenname` and `telephoneNumber` attributes. The values assigned to these attributes give the name and phone number of the person represented by the entry.

In many directory deployments, the attributes defined on the LDAP client side don't map to the ones defined on the server side. To facilitate communication between the clients and servers in such a setup, Directory Proxy Server supports renaming of attributes—that is, Directory Proxy Server can rename attributes in a client query to a form understood by a directory server before passing the query to a directory server, and do the same in the server response before passing it to a client.

Figure 7-1 illustrates how attribute renaming feature of Directory Proxy Server can be used for schema mapping.

Figure 7-1 Mapping Schema Using the Attribute Renaming Property



Notice that the email client expects the last names of people to be the value of an attribute named "surname," whereas in the LDAP server, the last names are specified by the attribute named "sn." When Directory Proxy Server maps these two attributes, only the attribute names are affected; the attribute values remain unchanged.

You use the Attribute Renaming property to define the rules that govern renaming of client and server attributes. You specify the names of the client attributes that need to be mapped to the corresponding server attributes and vice versa. This way, if a client request contains an attribute name unknown to the server, Directory Proxy Server would be able to map it to a name known to the server and help the client communicate with the server. Similarly, when the server responds back, Directory Proxy Server would translate any attributes that are unknown to the client to known forms.

The section that follows explains how to create an object for the attribute renaming property from the Directory Proxy Server Configuration Editor Console.

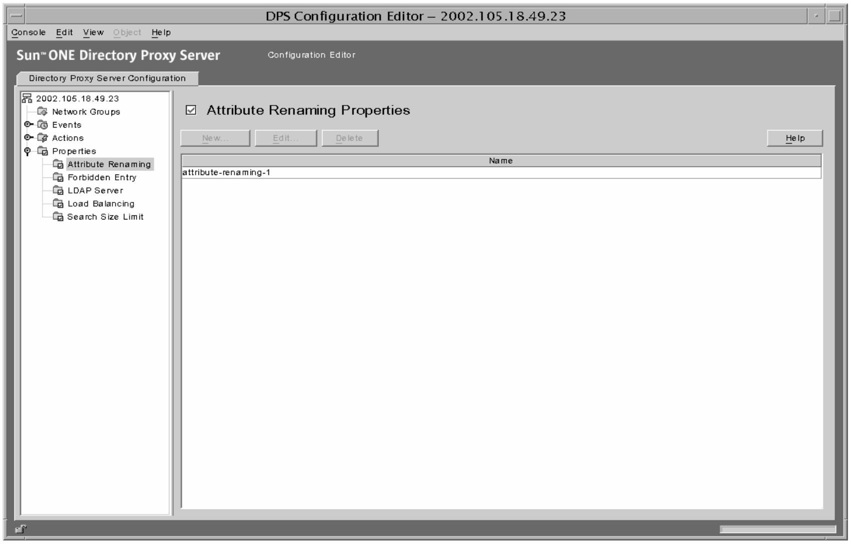
NOTE Any object you create for the attribute-renaming property must have both server and client attributes. Otherwise, Directory Proxy Server will fail to start.

Creating Attribute Renaming Property Objects

To identify the client and server attributes that Directory Proxy Server should rename:

1. Access the Directory Proxy Server Configuration Editor Console; see "Accessing the Directory Proxy Server Consoles," on page 36.
2. In the navigation tree, expand the Properties node, and then select Attribute Renaming.

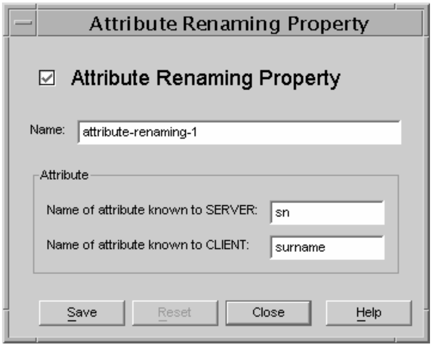
   The right pane shows the list of existing objects for the attribute renaming property.



Name
attribute-renaming-1

3. Click New.

   The Attribute Renaming Property window appears.



Name: attribute-renaming-1

Name of attribute known to SERVER: sn

Name of attribute known to CLIENT: surname

4. In the Name field type, a name for the property object. The name must be a unique alphanumeric string.

NOTE Attribute names can only be in 7 bit characters.

---

5. In the remaining fields, identify the attributes for mapping:

   Attribute renaming values may be written as decimal digits with components separated by periods; for example `2.5.4.10`. Attribute renaming values may also assign one or more textual names for an attribute type. These names must begin with a letter, and may only contain ASCII letters, digit characters, and hyphens. The value is case insensitive.

   Name of attribute known to SERVER. Enter a value to specify the name of the attribute known to the server.

   Name of attribute known to CLIENT. Enter a value to specify the name of the attribute known to the client.

   If a client request contains an attribute name specified by the “Name of attribute known to CLIENT,” it will be transformed to the value of “Name of attribute known to SERVER.” Similarly, if a result sent by the server contains an attribute name specified in “Name of attribute known to SERVER,” it will be transformed to the value of “Name of attribute known to CLIENT.”

6. Click Save to create the object.

   The Directory Proxy Server configuration is modified, and you’re prompted to restart the servers that rely on this configuration. Don’t restart the servers yet. You can do this after you’ve completed all the configuration changes.

7. Repeat Step 3 through Step 6 to create any additional objects.

8. Restart the servers; see “Restarting Directory Proxy Server,” on page 50.

Forbidden Entry Property

For various reasons, certain entries (or the attributes that represent these entries) in an LDAP directory will need to be hidden from the LDAP clients. For example, if your directory contains entries for all the employees and each of these entries contain relevant attributes for employee data, such as the name, email address, department, office location, office phone number, and home phone number, you can hide all employees’ home phone numbers from being visible to clients.

A forbidden entry refers to an entry in an LDAP directory that needs to be hidden from LDAP clients. To facilitate communication between the clients and directory servers in such a setup, Directory Proxy Server supports forbidden entries—that is, Directory Proxy Server can hide LDAP entries and the attributes of these entries from LDAP clients.

You use the Forbidden Entry property to define the rules that govern hiding of directory entries and their attributes. This property enables you to specify a list of entries or the attributes of the entries that need to be hidden in several ways. For example, you can specify:

- DNs of entries or attributes in those entries that you want to hide.
- Regular expressions of DNs of entries or attributes in those entries that you want to hide (for example, `.*OU=INTERNAL.*`).
- Attribute name/value pairs of an entry (for example, `secret:yes`). If an entry has an attribute name/value pair that matches any of the specified attribute name/value pairs, then that entry or some of its content will be hidden.

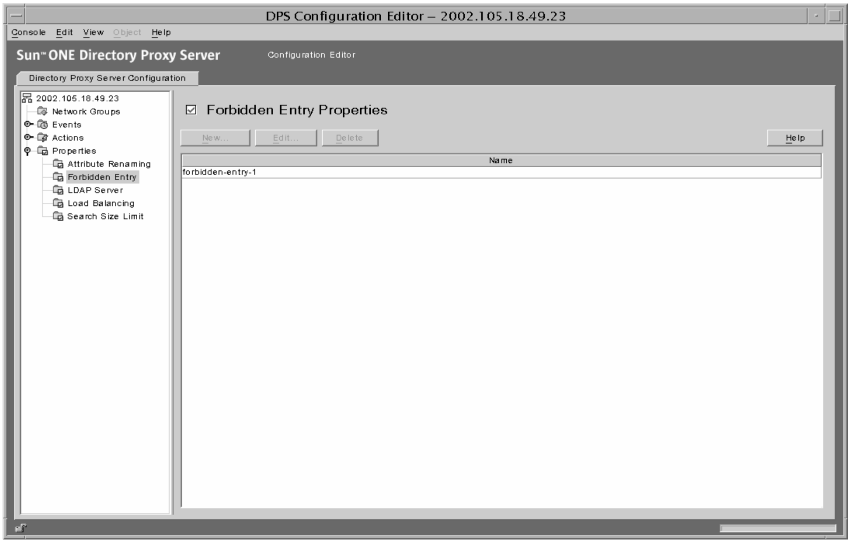
The section that follows explains how to create an object for the forbidden entry property from the Directory Proxy Server Configuration Editor Console.

Creating Forbidden Entry Property Objects

To identify the entries or attributes of any entries that Directory Proxy Server should hide from clients:

1. Access the Directory Proxy Server Configuration Editor Console; see "Accessing the Directory Proxy Server Consoles," on page 36.
2. In the navigation tree, expand the Properties node, and then select Forbidden Entry.

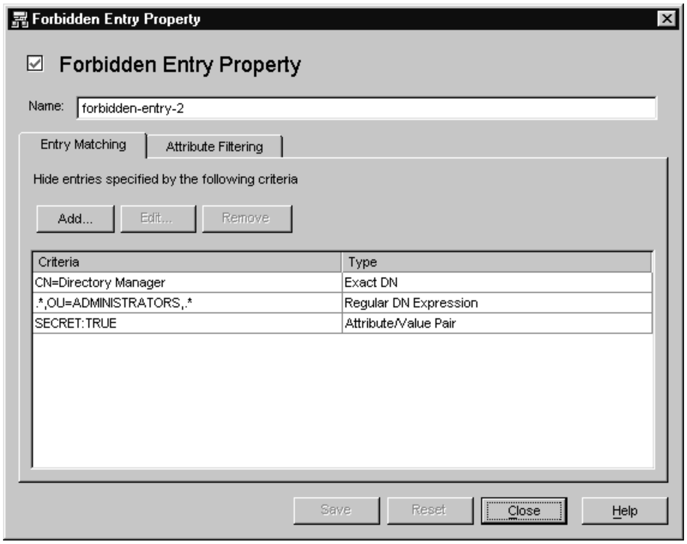
   The right pane shows the list of existing objects for the forbidden entry property.



Name
forbidden-entry-1

3. Click New.

   The Forbidden Entry Property window appears.



Name: forbidden-entry-2

Hide entries specified by the following criteria

Criteria	Type
CN=Directory Manager	Exact DN
.*,OU=ADMINISTRATORS,.*	Regular DN Expression
SECRET:TRUE	Attribute/Value Pair

4. In the Name field type a name for the property object. The name must be a unique alphanumeric string.

5. In the Entry Matching tab, specify the appropriate values; the tab displays settings for this property’s name and LDAP entries to hide.

Add. Displays a menu for adding criteria for hiding LDAP entries. Criteria can be of the following type: Exact DN, Regular DN Expression, or Attribute/Value Pair. You may type in an entry or browse the Directory Information Tree for existing entries.

Exact DN. Displays a dialog for entering the DN of an entry to hide.

Regular DN expression. Displays a dialog for entering a regular DN expression of entries to hide. The regular expression of the DN should be specified in the normalized form; that is, there should be no spaces between RDN components and the "=" sign and attribute names and values must be in all capital letters.

For example, to match any DN with a RDN component of "ou=internal," you must specify the following:

.*OU=INTERNAL.*

If the Attribute Filtering tab contains attribute names to be included, and an attribute does not match one of those listed, then it is not returned. If an LDAP entry has no attributes that match any attributes to be excluded in the Attribute Filtering tab, then it is returned.

The following book can be used as a reference on regular expressions: *Mastering Regular Expressions*, by Friedl and Oram, published by O'Reilly, ISBN: 1565922573.

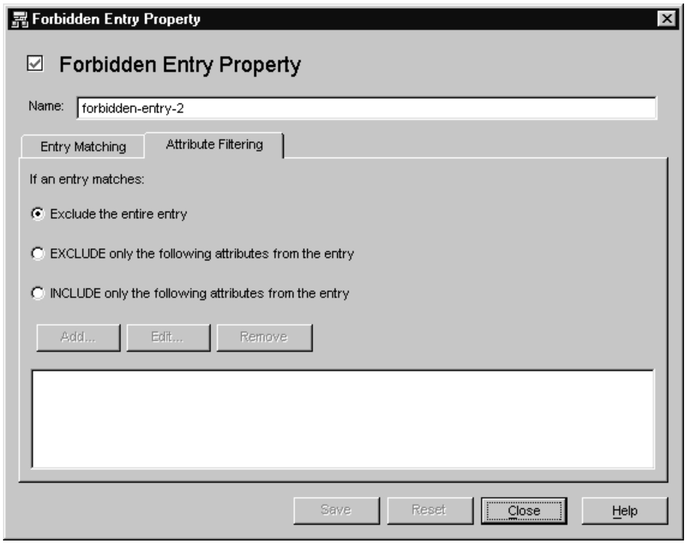
Attribute/Value pair. Displays a dialog used to specify attribute name/value pairs. If an entry has an attribute name/value pair that matches any of the specified attribute name/value pairs, then that entry or some of its content will be hidden.

For example, if you want to restrict all entries that have either "ou=internal" or "secret=yes" as one if its attributes, then you can specify the following: an attribute of "ou" and a value of "internal."

Edit. Displays a dialog for editing the currently-selected entry in the table.

Remove. Removes the currently-selected entry in the table.

6. Select the Attribute Filtering tab, and specify the appropriate values.



Name: forbidden-entry-2

If an entry matches:

● Exclude the entire entry

○ EXCLUDE only the following attributes from the entry

○ INCLUDE only the following attributes from the entry

The tab contains settings that allow certain attributes to be excluded, or specifically included:

Exclude the entire entry. Select this option to indicate that no attribute filtering is to be performed and that the entire entry is to be hidden.

EXCLUDE only the following attributes from the entry. Select this option to indicate that the table contains a list of attribute names that are to be excluded from the entry that has matched any of the above specifications.

INCLUDE only the following attributes from the entry. Select this option to indicate that the table contains a list of attribute names that may be returned as part of the entry that has matched any of the above specifications.

7. Click Save to create the object.

   The Directory Proxy Server configuration is modified, and you're prompted to restart the servers that rely on this configuration. Don't restart the servers yet. You can do this after you've completed all the configuration changes.

8. Repeat Step 3 through Step 7 to create any additional objects.

9. Restart the servers; see "Restarting Directory Proxy Server," on page 50.

LDAP Server Property

In a directory deployment, Directory Proxy Server is located between LDAP clients and LDAP directory servers. It filters requests from LDAP clients before routing them to LDAP directory servers and responses from directory servers before passing them to the clients. Directory Proxy Server also supports automatic load balancing and automatic failover and failback among a set of replicated directory servers.

You use the LDAP Server property to identify the directory servers that Directory Proxy Server should use as the backend servers. When defining this property, you specify all the details required by Directory Proxy Server—for example, the IP address or fully-qualified hostname of the directory server, the port number at which the directory server is listening for client connections, the LDAP versions supported by the server, the version to be used for communication between Directory Proxy Server and this server, and so on—to communicate with a directory server.

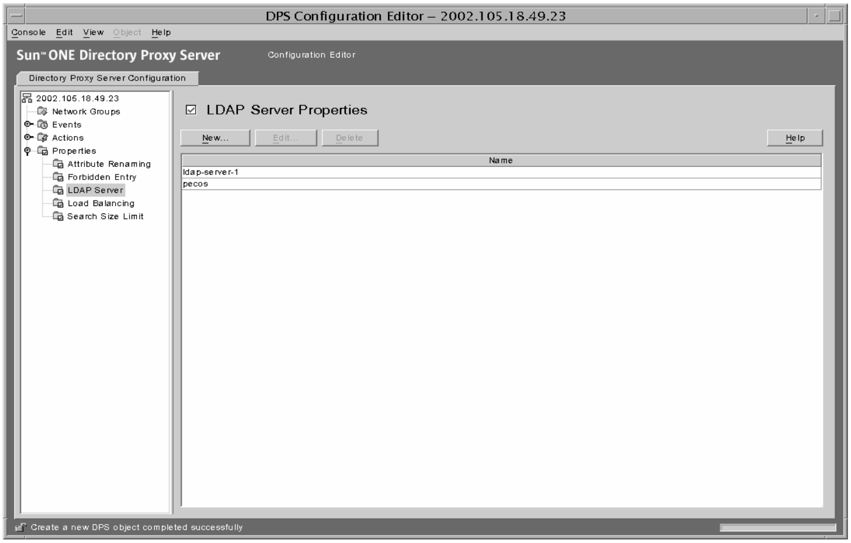
The section that follows explains how to create an object for the LDAP server property from the Directory Proxy Server Configuration Editor Console.

Creating LDAP Server Property Objects

To identify the directory servers that Directory Proxy Server should communicate with:

1. Access the Directory Proxy Server Configuration Editor Console; see "Accessing the Directory Proxy Server Consoles," on page 36.
2. In the navigation tree, expand the Properties node, and then select LDAP Server.

   The right pane shows the list of existing objects for the LDAP Server property.



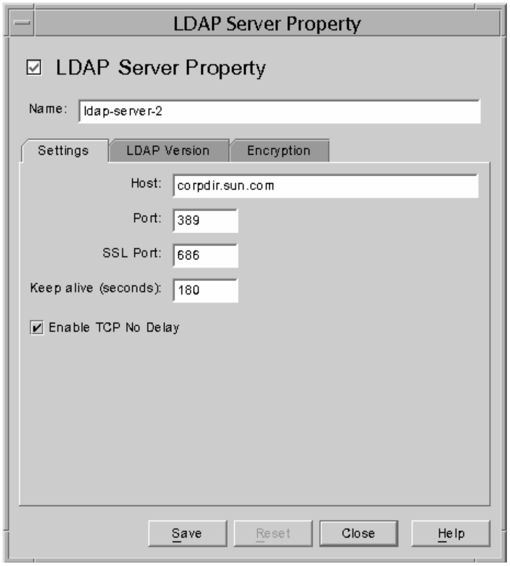
Name
ldap-server-1
pecos

Create a new DPS object completed successfully

3. Click New.

   The LDAP Server Property window appears.

4. In the Name field, type a name for the property object. The name must be a unique alphanumeric string.



Name: ldap-server-2

Host: corpdir.sun.com

Port: 389

SSL Port: 686

Keep alive (seconds): 180

☑ Enable TCP No Delay

5. In the Settings tab specify the basic settings of the LDAP server referred to by this property.

   Host. Enter a value specifying the full domain name or IP address of the host where the backend LDAP server is running. This attribute is mandatory.

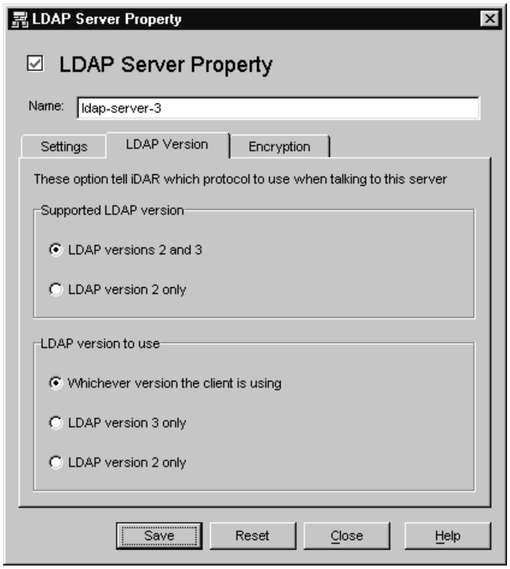
   Port. Enter a number specifying the port on which the backend LDAP server is running. The default port used, if this attribute is absent, is 389.

   SSL port. Enter a number specifying the port on which the backend LDAP server listens for LDAPS (LDAP over SSL) connections. Do not set any value for this attribute if the backend LDAP server does not support LDAPS.

   Keep alive interval. Enter the number of seconds after which Directory Proxy Server will poke an unresponsive server, to determine if the network link to an LDAP directory server is down or if the LDAP directory server has become unresponsive. If the client connected to Directory Proxy Server has pending operations and if Directory Proxy Server has not received any data from the connection's LDAP server for the number of seconds specified here, then Directory Proxy Server will test the availability of the LDAP server by opening another communication channel to it. If Directory Proxy Server is unsuccessful in doing so, it will fail over to another LDAP server, if available. The default value for this attribute is 180 seconds. It is recommended that you increase this value if the LDAP server is not on the same local network as Directory Proxy Server.

   Enable TCP no delay. Disable this option to cause Directory Proxy Server to use the Nagel Algorithm on connections to this server. The option must be disabled only if the network bandwidth between Directory Proxy Server and the server defined by this object entry is very limited. By default, this setting is enabled.

6. Select the LDAP Version tab and specify the appropriate values.



☑ LDAP Server Property

Name: ldap-server-3

These option tell iDAR which protocol to use when talking to this server

Supported LDAP version
- ● LDAP versions 2 and 3
- ○ LDAP version 2 only

LDAP version to use
- ● Whichever version the client is using
- ○ LDAP version 3 only
- ○ LDAP version 2 only

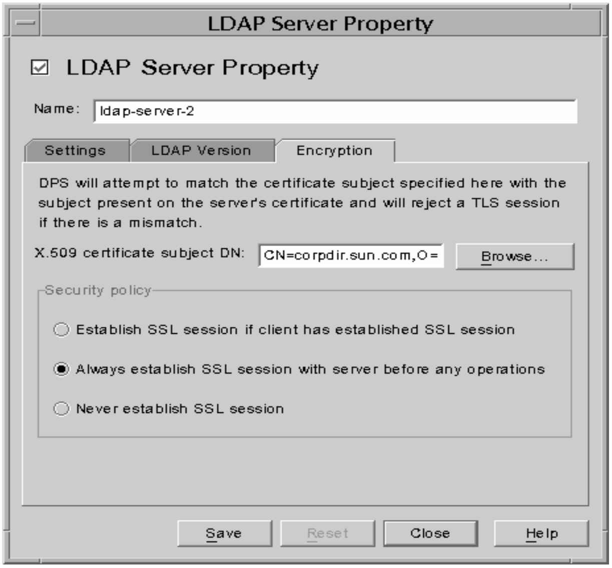
The tab displays settings indicating which versions of LDAP are supported by this server, and which version should be used for communication between Directory Proxy Server and this server.

Supported LDAP version. Select one of the two options present: LDAP versions 2 and 3, or LDAP version 2 only. The default is LDAP versions 2 and 3.

LDAP version to use. Select one of the three options present: "Whichever version the client is using," "LDAP version 3 only," or "LDAP version 2 only." This attribute tells Directory Proxy Server the preferred LDAP protocol version to use when talking to the backend server this entry defines. By default, "Whichever version the client is using" is selected.

This option is useful when you have an LDAPv2 client for which Directory Proxy Server needs to follow referrals. In this case Directory Proxy Server itself needs to connect as LDAPv3 client to the backend server in order for the backend server to send referrals back to it. LDAP version 3 only must be selected if the network group referring to this property allows multiple LDAP version 2 binds.

7. Select the Encryption tab and specify the appropriate values.



☑ LDAP Server Property

Name: ldap-server-2

DPS will attempt to match the certificate subject specified here with the subject present on the server's certificate and will reject a TLS session if there is a mismatch.

X.509 certificate subject DN: CN=corpdir.sun.com,O=

Security policy

○ Establish SSL session if client has established SSL session

● Always establish SSL session with server before any operations

○ Never establish SSL session

The tab displays settings relating to secure communications for the LDAP server referred to by this property.

X.509 certificate subject DN. Specify the LDAP server's certificate subject name. If specified, Directory Proxy Server will attempt to match the certificate subject with the subject present on the LDAP server's certificate and will reject a TLS session if there is a mismatch. (This attribute allows Directory Proxy Server to authenticate the LDAP server to which it is connecting. Directory Proxy Server accepts any name if this attribute is not set.)

Security policy. Select one of the options that define the security policy for connections between Directory Proxy Server and the backend server: "Establish SSL session if client has established SSL session," "Always establish SSL session with server before any operations," "or Never establish SSL session."

8. Click Save to create the object.

   The Directory Proxy Server configuration is modified, and you're prompted to restart the servers that rely on this configuration. Don't restart the servers yet. You can do this after you've completed all the configuration changes.

9. Repeat Step 3 through Step 8 to create any additional objects.
10. Restart the servers; see "Restarting Directory Proxy Server," on page 50.

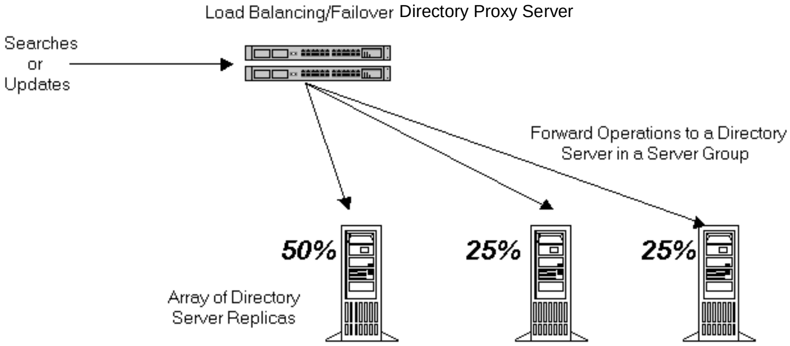
Load Balancing Property

Directory Proxy Server enables high availability of directory deployments by providing both automatic load balancing and automatic failover and failback among a set of replicated LDAP directory servers. In order for Directory Proxy Server to do this, you need to identify the directory servers that Directory Proxy Server should work with and specify how client load is to be distributed among these servers.

You configure Directory Proxy Server for load balancing using the Load Balancing property. This property enables you to identify the back-end directory servers that Directory Proxy Server should communicate with and specify the percentage of total client load each directory server should receive. Once configured, Directory Proxy Server automatically distributes client queries to different directory servers conforming to the load criteria defined in the configuration. If a directory server becomes unavailable, Directory Proxy Server distributes the load percentage of that server proportionally among the available servers based on their load percentage. Directory Proxy Server starts rejecting client queries if all back-end LDAP servers become unavailable.

Figure 7-2 shows client load distributed among a set of three directory server replicas.

Figure 7-2 Load Balancing Across a Set of LDAP Directory Replicas


Load Balancing/Failover Directory Proxy Server
Searches or Updates
Forward Operations to a Directory Server in a Server Group
50%
25%
25%
Array of Directory Server Replicas

Load balancing in Directory Proxy Server is session based. This means that the decision function that chooses a particular directory server to which a client's queries will be directed is applied once per client session, in particular, at the start of the client session. All subsequent client queries in that session are directed to the same directory server that was chosen at the beginning of the session.

The number of back-end directory servers that Directory Proxy Server can load balance depends on several factors, some of which are listed below:

- The size of the host running Directory Proxy Server
- The network bandwidth available
- The query mix that Directory Proxy Server receives
- The length of client sessions
- The Directory Proxy Server configuration

In general, Directory Proxy Server can support fewer directory servers if most sessions are short lived and queries are computationally intensive. Computationally intensive queries are those that require the inspection of the entire message such as, if the attribute renaming (see “Attribute Renaming Property,” on page 100) feature is used.

Directory Proxy Server detects when a directory server becomes unavailable either when a connection attempt is returned with a connection refused error or when it times out. Because both these cases occur at the initial stages of the session, and no operations have yet been processed for that session, Directory Proxy Server fails over to another server provided one is available transparently. In the connect-attempt-timeout case, the client can experience significant delay in getting a response. If a connection between Directory Proxy Server and a back-end server is abruptly lost, Directory Proxy Server returns `LDAP_BUSY` error for all outstanding operations to the affected client. Subsequently, Directory Proxy Server fails over that client session to another directory server.

In order to avoid Directory Proxy Server from becoming the single point of failure for your directory deployment, we recommend you use at least two Directory Proxy Servers with an IP appliance in front of it. This is described in Chapter 2, “Sun ONE Directory Proxy Server Deployment Scenarios.” In case it is not possible to deploy Directory Proxy Server this way, we recommend that you use the -M switch (see “Supported Flags,” on page 194), which will enable Directory Proxy Server to monitor itself.

Directory Proxy Server uses a monitor process to make health checks on its backend servers. This feature is automatically enabled if load balancing is used. Directory Proxy Server makes an anonymous search operation for the Root DSE every 10 seconds for each of its backend directory servers. If one of them becomes unavailable or unresponsive, Directory Proxy Server removes it from the active load balanced server set. When the server becomes available again, it is reintroduced in the set. In order for the monitoring feature to work efficiently, you must have configured the host on which Directory Proxy Server is running according to the recommendations of the `idsktune</code>` utility described in Chapter 2, “Computer System Requirements” of the *Directory Proxy Server Installation Guide*. In case a server has only its secure port enabled, the Directory Proxy Server will try to perform the health checks securely.

The section that follows explains how to create an object for the load balancing property from the Directory Proxy Server Configuration Editor Console.

NOTE Any object you create for the load balancing property must have at least one LDAP Server property and the percentages must add up to 100 percent. Otherwise, Directory Proxy Server will fail to start.

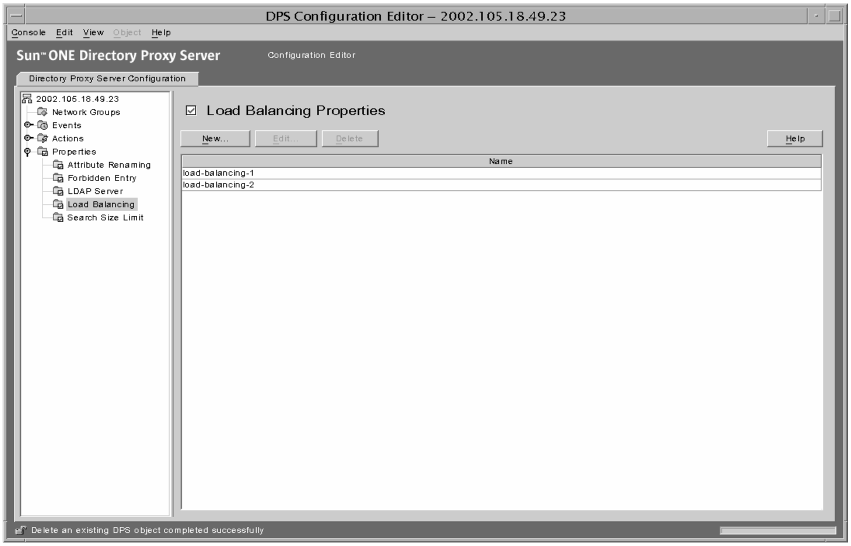
Creating Load Balancing Property Objects

This section explains how to configure Directory Proxy Server for load balancing. Before you create objects for the load balancing property, be sure to identify the LDAP directory servers that Directory Proxy Server should use for balancing the client load. For details, see “LDAP Server Property,” on page 108.

To define how Directory Proxy Server should balance load among a set of directory servers:

1. Access the Directory Proxy Server Configuration Editor Console; see “Accessing the Directory Proxy Server Consoles,” on page 36.
2. In the navigation tree, expand the Properties node, and then select Load Balancing.

   The right pane shows the list of existing objects for the Load Balancing property.

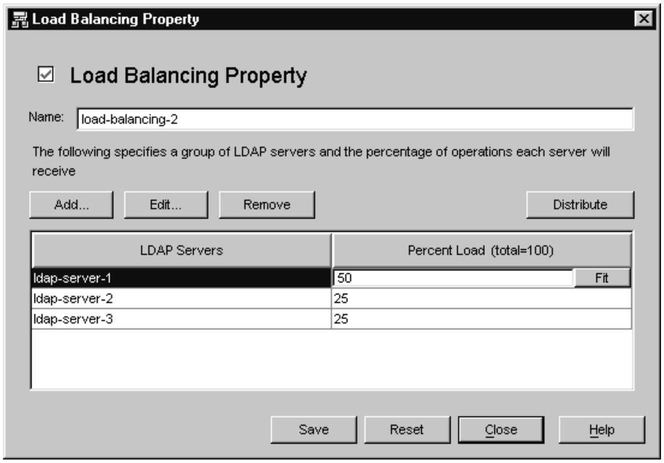


Name
load-balancing-1
load-balancing-2

Delete an existing DPS object completed successfully

3. Click New.

The Load Balancing Property window appears.



Name: load-balancing-2

The following specifies a group of LDAP servers and the percentage of operations each server will receive

LDAP Servers	Percent Load (total=100)
ldap-server-1	50
ldap-server-2	25
ldap-server-3	25

4. In the Name field, type a name for the property object. The name must be a unique alphanumeric string.

5. Use the remaining form elements to get the desired results.

To edit a percentage, click the Percentage Load column next to the row containing an LDAP Server, type a number between 0 and 100, and click the Fit button. This action assigns the percentage to the current row and attempts to make the sum of all the percentages 100. The current percentage sum is displayed in the Percentage Load column heading.

Add. Displays a dialog for adding a reference to an LDAP server property. By default, the first server added is assigned 100 percent of the load with subsequent additions getting 0 percent.

Edit. Displays a dialog for editing the currently-selected item from the table.

Remove. Removes the currently-selected LDAP server from the list of servers across which load balancing will be performed.

Distribute. Distributes the percentage load evenly across all LDAP servers currently referred to in the table.

6. Click Save to create the object.

   The Directory Proxy Server configuration is modified, and you're prompted to restart the servers that rely on this configuration. Don't restart the servers yet. You can do this after you've completed all the configuration changes.

7. Repeat Step 3 through Step 6 to create any additional objects.
8. Restart the servers; see "Restarting Directory Proxy Server," on page 50.

Search Size Limit Property

An LDAP directory typically functions as a central repository for an organization, enabling LDAP clients deployed across the organization to look up information. LDAP clients generally look up information by searching for specific information using search filters. When searching for an entry, clients generally specify attributes associated with that type of entry; for example, when you search for people entries, you can use the `CN` attribute to search for people with a specific common name.

Directory Proxy Server can handle thousands of LDAP client requests and can be configured to apply fine-grained access control policy on LDAP directories, such as controlling who can perform different types of operations on different parts of the Directory Information Tree (DIT). You can also configure Directory Proxy Server to disallow certain kinds of operations, such as the ones performed by web trawlers and robots to collect information contained in a directory.

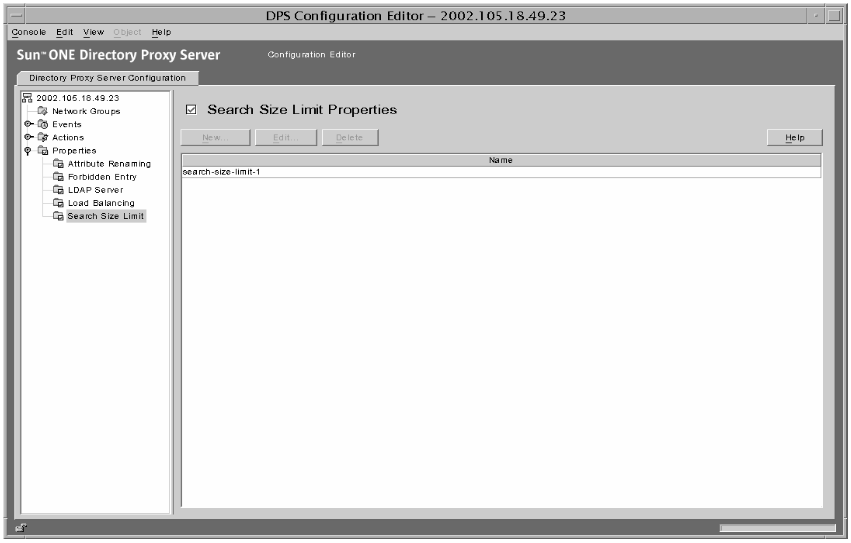
You use the Search Size Limit property to apply size limits based on the search base and search scope. If neither the search base nor search scope specified in this property object entry match a given search, the size limit defaults to the size limit specified in the Network Group object entry; see Chapter 6, “Creating and Managing Groups.”

The section that follows explains how to create an object for the search size limit property from the Directory Proxy Server Configuration Editor Console.

Creating Search Size Limit Property Objects

To define how Directory Proxy Server should limit search sizes:

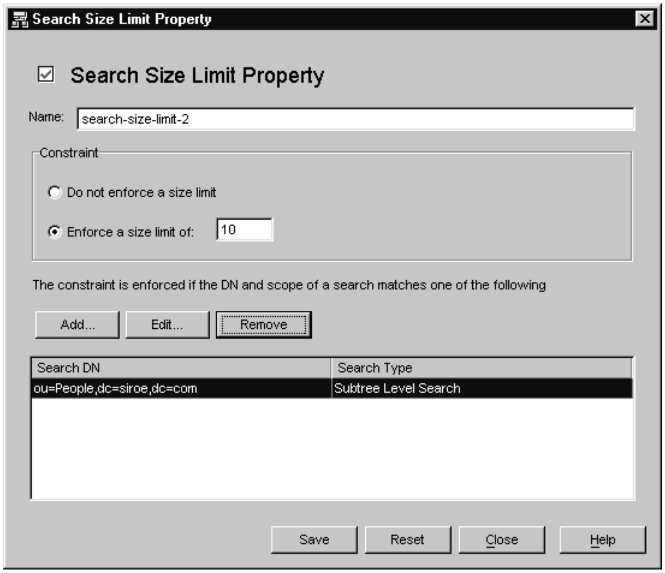
1. Access the Directory Proxy Server Configuration Editor Console; see “Accessing the Directory Proxy Server Consoles,” on page 36.
2. In the navigation tree, expand the Properties node, and then select Search Size Limit.



Name
search-size-limit-1

3. Click New.

   The Search Size Limit Properties window appears.



☑ Search Size Limit Property

Name: search-size-limit-2

Constraint

○ Do not enforce a size limit

● Enforce a size limit of: 10

The constraint is enforced if the DN and scope of a search matches one of the following

Search DN	Search Type
ou=People,dc=siroe,dc=com	Subtree Level Search

4. In the Name field, type a name for the property object. The name must be a unique alphanumeric string.

5. Use the remaining form elements to get the desired results:

   Constraint. Specifies whether or not to enforce a size limit constraint.

   Do not enforce a size limit. Select this option to specify that no size limit will be enforced.

   Enforce a size limit of. Select this option and enter an integer value, specifying the size limit to enforce.

   Add. Displays a menu for adding a size limit condition. Conditions must be one of two types: one level search and subtree level search.

   One level search. Displays a dialog for entering a DN and adding it to the condition table. If the DN of the search base of a one level search matches one of the distinguished names specified for one level searches from the condition table, the size limit specified is enforced as the size limit of that search.

   Subtree level search. Displays a dialog for entering a DN. If the DN of the search base of a subtree search matches one of the distinguished names specified for subtree level searches from the condition table, the size limit specified is enforced as the size limit of that search.

   Edit. Displays a dialog for editing the currently-selected entry in the table.

Remove. Removes the currently-selected entry in the table.

6. Click Save to create the object.

   The Directory Proxy Server configuration is modified, and you're prompted to restart the servers that rely on this configuration. Don't restart the servers yet. You can do this after you've completed all the configuration changes.

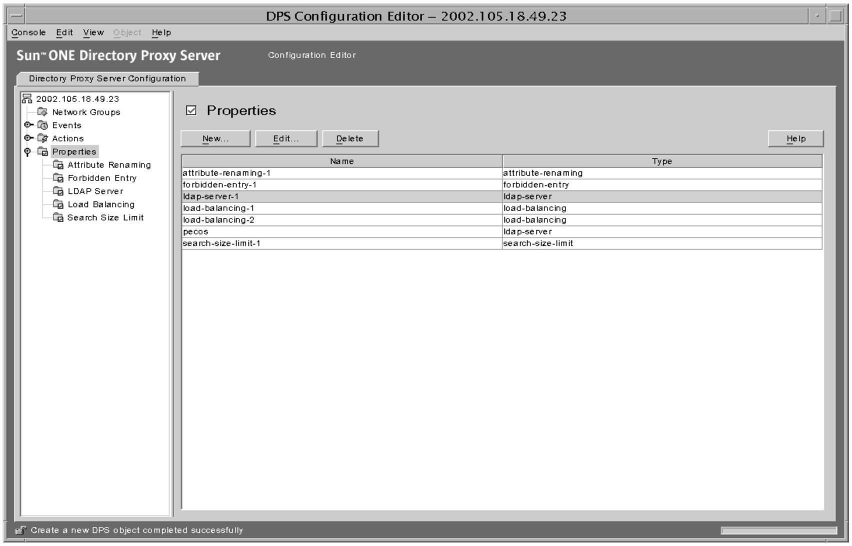
7. Repeat Step 3 through Step 6 to create any additional objects.
8. Restart the servers; see "Restarting Directory Proxy Server," on page 50.

Modifying Property Objects

To modify a property object:

1. Access the Directory Proxy Server Configuration Editor Console; see "Accessing the Directory Proxy Server Consoles," on page 36.
2. In the navigation tree, select the Properties node.

   The right pane shows the list of existing property objects. To view objects pertaining to a specific property, expand the Properties node, and then select the property of your interest.



Name	Type
attribute-renaming-1	attribute-renaming
forbidden-entry-1	forbidden-entry
ldap-server-1	ldap-server
load-balancing-1	load-balancing
load-balancing-2	load-balancing
pecos	ldap-server
search-size-limit-1	search-size-limit

Create a new DPS object completed successfully

3. In the list, select the object you want to modify and click Edit.

4. Make the required modifications.
5. Click Save to save your changes.

   The Directory Proxy Server configuration is modified, and you're prompted to restart the servers that rely on this configuration. Don't restart the servers yet. You can do this after you've completed all the configuration changes.

6. Repeat Step 3 through Step 5 to modify any additional objects.
7. Restart the servers; see "Restarting Directory Proxy Server," on page 50.

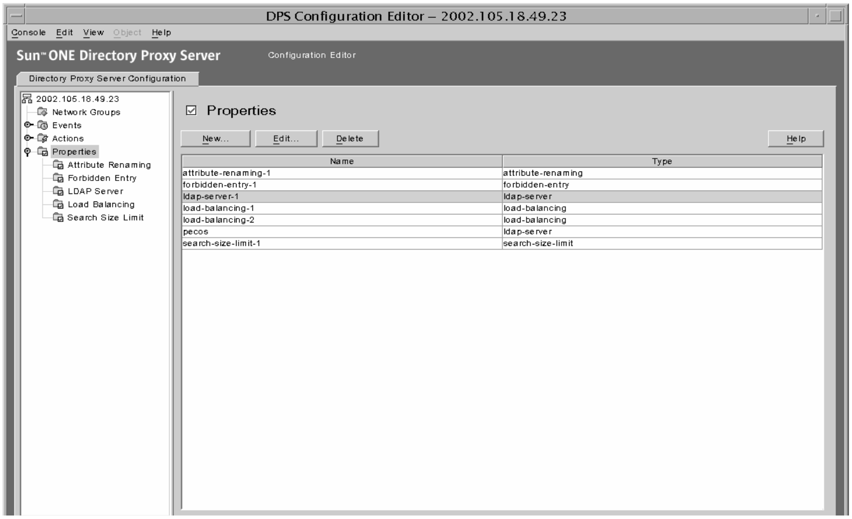
Deleting Property Objects

You can delete any unwanted property objects from the Directory Proxy Server configuration. Before deleting an object, make sure that it's not used in any other configuration entries.

To delete a property object:

1. Access the Directory Proxy Server Configuration Editor Console; see "Accessing the Directory Proxy Server Consoles," on page 36.
2. In the navigation tree, select the Properties node.

   The right pane shows the list of existing property objects. To view objects pertaining to a specific property, expand the Properties node, and then select the property of your interest.



Name	Type
attribute-renaming-1	attribute-renaming
forbidden-entry-1	forbidden-entry
ldap-server-1	ldap-server
load-balancing-1	load-balancing
load-balancing-2	load-balancing
pecos	ldap-server
search-size-limit-1	search-size-limit

3. In the list, select the object you want to delete and click Delete.
4. Confirm your action.

   The Directory Proxy Server configuration is modified, and you're prompted to restart the servers that rely on this configuration. Don't restart the servers yet. You can do this after you've completed all the configuration changes.
5. Repeat Step 3 and Step 4 to delete any additional objects.
6. Restart the servers; see "Restarting Directory Proxy Server," on page 50.

Chapter 8

Creating and Managing Event Objects

Sun ONE Directory Proxy Server supports event-driven actions; that is, you can configure Directory Proxy Server to execute specified actions when specific events occur. This chapter explains how to create and manage event objects using the Directory Proxy Server Configuration Editor Console.

The chapter has the following sections:

Overview of Events

An *event* is a certain Directory Proxy Server state at a certain point while it's running. You use event objects to specify conditions that Directory Proxy Server should evaluate at predetermined states. As a part of defining an event object, you also specify the action Directory Proxy Server should take if the conditions are satisfied. For details about actions, see Chapter 9, "Creating and Managing Action Objects."

Currently, Directory Proxy Server can recognize or keep track of two types of events:

- OnBindSuccess event—This event is evaluated when a client successfully completes a bind operation.

- OnSSLEstablished event—This event is evaluated when a client successfully establishes an SSL session. This event does not have any associated conditions and always executes its list of actions.

You can define event objects based on these two events only. For example, you can define an event object for detecting when a client completes a successful bind. A part of this definition could be to take certain action when the event occurs, for example, to change the access group of that client. For details about groups, see Chapter 6, “Creating and Managing Groups.”

Creating Event Objects

This section explains how to create event objects that are based on OnBindSuccess and OnSSLEstablished events. For details about these events, see “Overview of Events,” on page 123.

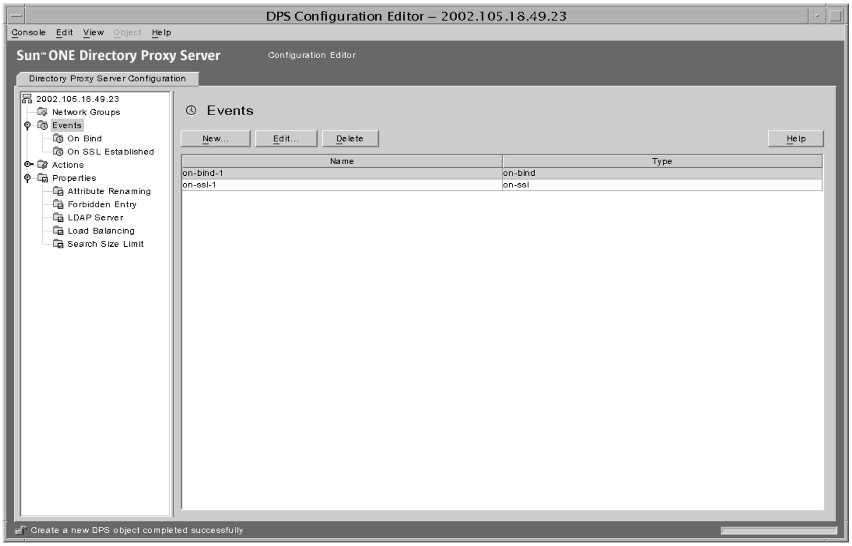
- Creating OnBindSuccess Event Objects
- Creating OnSSLEstablished Event Objects

Creating OnBindSuccess Event Objects

To create an event object based on the OnBindSuccess event:

1. Access the Directory Proxy Server Configuration Editor Console; see “Accessing the Directory Proxy Server Consoles,” on page 36.
2. In the navigation tree, expand the Events node, and then select On Bind.

   The right pane shows the list of existing event objects that are based on the OnBindSuccess event.

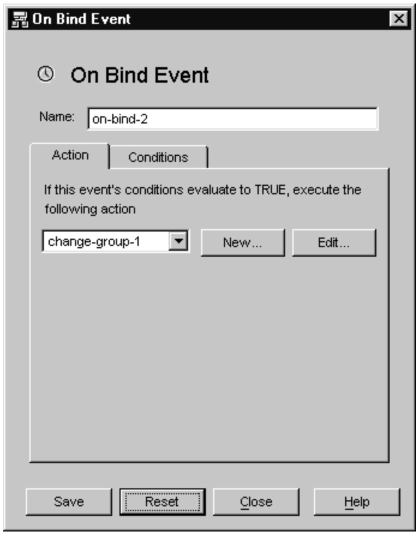


Name	Type
on-bind-1	on-bind
on-ssl-1	on-ssl

Create a new DPS object completed successfully

3. Click New.

   The On Bind Event window appears.



Name: on-bind-2

If this event's conditions evaluate to TRUE, execute the following action

change-group-1

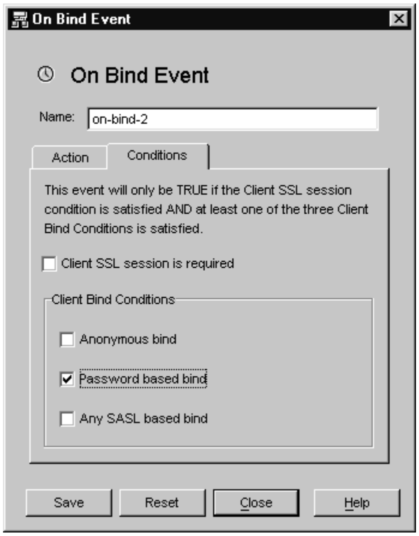
4. In the Name field, type a name for the event object. The name must be a unique alphanumeric string.

5. In the Action tab, select the action to be performed when the event occurs (that is, when the event evaluates to true).

New. You can also define a new action object by clicking the New button.

Edit. Click the Edit button to modify the parameters pertaining to the currently-selected action object.

6. Select the Conditions tab and specify the conditions.



Name: on-bind-2

This event will only be TRUE if the Client SSL session condition is satisfied AND at least one of the three Client Bind Conditions is satisfied.

☐ Client SSL session is required

Client Bind Conditions

☐ Anonymous bind

☑ Password based bind

☐ Any SASL based bind

The event will evaluate to TRUE only when the specified conditions are met—that is, the criteria specified in this tab must evaluate to TRUE in order for the action specified in the Action tab to be executed. The conditions will only be TRUE if the Client SSL session condition is satisfied and at least one of the three client bind conditions is satisfied.

Client SSL session is required. Select this option to indicate that the condition will evaluate to TRUE only if the client has established an SSL session with Directory Proxy Server. The default is FALSE.

Client bind conditions. Conditions are one of the following: “Anonymous bind,” “Password based bind,” and “Any SASL based bind.”

Anonymous bind. Select this option to indicate that the condition will evaluate to TRUE only if the Client SSL session requirement is met and the client has just completed a successful anonymous bind.

Password based bind. Select this option to indicate that the condition will evaluate to TRUE only if the Client SSL session requirement is met and the client has just completed a successful password based bind.

Any SASL based bind. Select this option to indicate that the condition will evaluate to TRUE only if the Client SSL session requirement is met and the client has just completed a successful bind using any SASL mechanism.

7. Click Save to create the event object.

   The Directory Proxy Server configuration is modified, and you're prompted to restart the servers that rely on this configuration. Don't restart the servers yet. You can do this after you've completed all the configuration changes.

8. Repeat Step 3 through Step 7 to create any additional objects.

9. Restart the servers; see "Restarting Directory Proxy Server," on page 50.

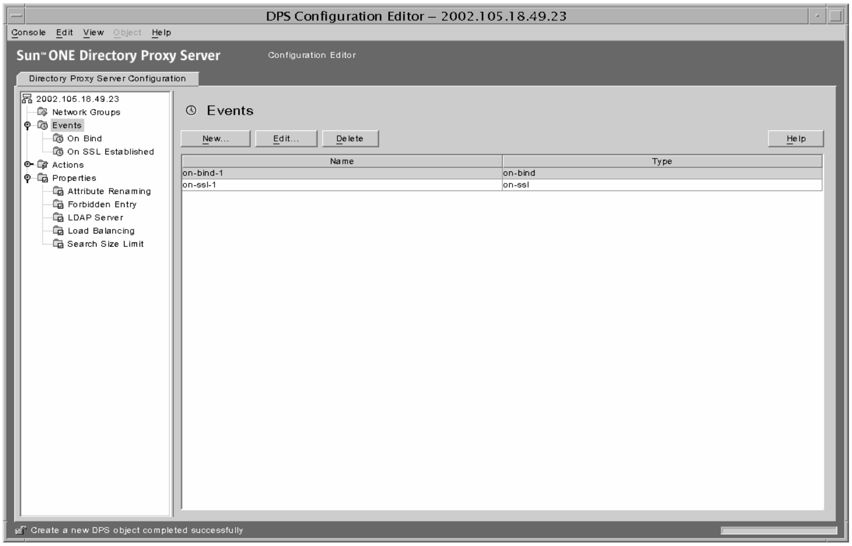
Creating OnSSLEstablished Event Objects

To create an event object based on the OnSSLEstablished event:

1. Access the Directory Proxy Server Configuration Editor Console; see "Accessing the Directory Proxy Server Consoles," on page 36.

2. In the navigation tree, expand the Events node, and then select On SSL Established.

   The right pane shows the list of existing event objects that are based on the OnSSLEstablished event.

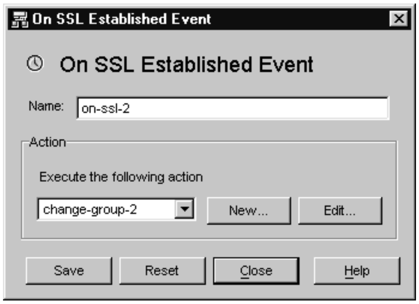


Name	Type
on-bind-1	on-bind
on-ssl-1	on-ssl

Create a new DPS object completed successfully

3. Click New.

   The On SSL Established Event window appears.



On SSL Established Event

Name: on-ssl-2

Action

Execute the following action

change-group-2

4. In the Name field, type a name for the event object. The name must be a unique alphanumeric string.
5. In the Action section, select the action to be performed when the event occurs (that is, when the event evaluates to TRUE).

   Click the Edit button to modify the parameters pertaining to the currently-selected action. You can also define a new action by clicking the New button.
6. Click Save to create the event object.

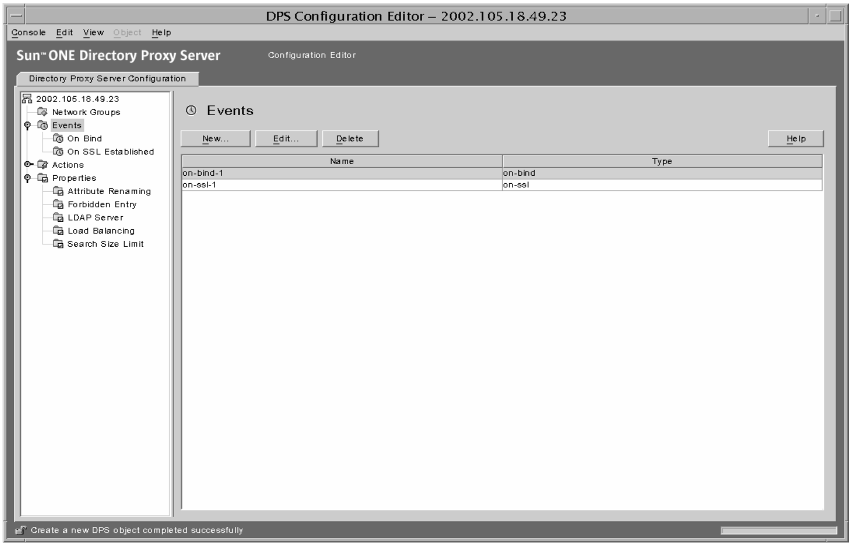
   The Directory Proxy Server configuration is modified, and you're prompted to restart the servers that rely on this configuration. Don't restart the servers yet. You can do this after you've completed all the configuration changes.
7. Repeat Step 3 through Step 6 to create any additional objects.
8. Restart the servers; see "Restarting Directory Proxy Server," on page 50.

Modifying Event Objects

To modify an event object:

1. Access the Directory Proxy Server Configuration Editor Console; see "Accessing the Directory Proxy Server Consoles," on page 36.
2. In the navigation tree, select Events.

   The right pane shows the list of existing event objects. To view objects pertaining to an event type, expand the Events node, and then select the event type of your interest.



Name	Type
on-bind-1	on-bind
on-ssl-1	on-ssl

Create a new DPS object completed successfully

3. In the list, select the event object you want to modify and click Edit.

4. Make the required modifications.

5. Click Save to save your changes.

   The Directory Proxy Server configuration is modified, and you're prompted to restart the servers that rely on this configuration. Don't restart the servers yet. You can do this after you've completed all the configuration changes.

6. Repeat Step 3 through Step 5 to modify any additional objects.

7. Restart the servers; see "Restarting Directory Proxy Server," on page 50.

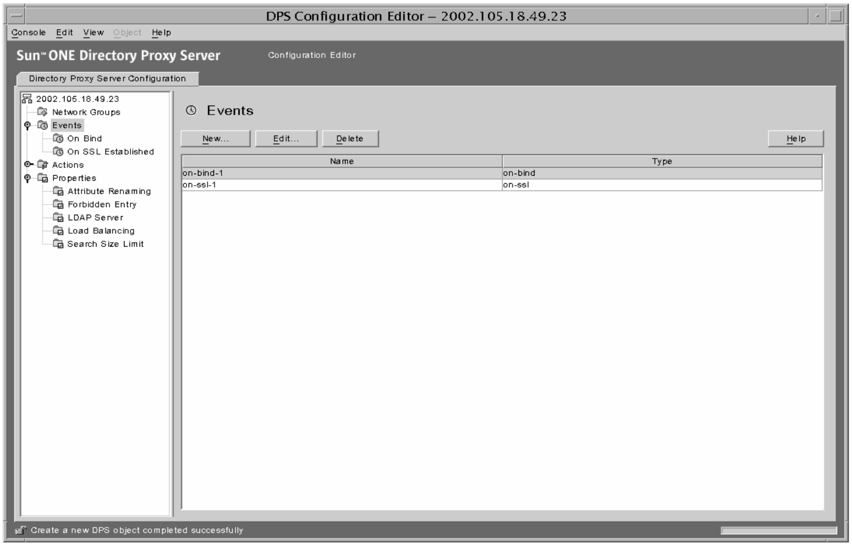
Deleting Event Objects

You can delete any unwanted event objects from the Directory Proxy Server configuration. To delete an event object:

1. Access the Directory Proxy Server Configuration Editor Console; see "Accessing the Directory Proxy Server Consoles," on page 36.

2. In the navigation tree, select the Events node.

   The right pane shows the list of existing event objects. To view objects pertaining to an event type, expand the Events node, and then select the event type of your interest.



Name	Type
on-bind-1	on-bind
on-ssl-1	on-ssl

Create a new DPS object completed successfully

3. In the list, select the event object you want to delete and click Delete.

4. When prompted, confirm your action.

   The name of the event object you deleted is now removed from the list. The Directory Proxy Server configuration is modified, and you're prompted to restart the servers that rely on this configuration. Don't restart the servers yet. You can do this after you've completed all the configuration changes.

5. Repeat Step 3 and Step 4 to delete any additional objects.

6. Restart the servers; see "Restarting Directory Proxy Server," on page 50.

Chapter 9

Creating and Managing Action Objects

Sun ONE Directory Proxy Server supports event-driven actions, that is, you can configure Directory Proxy Server to execute specified actions when specific events occur. This chapter explains how to create and manage action objects using the Directory Proxy Server Configuration Editor Console.

The chapter has the following sections:

Overview of Actions

An *action* refers to a task that Directory Proxy Server can execute. You use an action object to specify the action Directory Proxy Server should take if the rules or conditions defined by an event object evaluates to `TRUE`. Event objects are used to specify conditions which are evaluated by Directory Proxy Server at predetermined states. For details about events, see Chapter 8, “Creating and Managing Event Objects.”

Currently, Directory Proxy Server can execute one action called `ChangeGroup`. This action enables you to configure Directory Proxy Server to change a client from one access group to another based on the evaluation of a rule. For details about groups, see Chapter 6, “Creating and Managing Groups.”

The change-group feature is especially useful if your LDAP directory contains information about mobile users, for example, users who connect to the directory from different IP addresses or physical locations. You can setup Directory Proxy Server in such a way that a mobile user would connect to Directory Proxy Server with a dynamic IP address and drop into a “default” access group. The “default” access group would have a rule based on the `OnBindSuccess` event, that evaluates to TRUE only if the bind credentials provided by the mobile user are authenticated. This rule would also have the `ChangeGroup` action configured to change the mobile user’s access group from “default” to the access group the mobile user is usually assigned to when accessing Directory Proxy Server with a static IP address.

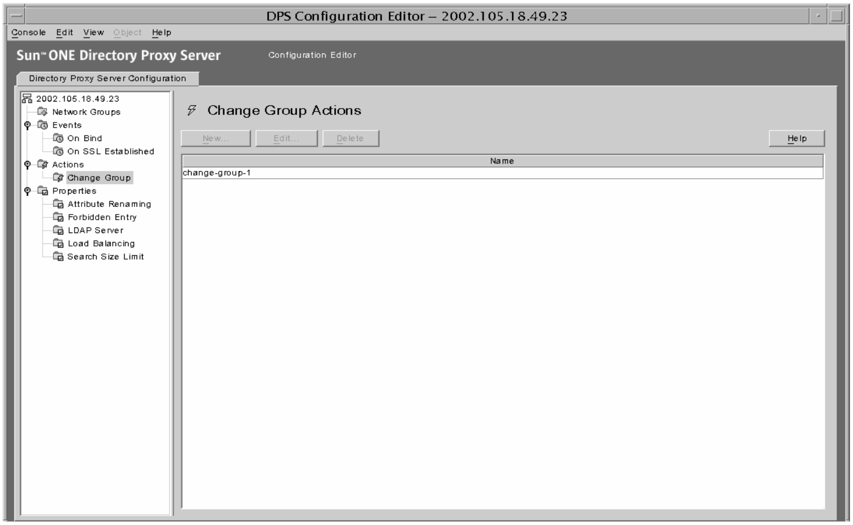
Creating Action Objects

You can create objects for actions that need to be executed when certain events occur. The instructions below explain how to create an action object for changing groups.

To create an action object for a client to change from one group to another:

1. Access the Directory Proxy Server Configuration Editor Console; see “Accessing the Directory Proxy Server Consoles,” on page 36.
2. In the navigation tree, expand the Actions node, and then, select Change Group.

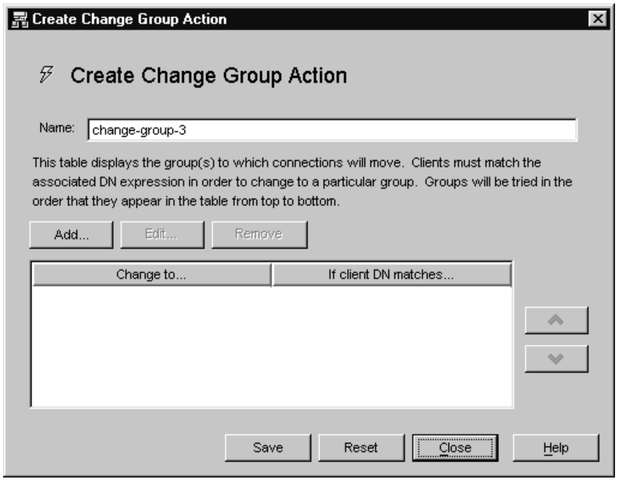
   The right pane shows the list of existing action objects.



Name
change-group-1

3. Click New.

The Create Change Group Action window appears.



Create Change Group Action

Name: change-group-3

This table displays the group(s) to which connections will move. Clients must match the associated DN expression in order to change to a particular group. Groups will be tried in the order that they appear in the table from top to bottom.

4. In the Name field, type a name for the object. The name must be a unique alphanumeric string.

5. In the Action tab, select the action to be performed when the event occurs (that is, when the event evaluates to TRUE).

Change to... Displays a list of groups to which a client can change. For a change to occur, the client must match a DN expression associated with each group. To edit the DN expression associated with a particular group or "no change" entry, click the "If client DN matches" column in the table. The list is evaluated from top to bottom until a DN expression is matched. Therefore, it is important that the most general DN expression is at the bottom of the list so that all expressions will be evaluated.

Regular expressions must be normalized, that is, there should be no spaces in between RDN components and the equal to (=) sign, and all attribute names and values must be capitalized.

You can use the following book as a reference on regular expressions: *Mastering Regular Expressions*, by Friedl and Oram, published by O'Reilly, ISBN: 1565922573.

Add. Displays a menu for adding a group to which a client connection could potentially change. Group change entries can be of the following types: "Group change entry," or "No change entry."

Group change entry. Displays a dialog for selecting a network group to which a client will change depending on whether or not the associated DN expression evaluates to TRUE.

No change entry. Adds a row to the table indicating that NO change should occur if the associated DN expression evaluates to TRUE. This is useful in providing a “short circuit” of the evaluation of the change group list.

Edit. Displays a dialog for editing the currently-selected entry in the table.

Remove. Removes the currently-selected entry in the table.

6. Click Save to create the action object.

   The Directory Proxy Server configuration is modified, and you’re prompted to restart the servers that rely on this configuration. Don’t restart the servers yet. You can do this after you’ve completed all the configuration changes.

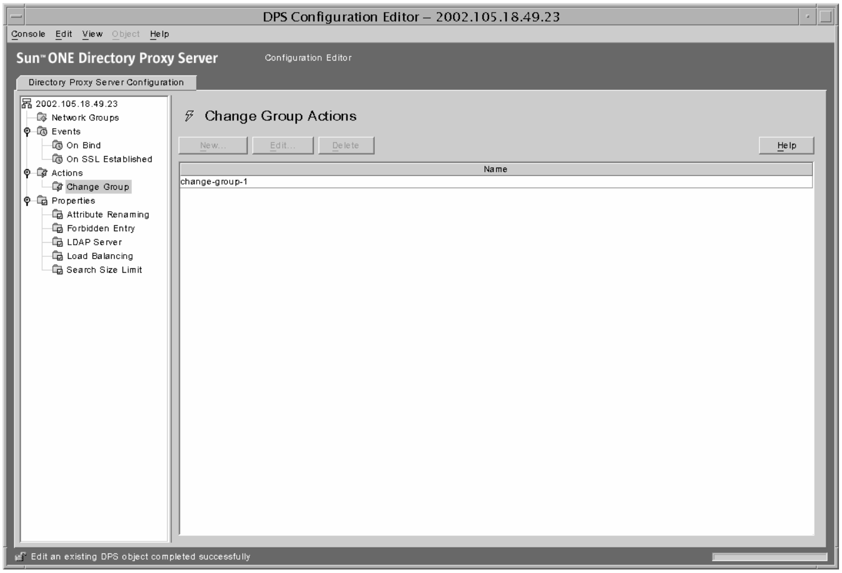
7. Repeat Step 3 through Step 6 to create any additional objects.
8. Restart the servers; see “Restarting Directory Proxy Server,” on page 50.

Modifying Action Objects

To modify an action object:

1. Access the Directory Proxy Server Configuration Editor Console; see “Accessing the Directory Proxy Server Consoles,” on page 36.
2. In the navigation tree, select Actions.

   The right pane shows the list of existing action objects.



Name
change-group-1

Edit an existing DPS object completed successfully

3. In the list, select the action object you want to modify and click Edit.
4. Make the required modifications.
5. Click Save to save your changes.

   The Directory Proxy Server configuration is modified, and you are prompted to restart the servers that rely on this configuration. Don't restart the servers yet. You can do this after you've completed all the configuration changes.

6. Repeat Step 3 through Step 5 to modify any additional objects.
7. Restart the servers; see "Restarting Directory Proxy Server," on page 50.

Deleting Action Objects

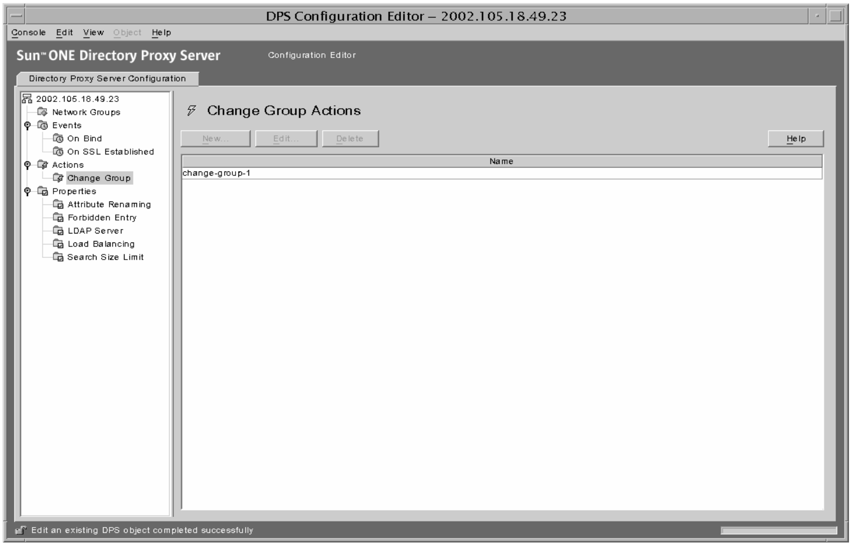
You can delete any unwanted action objects from the Directory Proxy Server configuration. Before deleting an action object, make sure that it's not used in the configuration of any event objects.

To delete an action object:

1. Access the Directory Proxy Server Configuration Editor Console; see "Accessing the Directory Proxy Server Consoles," on page 36.

2. In the navigation tree, select Actions.

   The right pane shows the list of existing action objects.



Name
change-group-1

Edit an existing DPS object completed successfully

3. In the list, select the action you want to delete and click Delete.

4. Confirm your action.

   The name of the object you deleted is now removed from the list. The Directory Proxy Server configuration is modified, and you are prompted to restart the servers that rely on this configuration. Don’t restart the servers yet. You can do this after you’ve completed all the configuration changes.

5. Repeat Step 3 and Step 4 to delete any additional objects.

6. Restart the servers; see “Restarting Directory Proxy Server,” on page 50.

Chapter 10

Configuring and Monitoring Logs

This chapter explains how to configure Sun ONE Directory Proxy Server to log entries or messages and then monitor its activities with the help of the logged entries using the Directory Proxy Server Server Console.

The chapter has the following sections:

- Overview of Logging (page 137)
- Configuring Logs (page 141)
- Monitoring Logs From Directory Proxy Server Server Console (page 146)

Overview of Logging

Directory Proxy Server can maintain two types of logs:

- System Log
- Audit Log

The sections that follow explain both in detail.

System Log

Directory Proxy Server can maintain extensive log records of various events and system errors so that you can monitor and debug the system. All log records can be maintained in text files and can be stored in your local file system for quick and easy retrieval. By default, Directory Proxy Server writes log entries to this file:

`<server-root>/dps-<hostname>/logs/fwd.log`

Each message in the log file is time stamped. It also has the process number and a message number that is internal to Directory Proxy Server.

For identification and filtering purposes, events logged by Directory Proxy Server are classified into various categories. These are listed in Table 10-1. Each category represents messages that are of the same or a similar nature or that belong to a specific functional area. Based on the configuration, a log file can record entries that fall under one or more of these categories.

In the Directory Proxy Server configuration, each message category corresponds to a specific log level. Log levels indicate the level of logging to be performed by the server—that is, how detailed the logging should be.

- A higher priority level means less detail because only events of high priority are logged.
- A lower priority level means greater detail because more kinds of events are recorded in the log file.

Table 10-1 lists the message categories in the descending order of priority—`Critical` has the highest priority level and `Detailed trace` has the lowest priority level.

Table 10-1 Log Levels

Log Level or Severity	Description
Mandatory	Mandatory messages are those that are always written to the log. These messages indicate the configuration that Directory Proxy Server read, Directory Proxy Server version number on startup, etc. Messages pertaining to this level are not configurable.
Critical	These messages indicate Directory Proxy Server encountered some problems that need immediate attention. For example, *Directory Proxy Server process 1234 has exited, attempting restart in 10 seconds*.
Exception	These messages indicate unexpected error conditions, such as an incorrectly formatted LDAP message received from client/server by Directory Proxy Server. For example, *Could not decode search request*.
Warning	These messages specify error conditions that Directory Proxy Server can ignore but must be investigated by the administrator. For example, *Local host name lookup failed. System default group may not function correctly*.

Table 10-1 Log Levels *(Continued)*

Log Level or Severity	Description
Notice	These messages are informational. For example, *Received NULL continuation reference from server. Discarding...*
Trace	These are debug messages. For example, *Result received from server lderr =32, matched=o=sun.com, errtxt=no such object*. Trace messages include protocol dumps. Use of Trace level can generate very large log files very quickly.
Detailed trace	These messages provide more detailed debugging information such as Requested Anonymous bind for recycling connection. These messages usually have meaning for the Directory Proxy Server engineering/support team.

Directory Proxy Server enables you to specify the amount of logging—you can use log levels to filter log entries based on the severity of an event. By default, the level is set to `Warning`.

NOTE The log level is additive; that is, if you choose `Warning` as the log level, `Warning`, `Exception`, and `Critical` level messages will be logged. Log data can be voluminous, especially at lower (more verbose) logging levels. Make sure that the host machine has sufficient disk space for all the log files.

Optionally, on platforms other than Windows NT, you can configure Directory Proxy Server to send log messages to the `syslog` daemon instead of a file; you cannot send the log messages to both a file and to the `syslog` daemon at the same time. If you opt for this configuration, make sure that your `syslogd` is properly configured. For example, to have all the messages written to a particular file `/var/adm/messages` the following line must be added to the file `/etc/syslog.conf`:

```
daemon.crit;daemon.warning;daemon.info;daemon.debug
/var/adm/messages
```

Note that Directory Proxy Server uses the `daemon` facility, with the `crit`, `warning`, `info`, and `debug` priorities or log levels. Table 10-1 shows the mapping between syslog events and Directory Proxy Server events.

Table 10-2 Mapping of Log Levels

Directory Proxy Server Event	syslog Event
Mandatory	info
Critical	crit
Exception	err
Warning	warning
Notice	info
Trace	info
Detailed trace	info

To rotate Directory Proxy Server logs and control other logging features use the following object class:

`ids-proxy-sch-LogProperty`

Refer "dpsconfig2ldif," on page 187 for detailed information about this object class and its usage.

Audit Log

In addition to logging system and error messages, Directory Proxy Server can also maintain audit trails for all events and connection statistics—for example, the DN of a client that just completed a bind / unbind with an LDAP directory can be logged.

By default, Directory Proxy Server is not configured to log audit messages. You can enable this feature at any time. You can also specify whether to log audit messages to the same file to which system log entries are written or to an alternate file. Unless configured to write to a different file, the audit messages (along with the other log messages) are logged to the same file to which system log entries are written; for details, see "System Log," on page 137.

NOTE Audit records enable you to detect any unauthorized access or activity. It's recommended that you enable this feature. Also, as a security measure, you should periodically examine the Directory Proxy Server audit log for any unusual activity.

Configuring Logs

To configure Directory Proxy Server to log entries, follow these steps:

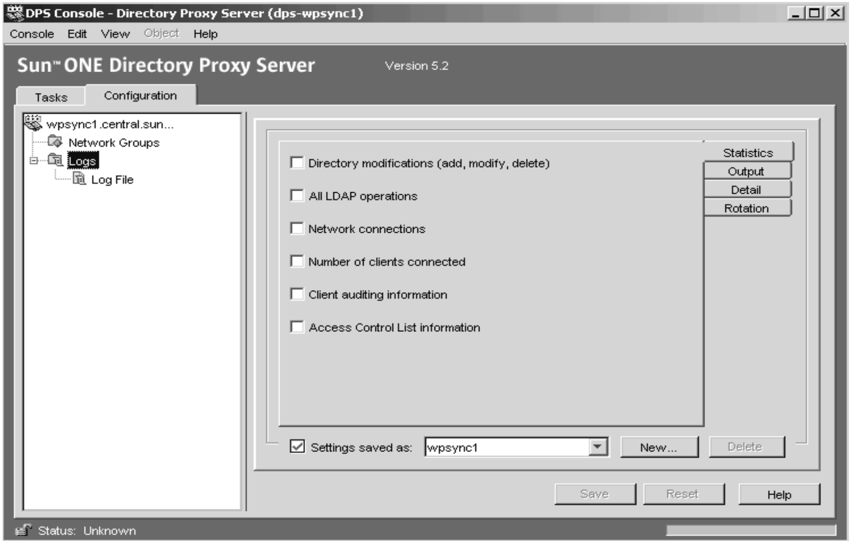
- Step 1. Define The Log Settings
- Step 2. Specify the Logging Property to Use

Step 1. Define The Log Settings

This step is required only if you want to create or define an object for the Log Property. If you have already created objects for the log property and want to use one of them, then skip to the next step.

1. Access the Directory Proxy Server Console; see “Accessing the Directory Proxy Server Consoles,” on page 36.
2. Select the Configuration tab, and then, in the navigation tree, expand Logs.

   The right pane shows the list of existing objects for the logging property on the right.



☐ Directory modifications (add, modify, delete)
☐ All LDAP operations
☐ Network connections
☐ Number of clients connected
☐ Client auditing information
☐ Access Control List information

☑ Settings saved as: wpsync1

3. Click New to define a new object.

   The Log Property window Statistics tab becomes active.

4. In the Name field, type a name for the object. The name must be a unique alphanumeric string.

5. In the Statistics tab, specify the kind of information to be logged.

   Check the boxes referring to the type of logging messages desired. By default none of the options are selected. Log messages are classified into the following groups: directory modifications, all LDAP operations, network connections, number of clients connected, and client auditing information.

   Directory modifications. Statistics about operations that write to the directory, like add, modify, and delete will be logged.

   All LDAP operations. Statistics about all LDAP operations will be logged.

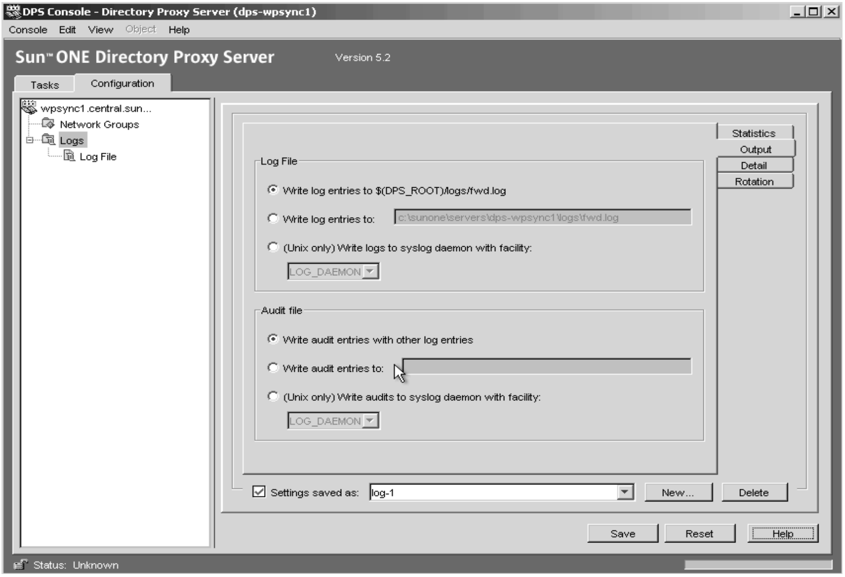
   Network connections. Statistics about network connections will be logged.

   Number of clients connected. General statistics such as how many clients are connected will be logged.

   Client auditing information. Audit information such as the DN of client that just completed a bind / unbind will be logged.

   Access Control List Information. This contains a list of users that have access to log information.

6. Select the Output tab and specify where log entries should be sent and whether to log audit traces.



Log File

● Write log entries to $(DPS_ROOT)/logs/fwd.log

○ Write log entries to: c:\sunone\servers\dps-wpsync1\logs\fwd.log

○ (Unix only) Write logs to syslog daemon with facility: LOG_DAEMON

Audit file

● Write audit entries with other log entries

○ Write audit entries to:

○ (Unix only) Write audits to syslog daemon with facility: LOG_DAEMON

☑ Settings saved as: log-1

Log file. Displays options governing where Directory Proxy Server will write its log entries.

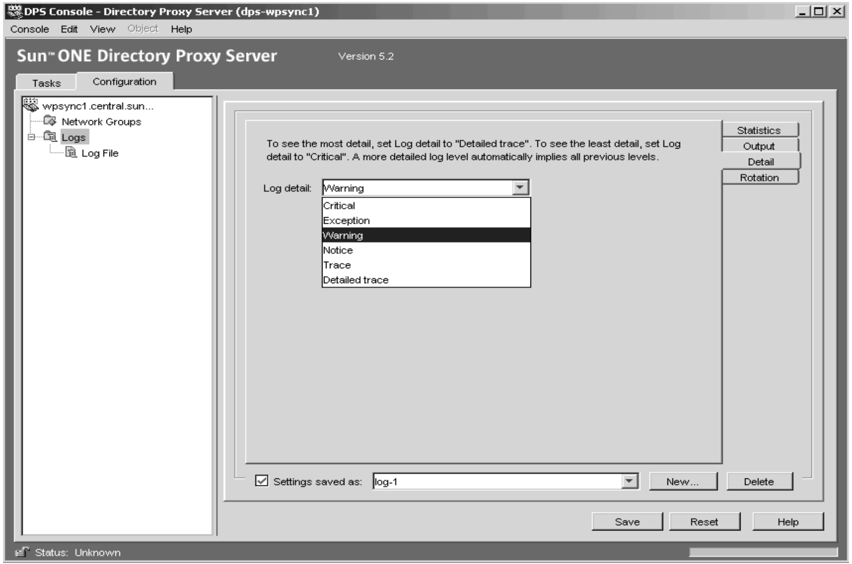
> **Write log entries to $(dps_ROOT)/logs/fwd.log.** This is the default setting in which Directory Proxy Server will write its log entries to the file `$(dps_ROOT)/logs/fwd.log` where `$(dps_ROOT)` is the directory under the server root where Directory Proxy Server is installed, typically `/usr/sunone/servers/dps-<hostname>` or `\Program\Files\sunone\Servers\dps-<hostname>`.
>
> **Write log entries to.** Specify an alternative file to which Directory Proxy Server will direct its log entries. The file separator must follow UNIX conventions regardless of platform.
>
> **Write logs to syslog daemon with facility.** (UNIX only) Choose a syslog facility code that Directory Proxy Server will use to log entries. This setting should be chosen only if this log property is to be used by Directory Proxy Server server installed on a UNIX machine. Specifying this option for Directory Proxy Server installed on a Windows NT system will make it inoperable. It is recommended that if you would like to specify values for this attribute, you should create separate log properties for Windows NT and UNIX.

Audit File. Displays options governing where Directory Proxy Server will write its audit log entries. For this feature to work, audit logging must be enabled by selecting the “Client auditing information” option in the Statistics tab.

> **Write audit entries with other log entries.** This is the default setting in which Directory Proxy Server will write its audit log entries to the same output specified in the log file settings above.
>
> **Write log entries to.** Specify an alternative file to which Directory Proxy Server will direct its audit log entries. The file separator should follow UNIX conventions regardless of platform.
>
> **Write audits to syslog daemon with facility.** (UNIX only) Choose a syslog facility code that Directory Proxy Server will use to log audit entries. This setting should be chosen only if this log property is to be used by Directory Proxy Server servers hosted on a UNIX machine. Specifying this option causes a Windows NT based Directory Proxy Server to become inoperable. It is recommended that if you would like to specify values for this attribute, you should create separate Log Property objects for Windows NT and UNIX.

7. Select the Detail tab and specify the log level—the amount of logging detail desired.

Choose the logging level from the drop-down menu.

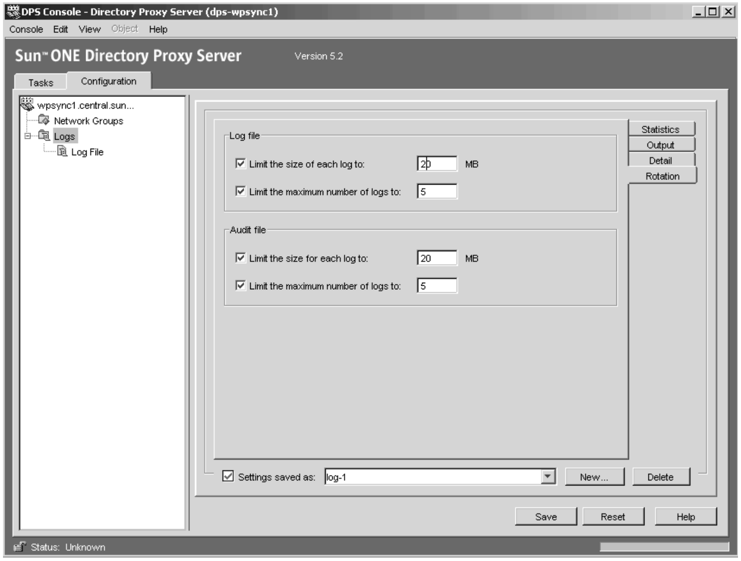


To see the most detail, set Log detail to "Detailed trace". To see the least detail, set Log detail to "Critical". A more detailed log level automatically implies all previous levels.

Log detail: Warning

☑ Settings saved as: log-1

8. Select the Rotation tab to control how logs are sized and rotated.



Log file

☑ Limit the size of each log to: 20 MB

☑ Limit the maximum number of logs to: 5

Audit file

☑ Limit the size for each log to: 20 MB

☑ Limit the maximum number of logs to: 5

☑ Settings saved as: log-1

Log file. Displays options limiting the size and maximum number of Directory Proxy Server log files.

Limit the size of each log to. Enter the maximum size in megabytes for each log file.

Limit the maximum number of logs to. Enter the maximum number of log files to be created and rotated.

Audit file. Displays options limiting the size and maximum number of Directory Proxy Server audit files.

Limit the size of each log to. Enter the maximum size in megabytes for each audit log file.

Limit the maximum number of logs to. Enter the maximum number of audit log files to be created and rotated.

9. Click Save to save your changes.

   The name of the object now appears in the list. The Directory Proxy Server configuration is modified, and you're prompted to restart the server.

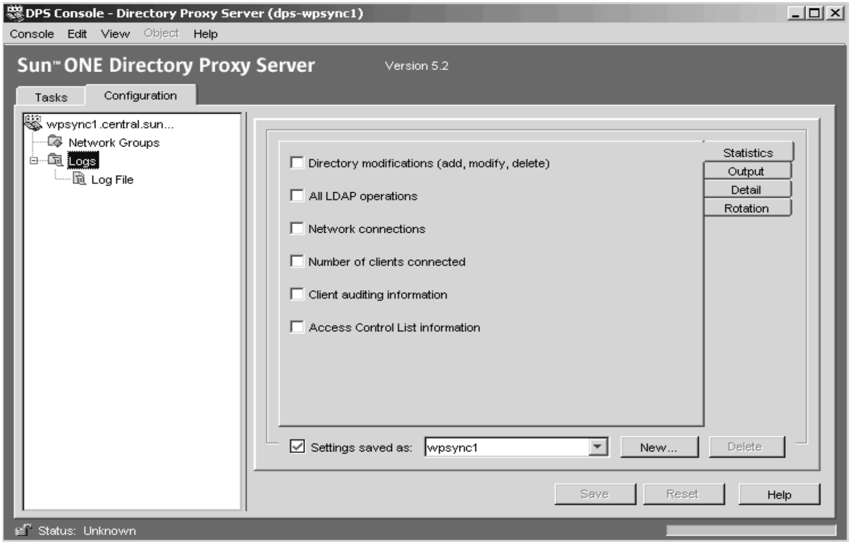
10. Restart the server; see "Restarting Directory Proxy Server," on page 50.

Step 2. Specify the Logging Property to Use

In this step, you select an existing log property to be used for logging messages.

1. Access the Directory Proxy Server Server Console; see "Accessing the Directory Proxy Server Consoles," on page 36.
2. Select the Configuration tab, and then, in the navigation tree, select Logs.

   The right pane shows information regarding the log property specified by the current system property.



☐ Directory modifications (add, modify, delete)

☐ All LDAP operations

☐ Network connections

☐ Number of clients connected

☐ Client auditing information

☐ Access Control List information

☑ Settings saved as: wpsync1

3. In the "Settings saved as" drop-down list, select the property you want to use.
4. Click Save to save your changes.

   Directory Proxy Server is now configured to log messages as defined in the configuration. The Directory Proxy Server configuration is modified, and you are prompted to restart the server.

5. Select the Tasks tab and restart the server; see "Restarting Directory Proxy Server," on page 50.

Monitoring Logs From Directory Proxy Server Server Console

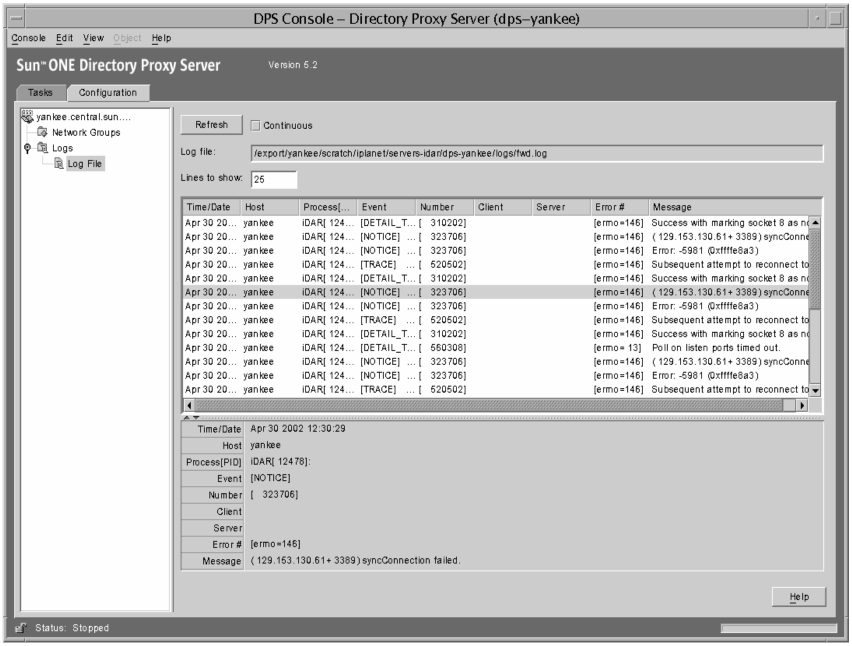
Once you've configured Directory Proxy Server to log messages (see "Configuring Logs," on page 141), you can monitor its activities by viewing the log messages. For example, when you have problems with Directory Proxy Server that require troubleshooting, you may find it helpful to check the error or informational messages that the server has logged. Also, by examining the log files you can monitor many aspects of Directory Proxy Server's operation.

To facilitate this, the Directory Proxy Server Server Console provides a simple mechanism for viewing the contents of log files. The contents of the log file you choose to view are displayed in the form of a table. The table is split; the top pane shows log records in tabular format and the bottom pane shows the currently-selected record in detail. Each log record contains information such as the date and time the message was logged, the severity of the message, and a general description of the log.

Once you open a log file for viewing, you can read its contents partially by specifying the number of records or entries to be displayed. The instructions below explain how to view log records in a file:

1. Access the Directory Proxy Server Server Console; see "Accessing the Directory Proxy Server Consoles," on page 36.
2. Select the Configuration tab, and then, in the navigation tree, expand Logs.
3. Select Log File.

   The right pane shows viewing options for entries logged to a file. You can select any of the log files specified in the current log property; Directory Proxy Server can contain separate files for logging and auditing information, if configured to do so.



☐ Continuous

Log file: /export/yankee/scratch/iplanet/servers-idar/dps-yankee/logs/fwd.log

Lines to show: 25

Time/Date	Host	Process[...	Event	Number	Client	Server	Error #	Message
Apr 30 20...	yankee	iDAR[124...	[DETAIL_T...	[310202]			[errno=146]	Success with marking socket 8 as no
Apr 30 20...	yankee	iDAR[124...	[NOTICE] ...	[323706]			[errno=146]	(129.153.130.61+ 3389) syncConne
Apr 30 20...	yankee	iDAR[124...	[NOTICE] ...	[323706]			[errno=146]	Error: -5981 (0xffffe8a3)
Apr 30 20...	yankee	iDAR[124...	[TRACE] ...	[520502]			[errno=146]	Subsequent attempt to reconnect to
Apr 30 20...	yankee	iDAR[124...	[DETAIL_T...	[310202]			[errno=146]	Success with marking socket 8 as no
Apr 30 20...	yankee	iDAR[124...	[NOTICE] ...	[323706]			[errno=146]	(129.153.130.61+ 3389) syncConne
Apr 30 20...	yankee	iDAR[124...	[NOTICE] ...	[323706]			[errno=146]	Error: -5981 (0xffffe8a3)
Apr 30 20...	yankee	iDAR[124...	[TRACE] ...	[520502]			[errno=146]	Subsequent attempt to reconnect to
Apr 30 20...	yankee	iDAR[124...	[DETAIL_T...	[310202]			[errno=146]	Success with marking socket 8 as no
Apr 30 20...	yankee	iDAR[124...	[DETAIL_T...	[560308]			[errno= 13]	Poll on listen ports timed out.
Apr 30 20...	yankee	iDAR[124...	[NOTICE] ...	[323706]			[errno=146]	(129.153.130.61+ 3389) syncConne
Apr 30 20...	yankee	iDAR[124...	[NOTICE] ...	[323706]			[errno=146]	Error: -5981 (0xffffe8a3)
Apr 30 20...	yankee	iDAR[124...	[TRACE] ...	[520502]			[errno=146]	Subsequent attempt to reconnect to

Time/Date	Apr 30 2002 12:30:29
Host	yankee
Process[PID]	iDAR[12478]:
Event	[NOTICE]
Number	[323706]
Client	
Server	
Error #	[errno=146]
Message	(129.153.130.61+ 3389) syncConnection failed.

Description of the form elements are as follows:

Refresh. Reads the log and displays the records in the table below.

Continuous. Select this setting to have this view continuously refreshed with the most current log records.

Log file. Displays the name of the file currently being viewed.

Lines to show. Specifies the maximum number of lines to read from the log file.

Chapter 11

Configuring Security

Sun ONE Directory Proxy Server supports SSL/TLS for secure communication between its clients and backend directory servers in the following sections:

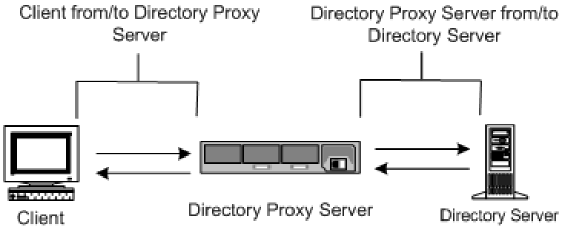
- Preparing to Set Up SSL and TLS
- Setting Up SSL Communication

Some of the information in this section is written with an assumption that you are familiar with the basic concepts of public-key cryptography and Secure Sockets Layer (SSL) protocol, and understand the concepts of intranet, extranet, and the Internet security and the role of digital certificates in an enterprise. If you are new to these concepts, we recommend you read the security-related appendixes of the manual, *Managing Servers with Sun ONE Console*.

If you are upgrading from iDAR 5.0x, then the procedure to migrate SSL configuration is detailed in the *Directory Proxy Server Installation Guide*.

Directory Proxy Server has two separately configurable communication links. Each communication link can be plaintext or encrypted using Transport Layer Security (TLS) or Secure Sockets Layer (SSL) protocol. Availability of the two separate communication links enables you to configure TLS- or SSL-enabled communication between an LDAP client and Directory Proxy Server and between Directory Proxy Server and an LDAP directory. Figure 11-1 illustrates this capability of Directory Proxy Server.

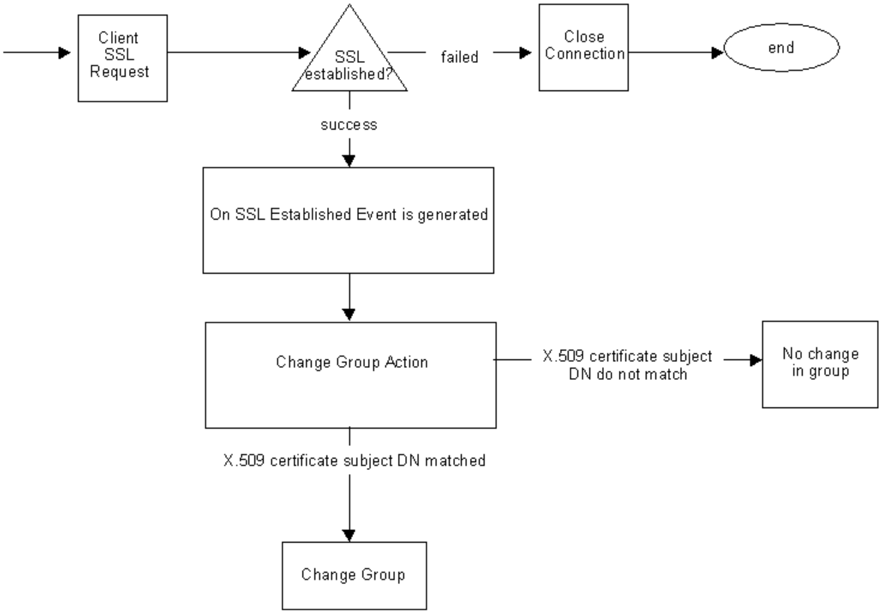
Figure 11-1 Two Separate Communication Links in Directory Proxy Server


Client from/to Directory Proxy Server
Directory Proxy Server from/to Directory Server
Client
Directory Proxy Server
Directory Server

Directory Proxy Server can verify both client and server certificates, provided the trusted root CA certificate for the certificate being validated is installed and is available to Directory Proxy Server.

Figure 11-2 illustrates how Directory Proxy Server can verify the certificates presented to it by the clients after they establish an SSL session.

Figure 11-2 Certificate-Based Authentication of Clients



Preparing to Set Up SSL and TLS

You will need to set up SSL and TLS differently depending on whether you are using an internal security device, an external hardware device, or both. This section will tell you how to do this.

Setting up SSL or TLS with an Internal Security Device

To set up SSL or TLS with an internal security device, you must request and install a certificate. To request a certificate, run the Certificate Request Wizard. To install the certificate, run the Certificate Installation Wizard. When prompted, specify that you want to install the certificate on the internal security device.

Setting up SSL or TLS with an External Security Device

To set up SSL with an external security device, such as FORTEZZA, first install the PKCS #11 module provided by the external device manufacturer. Then run the Certificate Request Wizard, specifying the external security device when prompted.

Setting Up SSL with Internal and External Security Devices

Some servers and clients in your enterprise may use only internal security devices, while others may use both internal and external security devices. If your server needs to communicate with products running both internal and external security devices, run the Certificate Request Wizard *two times*. During the first use, when prompted, specify the internal security device. During the second use, when prompted, specify the external security device.

Setting Up SSL Communication

In general, setting up Directory Proxy Server for SSL-enabled communication involves these steps:

- Step 1. Install a Server Certificate for Directory Proxy Server
- Step 2. Set Up SSL Connections Between Directory Proxy Server and Clients
- Step 3. Set Up SSL Connections Between Directory Proxy Server and LDAP Servers

Step 1. Install a Server Certificate for Directory Proxy Server

When requesting and installing certificates, you use two wizards. You use the Certificate Request Wizard to request a new server certificate or to renew a certificate that you're already using. You use the Certificate Installation Wizard to install a certificate that you've received from a *Certificate Authority* (CA). The first time you use the Certificate Request Wizard, it will also create and install a *key and certificate database* for you.

To install a server certificate for Directory Proxy Server, follow these steps:

- Step A. Generating a Server Certificate Request
- Step B. Sending a Server Certificate Request
- Step C. Installing the Certificate
- Step D. To Install a CA Certificate or Server Certificate Chain
- Step E. Backing Up and Restoring Your Certificate Database

SSL Certificates

Sun ONE Directory Proxy Server can install three types of certificates: server certificates, server certificate chains, or trusted CA certificates.

A *server certificate* is a single certificate associated only with your server. It identifies your server to clients. You must request this type of certificate from a CA. To obtain and install a Server Certificate, generate a request and send it to the CA. Then install the certificate.

A *server certificate chain* is a collection of certificates automatically generated for you by your company's internal certificate server or a known CA. The certificates in a chain trace back to the original CA, providing proof of identity. This proof is required each time you obtain or install a new server certificate.

A *trusted CA certificate* is a single certificate automatically generated for you by your company's internal certificate server or a known CA. A trusted CA certificate is used to authenticate clients.

To obtain a trusted CA certificate, first go to the internal certificate server or CA's web site. Copy the necessary certificate information and save it to a file. Then use the Certificate Installation Wizard to install the certificate.

You can install any number of SSL certificates on a server. When setting up SSL for an instance of Directory Server, you need to install at least a server certificate and a trusted CA certificate.

Step A. Generating a Server Certificate Request

You can use Sun ONE Directory Proxy Server to generate a certificate request which you can then submit to a Certificate Authority (CA).

1. In the Sun ONE Directory Proxy Server navigation tree, select the server instance with which you want to use SSL encryption.
2. Double-click the server instance or click Open to open the management window for the server instance.
3. From the Console menu, choose Security > Manage Certificates.

   You can also click the Manage Certificates task.

   If the security device does not have a password you are prompted to enter a new password.
4. Click Request to open the Certificate Request Wizard.
5. Choose "Request Certificate Manually," and then click Next.

6. Enter the requested information:

   Server Name. (Optional) Enter the fully qualified hostname of the machine for which you're requesting a certificate.

   Organization. (Optional) Enter your organization's name.

   Organizational Unit. (Optional) Enter your division, department, or other organizational unit.

   City/locality. (Optional) Enter the city or locality in which your organizational unit is located.

   State/province. (Optional) Enter the state or province in which your organizational unit is located.

   Country/region. (Optional) Select the state or province in which your organizational unit is located, from the drop-down menu.

   You can toggle between two views of the request form using the following buttons:

   Show DN. Click to show the requestor information in distinguished name (DN) format. This button is visible only when you are entering information in fields.

   Show Fields. Click to show the requestor information in fields. This button is visible only when you are entering information in DN format.

7. Click Next.

8. Enter the password for the security device that will store this certificate.

   If you are using the internal (software) security device, this is the password for the key and certificate database. If you are using an external (hardware) module, this is the password for your SmartCard or other security device.

9. Click Next.

10. Select one of the following:

    Copy to Clipboard. Click to copy your certificate request to the clipboard.

    Save to File. Click to save your request as a text file. You will be prompted to choose a name and location for the file.

11. Click Done to close the Certificate Request Wizard.

Step B. Sending a Server Certificate Request

Once you have generated a server certificate request, you send it to a CA for processing. Many CAs allow you to submit certificate requests through their web sites. Others may require you to send them an email message containing your request.

1. Use your email program to create a new email message.
2. Paste your certificate request into the message.

   If you saved your certificate request to a file, open it in a text editor. Copy and paste the request into the body of the message.

   If you copied the certificate request to the clipboard, paste it into the body of the message.
3. Enter a subject and recipient for your request. The type of subject and recipient varies depending on which CA you are using. For more information, see your CA's web site.
4. Send the email message to the CA.

Once you've submitted your request, you must wait for the CA to respond with your certificate. Turnaround time is highly variable and depends on the CA. If your company has an internal CA, it may take only a day or two to receive your certificate. If you are using an external CA, it could take as long as several weeks for that CA to respond to your request.

Step C. Installing the Certificate

Depending on the CA, you may receive your certificate in an email message or you may have to retrieve it from the CA's web site. Once you have the certificate, you can back it up and install it.

1. Save, in a text file, the certificate data you received from the CA.

   If you ever lose the certificate data, you can reinstall the certificate using this backup file.
2. In the Sun ONE Directory Proxy Server navigation tree, select the server instance on which you want to install the certificate.
3. Click Open to open the management window for the server instance.
4. On the Tasks tab, click the Manage Certificates task button.

   You can also open the Console menu, and then choose Security > Manage Certificates.

5. Click the Server Certs tab.
6. Specify where to store this certificate.
    - If you want to store this certificate on the internal security device, select internal (software) from the Security Device drop-down list, and then click Install.
    - If you want to store this certificate on an external hardware device, select the device from the Security Device drop-down list, and then click Install.
7. Enter the certificate's location or enter its text.

    In this local file. If your certificate is stored in a text file on your system, enter the full path to the file.

    In the following encoded text block. If you copied your certificate to the clipboard, paste the certificate's text into the text field by clicking the Paste from Clipboard button.
8. Click Next.

    If the certificate information you entered above is valid, you see a page containing the details of your certificate.
9. Verify that the certificate information is correct, and then click Next.
10. Enter a name for the certificate, and then click Next.
11. Enter the password for the security device that will hold this certificate.

    If you are installing the certificate on the internal (software) security device, enter the password for the key and certificate database. If you are installing a certificate on an external (hardware) security device, enter the password for the device.
12. Click Done.

Step D. To Install a CA Certificate or Server Certificate Chain

1. Obtain the CA certificate or Server Certificate Chain from your CA.
2. In the Sun ONE Directory Proxy Server navigation tree, select the server instance on which you want to install the CA certificate.
3. Click Open to open the management window for the server instance.
4. On the Tasks tab, click the Manage Certificates task button.

    You can also open the Console menu, and then choose Security > Manage Certificates.

5. Select the CA Certs tab, and then click Install.
6. Enter the certificate's location or enter its text:

   In this local file. If the certificate is stored in a text file on your system, enter the full path to the file.

   In the following encoded text block. If you copied the certificate to the clipboard, paste the certificate's text into the text field by clicking the Paste from Clipboard button.

7. Click Next.

   If the certificate information you entered above is valid, you see a page containing the details of the certificate.

8. Verify that the certificate information is correct, and then click Next.
9. Enter a name for the certificate, and then click Next.
10. Select the trust options for this certificate:

    Accepting Connections from Clients. Check this box if you want to trust client certificates issued by this CA.

    Making Connections to Other Servers. Check this box if you want to trust server certificates issued by this CA.

11. Click Done.

Step E. Backing Up and Restoring Your Certificate Database

Whenever you install a certificate, you should back up your certificate database. If your database ever becomes corrupted, you can restore your certificate information from this backup.

To Back Up Your Certificate Database

1. Open your server root folder.
2. Copy all files in the `alias` folder to another location (preferably on a different disk).

   This folder includes your certificates as well as the private key for your trust database.

To Restore Your Certificate Database From a Backup

- Copy your backup files to the `alias` sub-folder of your server root folder.

CAUTION If you restore your certificate database from a backup, any certificates that you installed after making the backup will be lost. Before restoring your certificate database, make sure that you have copies of all your certificates in case you need to reinstall them.

Step 2. Set Up SSL Connections Between Directory Proxy Server and Clients

To set up SSL connections between Directory Proxy Server and LDAP clients, follow these steps:

- Step A. Add Directory Proxy Server CA Certificate to Clients' Trust Databases
- Step B. Make Changes to the Directory Proxy Server System Configuration
- Step C. Make Changes to the Directory Proxy Server Network Groups

Step A. Add Directory Proxy Server CA Certificate to Clients' Trust Databases

---

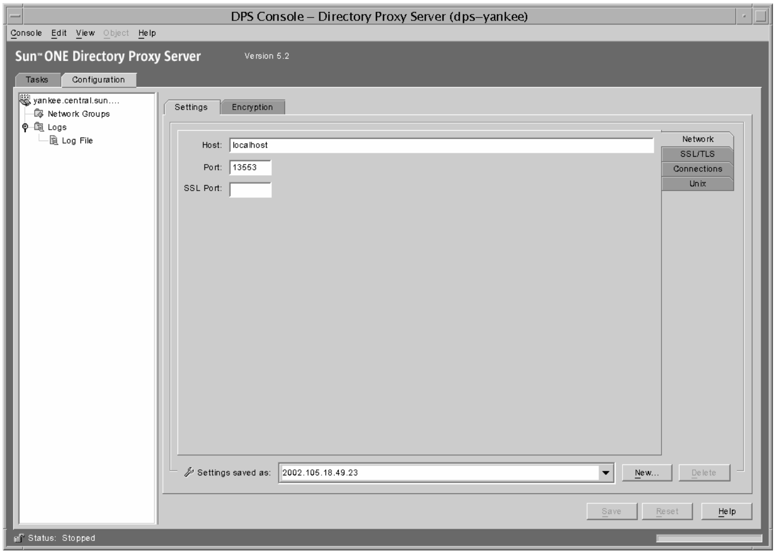
NOTE This step is necessary only if the client verifies the server certificate. All Netscape and Sun clients do verify. However, there are clients that do not verify. In that case setting the trust is not necessary.

When Directory Proxy Server presents its certificate to an LDAP client, the client tries to verify the validity of the certificate. As a part of this verification process, the client checks whether the CA that has issued the certificate is trusted by the client. For this reason, the root certificate of the CA that issued Directory Proxy Server's server certificate must be installed in the client's trust database.

In the last step of installing Directory Proxy Server's server certificate, you copied the Directory Proxy Server's CA certificate to a text file. Follow the documentation for each client application, and install the CA certificate in its trust database.

Step B. Make Changes to the Directory Proxy Server System Configuration

The Settings and Encryption tabs in the Directory Proxy Server Console window enable you to define SSL-enabled communication criteria for Directory Proxy Server. For details, see "Creating System Configuration Instances," on page 57.



Host: localhost
Port: 13553
SSL Port:
Settings saved as: 2002.105.18.49.23

Make the following changes to the appropriate system configuration instances, and save your changes.

- In the Settings tab, specify a value in the "SSL port" field. Directory Proxy Server will listen on the port number you specify for LDAPS (LDAP over SSL) connections. By default, Directory Proxy Server does not listen for connections from LDAPS clients. This value must be present to enable LDAPS connections from clients that use the alternative port 636 method to establish TLS/SSL. This value must be different from the value in the Port field. (This option also requires TLS/SSL configuration found on the Encryption tab.)

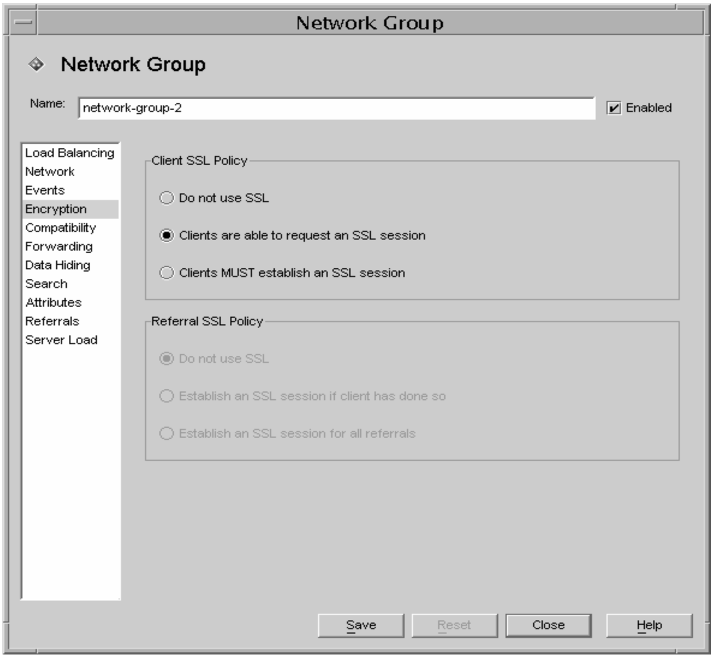
  If you need description for the parameters, click the Help button.

- In the SSL/TLS Encryption tab, specify all the required information.

  If you need description for the parameters, click the Help button.

Step C. Make Changes to the Directory Proxy Server Network Groups

Directory Proxy Server uses network groups to identify clients and determine their access privileges to the information contained in an LDAP directory; for details, see Chapter 6, “Creating and Managing Groups.”



Network Group

Name: network-group-2 ☑ Enabled

Client SSL Policy

○ Do not use SSL

● Clients are able to request an SSL session

○ Clients MUST establish an SSL session

Referral SSL Policy

● Do not use SSL

○ Establish an SSL session if client has done so

○ Establish an SSL session for all referrals

In each group that you’ve configured, set the appropriate options in the Encryption tab to indicate whether you want to force the client to start a TLS session before sending any LDAP operation, leave the decision to the client, or disallow the client to start a TLS session. For example, you might want to enable “SSL is available” and “Clients MUST establish an SSL session” options. For more information about the options presented in the Encryption tab, see Step 9 on page 77 of Chapter 6, “Creating and Managing Groups.”

If referral following is enabled, you should check the Referral SSL Policy. Referral following is enabled by selecting Referrals in the list on the left side of the window.

Directory Proxy Server can follow referrals returned by the backend servers. The LDAP URL’s returned must be in RFC 2255 format. If no host port is given, the client must have some knowledge of an appropriate LDAP server to contact.

Directory proxy server interprets LDAP URL’s with no host or port number as a referral to the same host that issued the referral. For example:

`ldap:///dc=central,dc=sun,dc=com`	Referral to the same host, port with a different base.
`ldap://:10389/`	Referral to the same host but different port.
`ldap://host/`	Referral to the host “host” on the default port 389.

Step 3. Set Up SSL Connections Between Directory Proxy Server and LDAP Servers

To set up SSL connections between Directory Proxy Server and LDAP servers, follow these steps:

- Step A. To Install a CA Certificate or Server Certificate Chain
- Step B. Add Directory Proxy Server CA Certificate to the LDAP Servers’ Trust Databases
- Step C. Make Changes to the LDAP Server Properties

Step A. To Install a CA Certificate or Server Certificate Chain

This step is required if you want Directory Proxy Server to verify the certificate presented to it by an LDAP server. For details, see “Step D. To Install a CA Certificate or Server Certificate Chain,” on page 156.

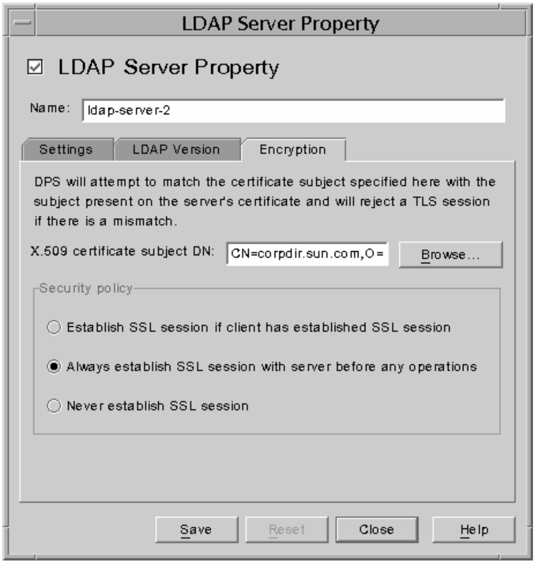
Step B. Add Directory Proxy Server CA Certificate to the LDAP Servers’ Trust Databases

When Directory Proxy Server presents its certificate to an LDAP server, the server tries to verify the validity of the certificate. As a part of this verification process, the server checks whether the CA that has issued Directory Proxy Server’s certificate is trusted by the server. For this reason, the root certificate of the CA that issued Directory Proxy Server’s server certificate must be installed in the LDAP server’s trust database.

In the last step of installing Directory Proxy Server's server certificate, you copied the Directory Proxy Server's CA certificate to a text file. Follow the documentation for each LDAP server, and install the CA certificate in its trust database. If you're using Sun ONE Directory Server, you can use the Manage Certificates Wizard, which can be launched from the Tasks tab of the Directory Server Console, to add the CA certificate to the Directory Server's trust database.

Step C. Make Changes to the LDAP Server Properties

The Encryption tab in the LDAP Server Property window enables you to define SSL-enabled communication criteria for each LDAP server. For details, see "Creating LDAP Server Property Objects," on page 108.



☑ LDAP Server Property

Name: ldap-server-2

DPS will attempt to match the certificate subject specified here with the subject present on the server's certificate and will reject a TLS session if there is a mismatch.

X.509 certificate subject DN: CN=corpdir.sun.com,O=

Security policy

○ Establish SSL session if client has established SSL session
● Always establish SSL session with server before any operations
○ Never establish SSL session

Make the following changes to the appropriate LDAP Server property objects, and save your changes.

- Set the "Security policy" option to an appropriate value so that Directory Proxy Server will always establish SSL/TLS to the backend server, never establish TLS/SSL to the backend server, or only establish SSL/TLS with the backend server when the client does the same to Directory Proxy Server.

- Set the “X.509 certificate subject DN” field to the LDAP server’s certificate subject name (the subject attribute in the X.509 certificate). If specified, Directory Proxy Server will attempt to match the certificate subject with the subject present on the LDAP server’s certificate and will reject a TLS session if there is a mismatch. (This attribute allows Directory Proxy Server to authenticate the LDAP server to which it is connecting. Directory Proxy Server accepts any name if this attribute is not set.)

Part 3

Appendixes

Appendix A

Directory Proxy Server Decision Functions

This appendix describes the flow of control in Directory Proxy Server for some specific functionalities. It includes:

- Establishing Group on Connection (page 167)
- Change Group on Bind (page 168)
- Change Group on Establishment of TLS (page 169)
- High Availability Setup (page 170)
- Following Referrals (page 171)

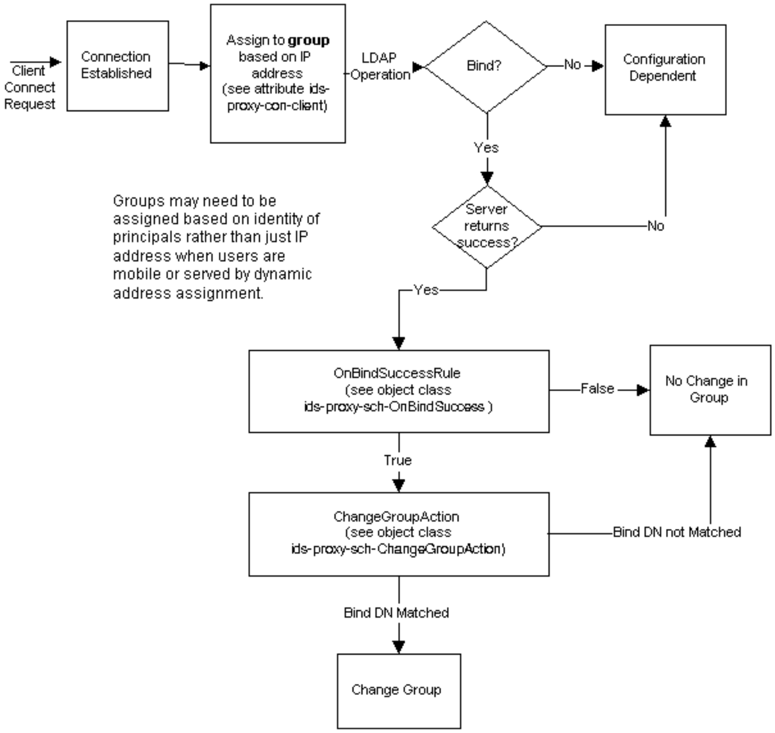
Establishing Group on Connection

When a client makes a connection to Directory Proxy Server, it checks the `ids-proxy-con-Client` attribute in `ids-proxy-sch-NetworkGroup` object entries until it finds a match. The `ids-proxy-sch-NetworkGroup` objects are tried in highest to lowest priority defined by the `ids-proxy-con-priority` attribute. Directory Proxy Server places the client in the first group whose `ids-proxy-con-client` attribute matches the IP address of the client. If no matching groups are found, the connection is closed.

Change Group on Bind

When the client initially connects, it is placed in a group based on its IP address. The client can be moved to a different group with different access controls when it binds to a directory. To accomplish this, the initial group object must include a rule object that is evaluated on a successful bind operation. If the rule evaluates to `TRUE`, the change group action is taken to move the client to a different group. Figure 11-3 illustrates this functionality.

Figure 11-3 Change Group on Bind


Client Connect Request
Connection Established
Assign to **group** based on IP address (see attribute ids-proxy-con-client)
LDAP Operation
Bind?
No
Configuration Dependent
Yes
Server returns success?
No
Yes
Groups may need to be assigned based on identity of principals rather than just IP address when users are mobile or served by dynamic address assignment.
OnBindSuccessRule (see object class ids-proxy-sch-OnBindSuccess)
False
No Change in Group
True
ChangeGroupAction (see object class ids-proxy-sch-ChangeGroupAction)
Bind DN not Matched
Bind DN Matched
Change Group

Configuring Change Group On Bind

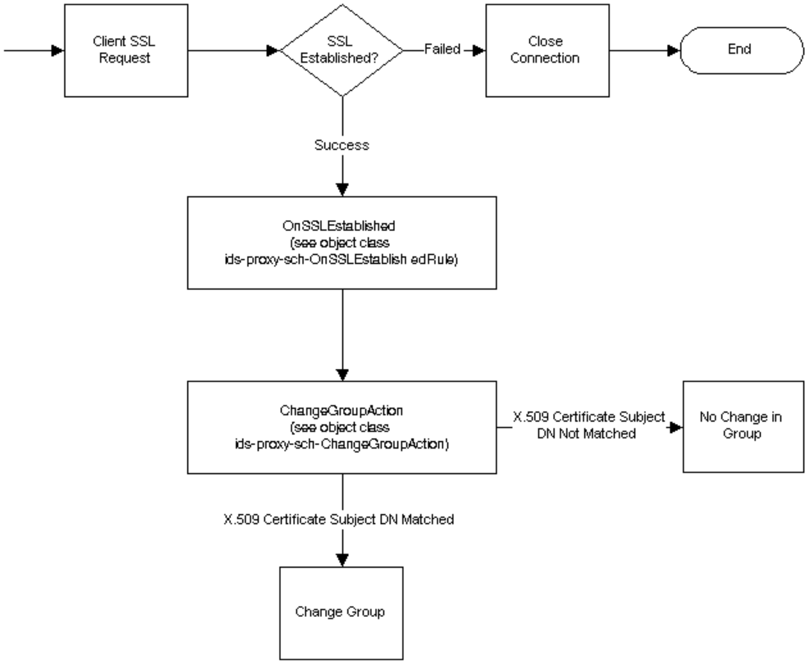
The following steps illustrate how to configure the Directory Proxy Server to change group upon a successful bind by “cn=Directory Manager” using the simple bind authentication mechanism.

1. Create a new Network Group to which the user cn=”Directory Manager” will move upon a successful bind. For more information see “Creating Groups,” on page 72. If a user can only be part of this group by changing into it, set “No IP Binding” in the Network tab of the Network Group panel. Also make sure this group come after all other Network Groups that allow some IP bindings.
2. Create a new “Change Group” action. For more information see “Creating Action Objects,” on page 132. Set changed to, to the name of the group you created in step 1. Set “if DN matches” to “cn=Directory Manager”. You can also set “NONE” (do not change group) for all others, i.e. “.*”.
3. Create a On Bind Event. For more information see “Creating OnBindSuccess Event Objects,” on page 124. On the actions tab set it to the change group action you created in step 2. On the condition tab select “Password based bind”.
4. Select the On Bind event you created in step 3 on the events tab in the Network Group you created in step 1. For more information see “Modifying Groups,” on page 95.

Change Group on Establishment of TLS

Similar to the change group on bind mechanism is the change group on establishment of TLS, whereby a client can change group when it successfully establishes an TLS session. The SSL Established rule is evaluated when the client establishes TLS, following which the Change Group action follows. This functionality is illustrated in Figure 11-4.

Figure 11-4 Change Group on Establishment of TLS


Client SSL Request
SSL Established?
Failed
Close Connection
End
Success
OnSSLEstablished (see object class ids-proxy-sch-OnSSLEstablishedRule)
ChangeGroupAction (see object class ids-proxy-sch-ChangeGroupAction)
X.509 Certificate Subject DN Not Matched
No Change in Group
X.509 Certificate Subject DN Matched
Change Group

High Availability Setup

If you have configured more than one backend directory server, then you can set up Directory Proxy Server to load balance across these and fail over to another if one of the backend servers goes down. In order to do this, you must create a Load Balance Property (see "Load Balancing Property," on page 113 or "ids-proxy-sch-LoadBalanceProperty Object Class," on page 222) and include it in the group object for which you want to load balance. You will also need to create LDAP Server Properties (see "LDAP Server Property," on page 108 or "ids-proxy-sch-LDAPServer Object Class," on page 227) for each of your backend servers and include it in the Load Balance Property. You must specify the amount of load in percentage of total load each of your backend servers should handle in the Load Balance Property object. With this setup, Directory Proxy Server will redistribute load across its backend directory servers if one of them goes down. It will fail over clients from one server to another in case the first goes down. Directory Proxy Server will also fail over if the network link between itself and the LDAP server is down or if the LDAP server becomes unresponsive (see "ids-proxy-con-keepalive-interval," on page 229).

NOTE Directory Proxy Server is unable to fail over if the client was bound using a SASL mechanism.

Following Referrals

Directory Proxy Server can be set up to follow referrals for LDAPv2 clients that cannot do so on their own. Your backend LDAP directory server must be capable of sending referrals, i.e., it must support LDAP v3 standards. Configure Directory Proxy Server to use LDAP v3 between itself and the backend LDAP server in order for Directory Proxy Server to receive referrals from the directory server (see “ids-proxy-con-use-version,” on page 228). Then set your group’s referral (see “Controlling the Return of Referrals,” on page 217) and continuation referral policy (see “ids-proxy-con-search-reference,” on page 217).

Directory Proxy Server FAQ, Features, and Troubleshooting

This appendix contains useful information on Sun ONE Directory Proxy Server. It contains answers for frequently asked questions (FAQs), clarifications on certain Directory Proxy Server features, and troubleshooting information.

The appendix has the following sections:

- Directory Proxy Server FAQ (page 173)
- Directory Proxy Server Features (page 175)
- Troubleshooting (page 177)

Directory Proxy Server FAQ

What is Directory Proxy Server?

Directory Proxy Server is an LDAP proxy for LDAP clients and LDAP servers. Requests from LDAP clients are forwarded to LDAP servers based on rules defined in Directory Proxy Server configuration. Results from the server are passed back to clients, again based on rules defined in the configuration. This process is totally transparent to the clients, which connect to Directory Proxy Server just as they would to any LDAP server.

Why do I need an LDAP Proxy Server?

Many enterprises want to make some part of their directory information externally visible, while keeping other parts internally private. With Directory Proxy Server you can accomplish this goal easily, and without assigning directory passwords to external clients. Directory Proxy Server can also be used as a high availability solution for enterprise directory service with load balancing and failover features.

Additional security features such as protection from denial of service attacks and search limits are also provided.

What version of the LDAP protocol does Directory Proxy Server support?

Directory Proxy Server supports LDAP clients or chaining LDAP servers that use either the LDAPv2 or the LDAPv3 protocol.

Does Directory Proxy Server support secure authentication and encryption?

Directory Proxy Server supports SSLv3 services for public-key based data encryption using certificates. Secure authentication and encryption available to LDAP clients can useeither the secure LDAP port or the Internet Transport Layer Security (TLS) model, which uses the Diffie-Hellman, Digital Signature Standard (DSA), and Triple-DES algorithms.

Does Directory Proxy Server work with any LDAP-enabled directory server?

Directory Proxy Server will work with any LDAP-conformant directory server. Some directory product vendors claim to implement LDAP in their marketing literature, but the reality is often a different story. Directory Proxy Server has been the most thoroughly tested with the Sun ONE Directory Server.

If the Directory Proxy Server 5.0 Console is used, the Sun ONE Directory Server 5.0 is the supported configuration depository.

Is there a configuration utility available to configure Directory Proxy Server?

Directory Proxy Server 5.0 includes a Java-based GUI (console) that can be used to configure Directory Proxy Server. The console uses the Sun ONE Directory Server to store the configuration it generates.

Directory Proxy Server Features

Can Directory Proxy Server be used to prevent denial-of-service attacks?

Yes. You can limit the number of simultaneous operations processed per connection, number of operations allowed per connection, total number of concurrent connections, maximum concurrent connections per defined group (network, subnetwork or based on bind DN), and maximum concurrent connections for a single IP address.

Does Directory Proxy Server support “reverse” proxying?

In a strict sense, Directory Proxy Server is a reverse proxy; however, the LDAP protocol does not support the concept of reverse proxying.

Can Directory Proxy Server be used to prevent “trawling” of an LDAP directory?

Yes. Trawling refers to very broad queries designed to download large portions of your directory, a practice many sites wish to prohibit. Directory Proxy Server can prohibit or limit trawling in a number of ways:

- The scope of searches can be limited to a single level of the directory tree, entire subtrees can be hidden, and a hard limit on the number of entries returned in response to a query can be set.
- Inequality searches can be forbidden, thus disallowing searches that return many results based on exclusion and substring searches can be restricted by length; for example, prohibiting searches for all entries with a surname starting with the letters A-Z.
- Directory Proxy Server can also be configured to deny un-indexed searches. Un-indexed searches are inefficient and can possibly have a negative impact in performance.

Does Directory Proxy Server do automatic load balancing of queries?

Directory Proxy Server supports automatic server load balancing among a set of back-end LDAP servers. Directory Proxy Server also supports automatic fail-over to a secondary LDAP server if the primary LDAP server is down.

How many LDAP servers can one Directory Proxy Server server load balance?

The performance needs of the directory server and the complexity of work being done by Directory Proxy Server determines the optimal number of directory servers that Directory Proxy Server should load balance. For example, if Directory Proxy Server is doing complicated work, such as attribute renaming, the number of directory servers Directory Proxy Server is configured to load balance should be reduced. Consider adding more Directory Proxy Server units to compensate for possible performance impacts of complex Directory Proxy Server configurations.

Can search requests be filtered?

Yes. You can configure Directory Proxy Server to refuse searches that attempt to search on a particular attribute. In addition, you can configure Directory Proxy Server to modify incoming search requests to conform to a designated minimum search base, search scope, and time limit.

Can search results be filtered?

Yes. Results can be filtered both in terms of number of entries returned and the attributes that are included in the result set. Search result entries can also be filtered based on the entry DN or content.

How are access groups defined?

Varying levels of access to the directory are provided to clients based on the network address of the client. Thus, different levels of access can be granted to clients outside the corporate firewall, inside the firewall, on the executive subnetwork, and even to individual machines. Further, access level can be changed upon a successful completion of a LDAP Bind operation by the client or when a SSL session is established.

Does Directory Proxy Server support protected password authentication?

Yes. Through the use of the SASL mechanism a variety of protected password authentication schemes can be implemented. These mechanisms must be supported by the back-end directory server. Directory Proxy Server does not support SASL mechanisms with connection protection and SASL EXTERNAL mechanism.

Does Directory Proxy Server automatically follow referrals?

The following of referrals is configurable based on access group. Various access groups can be configured to automatically follow referrals, return referrals, or discard referrals.

Does Directory Proxy Server cache search result information?

Directory Proxy Server Version 5.0 SP1 does not support search result caching.

Can Directory Proxy Server do attribute renaming?

Directory Proxy Server can transparently rename attribute names between clients and servers.

Troubleshooting

How can I analyze logs of connection attempts?

Directory Proxy Server can be configured to either use `syslog` or write to a specified log file. A popular UNIX utility known as swatch is freely available from Stanford University via ftp at (`ftp://ftp.stanford.edu/general/security-tools/swatch`). Swatch can be used to monitor the log files generated by Directory Proxy Server and to notify the administrator when defined events occur.

I have configured Directory Proxy Server to follow referrals. However, when I perform a search with a LDAPv2 client I get error 32 (No such object) or some other error.

In order for Directory Proxy Server to receive referrals from the back-end servers, it must use LDAPv3. Make sure you have selected “LDAP version 3 only” on each of your LDAP server properties.

I notice in the log files that some idle client connections are routinely failed over even though all my back-end servers are up.

Your back-end directory server is timing out idle connections and closing them. Directory Proxy Server fails over these closed connections. You must set an idle connection timeout for Directory Proxy Server as well. This will clean up idle and leaked client connections and also guard against one form denial of service attack.

Is there a way to restrict search requests containing the presence filter?

Directory Proxy Server Version 5.0 SP1 does not have any direct mechanisms to restrict clients from using the presence filter. There are two indirect ways to address this issue.

You can set the `ids-proxy-con-forbidden-compare` to the name of the attribute that you do not want to be compared. This method is over restrictive, as it will reject searches containing both (mail=*) and (mail=Andy*) filters.

On the other hand, since presence filters (attrName=*) always generate the same result (assuming the data did not change), we can use the ids-proxy-con-size-limit attribute and the `ids-proxy-sch-SizeLimitProperty` to limit the damage. Although LDAP does not require entries to be returned in a given order, under most (all) implementations, the set of results will either be returned in sorted order or unsorted order, and these will be the same every time. Hence, if Directory Proxy Server is configured with a size limit, (using the size-limit attribute or the SizeLimitProperty) only the first 'n' of these sets will be returned every time. Because there can only be two sets of these 'n' entries, the risk of trawling the directory is greatly reduced.

Note that Directory Proxy Server tries to set this size limit in the request itself when possible, and therefore the directory server will not be burdened with sending all the entries.

The size limit property gives you the option of applying exceptions to size limits imposed when necessary. Suppose, for example, that you have an entry of o=A, under which there are 400 organization units. Under each of those OU’s there are people. If you want clients to see all the OU’s but only see 5 people at a time, you can set up the `SizeLimitProperty` such that no limit is applied for a search with base o=A and one level scope. For all other searches a limit of 5 applies.

When I try to execute a task or perform some console function, I get an error message saying I need to make sure the Administration Server is running properly and that this host is permitted to connect to the Administration Server.

Log in to the Administration Server that is managing the Directory Proxy Server whose console produced the error messages. It may be necessary to start the Sun ONE Console on the host machine of the Administration Server. Open the server console for the Administration Server that is managing the Directory Proxy Server on which you are unsuccessfully trying to invoke tasks. Click the Configuration tab and then the Network tab. Under Connection Restrictions, make sure that the host machine of the Sun ONE Console that is unsuccessfully trying to manage Directory Proxy Server is not restricted from accessing the Administration Server. See the Sun ONE Console *Server Management Guide* for more information.

Appendix C

Directory Proxy Server Startup Configuration File

This appendix contains information about the Directory Proxy Server configuration file. It includes:

Configuration File Overview

The `tailor.txt` file contains the bootstrap information Directory Proxy Server needs to locate its main configuration. The directives in this file dictate if Directory Proxy Server will utilize an additional file for its main configuration or if Directory Proxy Server will solicit its main configuration from an LDAP server. By default, Directory Proxy Server expects to find the startup configuration file, `tailor.txt`, in the `etc` subdirectory of the installation's instance directory. Note: via the use of the command-line parameter `-t`, Directory Proxy Server can be instructed to use an alternate file as its startup configuration file.

As an aid in supporting high availability configurations, a startup configuration file may list several contact points for the main configuration's retrieval. Contact points are delineated within the startup configuration file by the use of two keywords: `Begin` and `End`. Directory Proxy Server will process the contact information one by one in the order given. Directory Proxy Server's actions on each contact point depends on the type of the given contact point (either an LDAP URL or an absolute path name to a file).

For LDAP-URL-based contact points, Directory Proxy Server will attempt to contact the given host. If the host is unwilling or unable to return a configuration, then Directory Proxy Server will proceed to its next contact point (if any). If the host returns a configuration, then Directory Proxy Server will edit the contents returned and will then either begin following the main configuration's directives or end its execution if the configuration was deemed invalid.

For file based contact points, Directory Proxy Server will attempt to load the given file as its main configuration. If the specified configuration is missing or is deemed invalid, Directory Proxy Server will end its execution. Directory Proxy Server will not attempt to move to the next contact point once it encounters a file based contact point.

In the case where Directory Proxy Server is retrieving its main configuration from an LDAP host, Directory Proxy Server can bind to the host using one of three methods: anonymous, simple, or by using SASL.

Anonymous binding is accomplished by omitting the `configuration_bind_pw` and `configuration_bind_dn` directives. In other words, your startup configuration's contact information would specify a `configuration_url` directive and nothing else.

Simple binding is supported through the use of both the `configuration_bind_pw` and the `configuration_bind_dn` directives.

SASL binding requires the specification of the `sasl_bind_mechanism`, `conguration_bind_pw` and one (and only one) of the following directives: either `configuration_bind_dn` or `configuration_username`.

Startup Configuration's Keywords

Each enumerated contact point uses the keyword `Begin` to signify the start of a contact point entry. Conversely, each contact point entry is terminated by the keyword `End`. Every directive stipulated in a startup configuration file is expressed on a line by itself. Line continuation within the startup configuration is not recognized nor supported. The configuration's options are specified via an option, followed by a colon, and a value triplet.

configuration_url

The `configuration_url` option specifies either an LDAP directory server and the distinguished name of the entry in that directory where the Directory Proxy Server configuration is stored, or a local file in LDIF format. For example, if the Directory Proxy Server configuration is stored in an LDAP directory on host `ldap.sun.com` with the LDAP service running on port `389` and the distinguished name of the Directory Proxy Server entry is "`ids-proxy-con-Server-Name=Directory Proxy Server`", then the following should be added to the configuration file:

```
Begin
configuration_url:
ldap://ldap.sun.com:389/ids-proxy-con-Server-Name=Directory Proxy
Server
End
```

If the configuration is to be kept in an LDAP server, you would probably need to specify a suffix following the `ids-proxy-con-Server-Name=Directory Proxy Server` in order to maintain compatibility with the host directory's naming context. For example:

```
Begin
configuration_url:
ldap://ldap.sun.com:389/ids-proxy-con-Server-Name=Directory Proxy
Server,
ou=services, dc=sun, dc=com
End
```

Each startup configuration directive should be specified as one contiguous line within the configuration file.

NOTE Do not interpret the line wrapping in the `configuration_url` examples as an instruction to insert a line break into your configuration file.

In the case where the configuration is stored in a LDIF formatted file, i.e., `<server-root>/dps-<hostname>/etc/tailor.ldif`, the following should be added to the configuration file:

```
Begin
configuration_url:
file://<server-root>/dps-<hostname>/etc/tailor.ldif#ids-proxy-con-S
erver-Name=Directory Proxy Server
End
```

configuration_bind_dn

The `configuration_bind_dn` option specifies the distinguished name to use when Directory Proxy Server binds to the LDAP server specified in the `configuration_url` option. Directory Proxy Server will perform a simple bind with this distinguished name and the value of `configuration_bind_pw` as the password. For example:

```
Begin
configuration_url:
ldap://ldap.sun.com:389/ids-proxy-con-Server-Name=Directory Proxy
Server
configuration_bind_dn: cn=Directory Manager
configuration_bind_pw: secret
End
```

The `configuration_bind_dn` option is not needed and ignored if `configuration_url` is of the "file" form. Note: the `configuration_bind_dn` and `configuration_username` directives are mutually exclusive.

configuration_bind_pw

The `configuration_bind_pw` option is used to specify the password to use when binding to the LDAP directory. The directive is used to specify the password to use for either simple or SASL based binding. In order to preserve security, the configuration file must be protected against unauthorized reading. The `configuration_bind_pw` option is not needed and ignored if `configuration_url` is of the "file" form. (See `configuration_bind_dn` for an example.)

configuration_username

The `configuration_username` option specifies the username to use when Directory Proxy Server binds to the LDAP server specified in the `configuration_url` option. This option is used only if SASL bind mechanism is used. Note: the `configuration_bind_dn` and `configuration_username` directives are mutually exclusive.

```
Begin
configuration_url:
ldap://ldap.sun.com:389/ids-proxy-con-Server-Name=Directory Proxy
Server
```

```
configuration_username: administrator
configuration_bind_pw: secret
sasl_bind_mechanism: CRAM-MD5
End
```

sasl_bind_mechanism

The `sasl_bind_mechanism` option can be set to either `CRAM-MD5` or `DIGEST-MD5` depending on which SASL bind mechanism you want Directory Proxy Server to use. Directory Proxy Server will perform either a simple bind or an anonymous bind if this option is absent. `DIGEST-MD5` provides a higher level of security than `CRAM-MD5` but `DIGEST-MD5` has not been as widely adopted as `CRAM-MD5`.

Appendix D

Command Reference

This appendix describes helpful command line programs associated with Sun ONE Directory Proxy Server.

The appendix has the following section:

- "dpsconfig2ldif," on page 187
- "dpsldif2config," on page 187

dpsconfig2ldif

The utility `dpsconfig2ldif` is used to download Directory Proxy Server configuration and save it in an LDIF file. The utility is found at the following location:

```
<Install Root>/bin/dps_utilities/dpsconfig2ldif
```

The utility requires two arguments:

Argument	**Description**
-t *filename*	*Filename* is the path to the startup configuration file. This will usually be the tailor.txt file in the etc directory.
-o *filename*	The name of the file in which to output the configuration.

dpsldif2config

ImportConfigLdif imports an LDIF file generated by dpsConfig2Ldif.The utility is found at the following location:

```
<Install Root>/bin/dps_utilities/dpsldif2config
```

The utility requires the following arguments:

Argument	**Description**
ldif	name of ldif file containing Directory Proxy Server objects options:
-C	name of configuration to create (’imported-configuration’ if unspecified)
-h	directory host name (localhost if unspecified)
-p	directory port number (389 if unspecified)
-D	directory user dn (anonymous bind if unspecified)
-w	directory user password (anonymous bind if unspecified)
-v	verbose

ImportConfigLdif imports three kinds of objects:

- Shared Configurations (i.e. those located in the Main Console Topology Tree under the “Directory Proxy Server Configuration” node)
- Shared System Properties
- Shared Log Properties.

The parameter “Configuration Name” applies only to Shared Configuration objects just described. System and Log properties are added “as is” from the ldif file. If a shared configuration object does not exist with the given parameter name, this script will create a new configuration using the given parameter name. If there ALREADY exists a configuration with the given name, no import will take place. System and Log properties will not be added either if they already exist in the directory.

Once a configuration has been imported, the Main Console must be restarted in order to view the configuration in the Topology Tree. In order to begin using a configuration, a Directory Proxy Server instance server will have to assign itself to each configuration: shared Configurations are assigned via the Network Groups Node in the Directory Proxy Server Server Console; System Properties are assigned via the systems node in the Directory Proxy Server Server Console (“settings saved as...”); and Log Properties are assigned via the Logs node in the Directory Proxy Server Server Console (“settings saved as...”).

Pre-conditions:

- Migration from 5.0(sp 1) has already taken place.

Post-Conditions:

- belongs-to attribute is ignored in the imported ldif file.

Index