Deployment Guide

iPlanet™ Portal Server: Instant Collaboration Pack

Release 3.0.1

March 2002

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

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

Contents

Deploying iPlanet Portal Server: Instant Collaboration Pack

This guide gives an overview of the issues involved in designing and installing an instant messaging solution with iPlanet™ Portal Server: Instant Messaging Pack (also referred to as iPlanet™ Instant Messaging Server). It outlines important deployment concepts and installation decisions to be considered.

This guide contains the following sections:

- Planning the Operating System and Hardware
- Deploying in Portal or Standalone Mode
- Other Software Dependencies
- Planning Your Server Configuration
- Planning Your Client Configuration
- Planning Your Multiplexor Configuration
- Planning Security
- Planning for Accessing iPlanet Instant Messenger Outside a Firewall
- Tuning and Performance Issues
- iPlanet Instant Messaging Server Deployment Example

Planning the Operating System and Hardware

The first step in planning your iPlanet Portal Server: Instant Collaboration Pack configuration is to decide on the operating system platform and identify server hardware requirements. See the *iPlanet Portal Server: Instant Collaboration Pack Release Notes* for more information.

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

NOTE Installing iPlanet Instant Messaging Server in portal mode requires that your operating system be Solaris. iPlanet Portal Server currently runs only on Solaris.

Deploying in Portal or Standalone Mode

This section provides an overview of deploying iPlanet Instant Messaging Server in both portal and standalone modes.

Deployment Options

You can install and configure iPlanet Instant Messaging Server in one of two ways:

- As part of the iPlanet Portal Server environment, making iPlanet™ Instant Messenger available as an application in the iPlanet Portal Server Desktop Applications channel (Solaris only)
- As a standalone server

Whether you install iPlanet Instant Messaging Server in the iPlanet Portal Server environment or as a standalone server, you can use a variety of configurations to fit your site needs. See the *iPlanet Portal Server: Instant Collaboration Pack Administrator's Guide* for more information on these configurations.

Deploying iPlanet Instant Messaging Server in Portal Mode

iPlanet Instant Messaging Server enables you to utilize a number of different portal deployment scenarios, including:

- Using an external LDAP server
- Using iPlanet Portal Server's internal directory (instead of an external LDAP server)
- Installing iPlanet Instant Messaging server and client components on the same host (the portal host)
- Installing iPlanet Instant Messaging server and client components on different hosts

- Using the iPlanet Portal Server: Secure Remote Access Pack (gateway) for encrypted communication (secure mode) between clients and the iPlanet Instant Messaging server

You can add iPlanet Instant Messaging Server software to an existing portal deployment or create a fresh installation. When deploying iPlanet Instant Messaging Server in portal mode, answer the following questions before starting the installation:

- Do I want to deploy all the components on the portal host, or do I want to separate components onto two hosts? See the *iPlanet Instant Messaging Server Installation Guide* for more guidelines.
- Do I want to run the iPlanet Instant Messenger client in secure or non-secure mode? In secure mode, information is encrypted between the client machines and the iPlanet Instant Messaging server. If you choose to use secure mode, you must install the iPlanet Portal Server: SRAP (gateway) product.
- Do I want to use an external LDAP directory server, or iPlanet Portal Server's internal directory, for the iPlanet Instant Messenger user IDs? (You can still use whatever portal authentication mechanism you choose.)
- Do I have all the other required software installed? See the "Other Software Dependencies," on page 6 for more information on what other software is required.

Deploying iPlanet Instant Messaging Server in Standalone Mode

When deploying iPlanet Instant Messaging Server in standalone mode, you do not need to install the iPlanet Portal Server software. You will need an external LDAP directory server to contain the user IDs that iPlanet Instant Messaging server will use for authentication.

iPlanet Instant Messaging Server enables you to utilize two different standalone deployment scenarios:

- Installing the iPlanet Instant Messaging server, multiplexor, and client components on the same system
- Installing the iPlanet Instant Messaging server, multiplexor, and client components on different systems.

Other Software Dependencies

This section describes the server and client software needed by iPlanet Instant Messaging Server and iPlanet Instant Messenger. This additional software is not included with the iPlanet Instant Messaging Server software package.

Be sure to install all the recommended operating system patches before installing any of the other required software or iPlanet Instant Messaging Server itself.

NOTE Currently, there are no high-availablity cluster agents for iPlanet Instant Messaging Server.

Server Software Dependencies

iPlanet Instant Messaging server depends on the following software for proper operation. This software is not included with the iPlanet Instant Messaging Server software. You must install and configure this software separately. See the *iPlanet Portal Server: Instant Collaboration Pack 3.0 Release Notes* for information on supported software and versions.

- **iPlanet Portal Server** - Required for deploying iPlanet Instant Messaging Server in a portal environment. If you are installing iPlanet Instant Messaging Server in a standalone environment, you do not need to install iPlanet Portal Server. (However, you still might be required to buy the iPlanet Portal Server software.)
- **Directory Server** - Either an external LDAP directory for standalone or portal modes, or iPlanet Portal Server's internal directory for portal mode, is required. See "How iPlanet Instant Messenger Uses the Directory Server," on page 13 for more information.

NOTE For both portal and standalone modes, you can use an existing directory server; you do not need to install a directory server dedicated for iPlanet Instant Messaging Server use. See "Indexed LDAP Attributes," on page 17 for information on which directory attributes need to be indexed to optimize for iPlanet Instant Messaging Server.

- **Web Server** - Required to serve up HTML to iPlanet Instant Messenger and resolve URLs included in instant messages and news channel content.

NOTE **iPlanet Portal Server installations**: You must install the iPlanet Instant Messaging Server client component on the host containing the iPlanet Portal Server and use the web server that ships with iPlanet Portal Server. You can install the iIM server and multiplexor components either on the iPlanet Portal Server host or on a separate host.

- **SMTP server** - Required to send email to users who receive alerts while offline. In the absence of an SMTP server, alerts cannot generate email for offline users; otherwise, the product still functions normally. You can use an existing SMTP server; you do not need an SMTP server dedicated for iPlanet Instant Messaging Server use.
- **(Optional) User Provisioning Tool** - Subscriber provisioning can be accomplished with LDAP command-line tools or through iPlanet Delegated Administrator, if you are using an external LDAP directory. All iPlanet Instant Messaging Server preferences are accessible with the iPlanet Instant Messenger. As such. the use and deployment of iDA is optional.

NOTE Use of the iPlanet Delegated Administrator is only recommended if you already use iPlanet Messaging Server and iPlanet Delegated Administrator for Messaging and Collaboration. Installing it just to provision iIM would generate too much overhead to justify its use.

Client Software Dependencies

iPlanet Instant Messenger depends on the following software (see the *iPlanet Portal Server: Instant Collaboration Pack Release Notes* for more information on supported software and versions):

- Java Runtime Environment
- Java Web Start or Java Plug-in

This software is not included with the iPlanet Instant Messaging Server software. Download this software from the Java Web Start web site and install it on each client running the iPlanet Instant Messenger client. Table 1 on page 8 shows the client software dependencies.

Table 1 Client Software Dependencies

Client Operating System	Client Software Options
Solaris (2.6 or 8)	You must use Java Web Start, Java Plug-in is not an option. Download both the JRE for Solaris and Java Web Start.
Windows 98, NT, or 2000	• If you download the JRE for Windows, it includes the Java Plug-in, so you don't need to download and install it separately. • If you download Java Web Start, the JRE is bundled and you don't need to download and install it separately.

See the *iPlanet Portal Server: Instant Collaboration Pack Installation Guide* for information on obtaining and installing Java Runtime Environment, Java Web Start, and Java Plug-in software.

The Java Web Start web site for downloads is:

`http://java.sun.com/products/javawebstart/index.html`

NOTE After downloading the Java software from the Java Web Start web site, consider setting up your own internal web site to stage this software. You can customize your own web pages based on the `index.html`, `solaris.htm`, and `windows.htm` files supplied with iPlanet Instant Messaging Server. See the *iPlanet Portal Server: Instant Collaboration Pack Administrator's Guide* for instructions on customizing these files.

Creating an internal web site prevents your users from having to go to the Internet to obtain this software, avoiding potential download delays and forcing individual users to register for the software. It also enables you to better control your client configurations. For example, if you want your users to use Java Web Start and not Java Plug-in, you configure your internal web site for the Java Web Start software only.

Planning Your Server Configuration

This section provides the namespace and LDAP server information you need to plan your configuration.

Namespace Management

A namespace is defined by a node in the directory under which all uids are unique. With the namespace you must be able to associate an instant messaging domain name. iPlanet Instant Messaging Server has the following namespace requirements:

- iPlanet Instant Messaging Server supports one namespace per iIM server.

  iPlanet Instant Messaging Server does not support multiple name spaces per single server. In addition, in a domain hosting environment, a given iPlanet Instant Messaging server instance cannot serve more than one domain, unless uids are unique across the entire site.

- iPlanet Instant Messaging Server supports one iIM server per namespace.

  To enable users in different domains to communicate, you need to enable server-to-server communication. See the *iPlanet Portal Server: Instant Collaboration Pack Administrator's Guide* for instructions on setting up server-to-server communications.

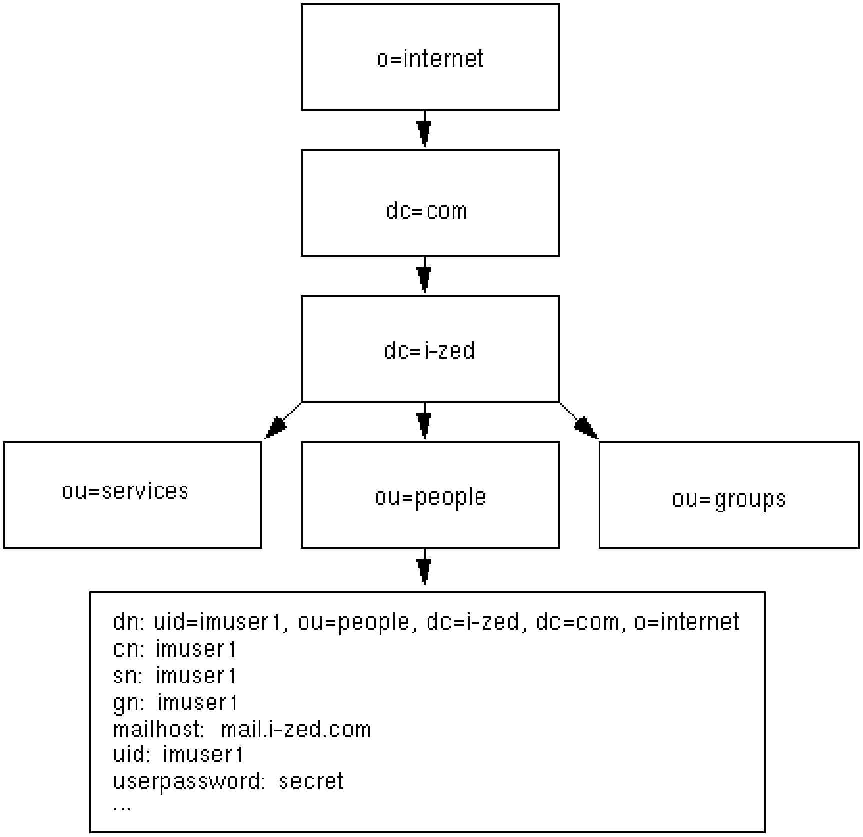
Directory Information Tree Examples

Use the following DIT examples to help determine how to deploy iPlanet Instant Messaging Server at your site.

DIT Example 1—Unique UIDs Across the DIT

Figure 1 on page 10 shows a DIT in which uids are unique across the tree.

Figure 1 DIT Example 1—Unique UIDs Across the DIT



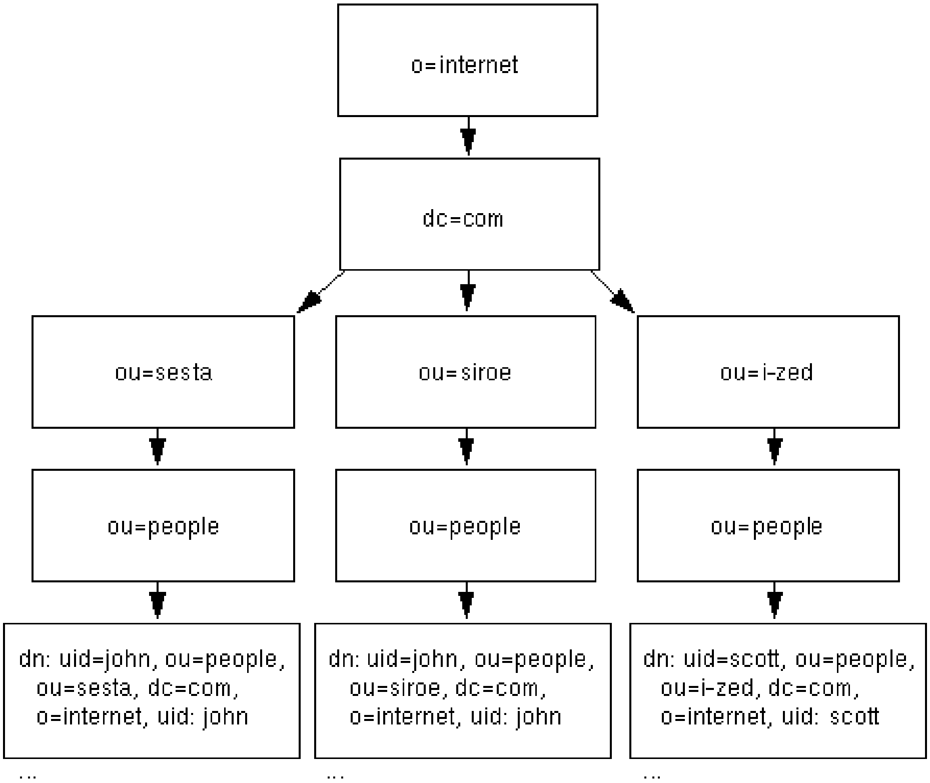
For this kind of tree structure, you would deploy a single iPlanet Instant Messaging Server server and make the base DN in the `iim.conf` file the following entry:

```
dc=i-zed, dc=com, o=internet
```

DIT Example 2—UIDs Unique Across Multiple Organizations

Figure 2 shows a DIT in which UIDs are unique for each organization (ou container).

Figure 2 DIT Example 2—UIDs Unique Across Multiple Organizations


o=internet
dc=com
ou=sesta
ou=siroe
ou=i-zed
ou=people
ou=people
ou=people
dn: uid=john, ou=people, ou=sesta, dc=com, o=internet, uid: john
dn: uid=john, ou=people, ou=siroe, dc=com, o=internet, uid: john
dn: uid=scott, ou=people, ou=i-zed, dc=com, o=internet, uid: scott
...
...
...

For this kind of tree structure, deploy one iPlanet Instant Messaging Server server for each logical subtree and use the following base DN entries:

- `Server 1: ou=sales, dc=i-zed, dc=com, o=internet`
- `Server 2: ou=engineer, dc=i-zed, dc=com, o=internet`

- `Server 3: ou=marketing, dc=isp, dc=com, o=internet`

NOTE These base DNs would also enable iPlanet Instant Messaging server to search LDAP groups, which appear at the same node in the DIT as the `people` containers. For simplicity's sake, Figure 2 on page 11 does not show any `group` containers.

When deploying multiple iIM servers in this example, pay attention to the following:

- You need to install three hosts each with its own iPlanet Instant Messaging server process. When running multiple hosts, users must be informed how to connect to the proper multiplexor. You accomplish this by installing a specific client component for each server instance. Therefore, the proper multiplexor host name that the client connects to gets filled in the appropriate launch file (`iim.html`, or `iim.jnlp/iimres.jnlp`). You can install a single client component, but then you need to edit the appropriate launch files to point users to the proper multiplexor. See the *iPlanet Portal Server: Instant Collaboration Pack Administrator's Guide* for more information on customizing these files.
- iPlanet Instant Messenger distinguishes users in different instant messaging domains by appending the instant messaging domain name to the user name, for example, `john@sales`, `scott@marketing`, and so on. In iPlanet Instant Messenger, when you place your cursor over a userID, a tooltip message appears, displaying the user's status. If the user is on a server (domain) different than yours, the tooltip displays the userID in the form *userID@domain*.

NOTE To see and communicate with users in instant messaging domains on different servers, you need to configure iPlanet Instant Messaging Server for server-to-server communication. See the *iPlanet Portal Server: Instant Collaboration Pack Administrator's Guide* for more information.

Directory Server and Provisioning iPlanet Instant Messenger Users

iPlanet Instant Messaging Server itself does not store iIM user provisioning information, but does store data such as user preferences. The user ID information is maintained in a directory that you specify during the installation process.

iPlanet Instant Messaging Server does not provide user administration tools. If you choose, you can install iPlanet Delegated Administrator for Messaging to perform that role, or use the site provisioning tools for your directory server.

There are no iPlanet Instant Messaging Server specific commands to add, modify, or delete an iPlanet Instant Messenger user. Because users exist in the directory, use your site provisioning tools to perform these operations.

Likewise, you cannot disable an iPlanet Instant Messenger user. The only way to prevent users from using iPlanet Instant Messaging Server is to delete them from the directory.

How iPlanet Instant Messenger Uses the Directory Server

iPlanet Instant Messenger uses the directory server for user authentication and/or user search depending on the following configurations:

- **External LDAP** - If you use an external LDAP directory server—either in standalone mode or portal mode—the uids contained in the directory become user IDs for iPlanet Instant Messenger users. Additionally, iPlanet Instant Messenger performs user searches with that directory. In portal mode, iPlanet Instant Messaging users can also log on directly to the iPlanet Instant Messaging Server without first starting a session with iPlanet Portal Server.
- **Internal directory** - If you use iPlanet Portal Server’s internal directory (portal mode only), iPlanet Instant Messenger does not authenticate the user IDs in the directory, it just performs user searches with the directory. (iPlanet Portal Server itself performs the authentication based on whatever portal authentication mechanism is used.) When configured to use the internal directory, iPlanet Instant Messaging users must first establish a session with iPlanet Portal Server to use iPlanet Instant Messaging. Users cannot log on to iIM in standalone mode.

iPlanet Portal Server Namespace Implications

When you install iPlanet Instant Messaging Server in portal mode, either iPlanet Portal Server itself, or an external LDAP directory, can manage the user namespace. This has deployment implications.

First Case: External LDAP Directory

While iPlanet Portal Server Profile Service maintains information about each user in the domain, you create and remove users by adding and removing entries in the external LDAP directory.

In addition, the external LDAP directory might physically maintain some portal attributes. You can use the iPlanet Portal Server Administration Console to map attributes between portal attribute names and LDAP user attribute names using the External LDAP configuration.

In this scenario, the installer automatically creates an attribute mapping between the portal user attribute `iwtUser-iIMUserId` and the LDAP user attribute `uid`. iPlanet Instant Messaging server uses the external LDAP uids as user IDs, and uses the external LDAP directory to search for users. This means that when configured for external LDAP, iPlanet Instant Messaging users can log on directly to the iPlanet Instant Messaging Server (standalone mode) without first starting a session with iPlanet Portal Server.

Second Case: Namespace Maintained by iPlanet Portal Server Only

In this scenario, iPlanet Instant Messaging server uses iPlanet Portal Server Profile Service's internal LDAP store for user search. iPlanet Instant Messaging server performs no authentication, thus it does not support standalone mode. Users must have an active iPlanet Portal Server session to be able to use iPlanet Instant Messaging server. In this scenario, the installer does not create any attribute mapping.

Logical Domain vs. DNS Domain

An important distinction needs to be made between the iPlanet Instant Messaging Server domain (instant messaging domain) and the DNS domain, as they are not equivalent. The instant messaging domain name is the *logical* domain name you want the iPlanet Instant Messaging server to support. This is the name that is used by other iPlanet Instant Messaging servers in the network to identify this server (the name tagged to users on this server when displayed to users on other server). It is also the name used by this server to identify its users to other servers. This is not necessarily the FQDN (fully qualified domain name) of the system running the iPlanet Instant Messaging server.

During installation, the installer prompts you to enter the iPlanet Instant Messaging Server domain name, which is stored in the `iim.conf` file as the `iim_server.domainname` parameter. This name can, and probably should be, different than the underlying DNS domain name. For example, if your DNS domain is `www.i-zed.com`, rather than use the same name for the instant messaging domain, consider using something such as `iim.i-zed.com`. This could help alleviate confusion that the iPlanet Instant Messenger ID is not an email address.

The result of this is that an iPlanet Instant Messenger user ID, *user@domain*, which looks like an email address, is in fact not an email address. In some cases the iPlanet Instant Messenger user ID might map to an email address, but not necessarily. Thus, users might have a user ID such as `johndoe@i-zed.com` and an iPlanet Instant Messenger ID of `johndoe@iim.i-zed.com` (the ID displayed by the tooltip in the iPlanet Instant Messenger client).

In addition, if you install multiple iPlanet Instant Messaging servers, hence multiple instant messaging logical domains, users need to know about these domains to search for and locate appropriate contacts. Users can use the Domain to search on pull-down menu in the various iPlanet Instant Messenger windows to search other domains they are configured to access.

NOTE In the future, the product might be redesigned to use DNS. At such point in time, the logical instant messaging domain name would no longer apply and you would want to use the DNS name.

Searching the Directory and Anonymous Bind

iPlanet Instant Messaging Server needs to be able to search the directory to function correctly. If your directory is configured to be searchable by anonymous users, iPlanet Instant Messaging Server has the capability it needs. If the directory is not readable by anonymous users, you must take additional steps to configure the `iim.conf` file with the credentials of a user ID that has at least read access to the directory.

These credentials consist of:

- A distinguished name (`dn`)
- The password of the above `dn`

Thus, you need to modify the `iim.conf` file if either one of the following conditions exists:

- The external LDAP directory server does not allow anonymous bind.
- You are using iPlanet Portal Server's internal directory, because the internal directory server in general does not allow anonymous bind.

See the *iPlanet Instant Messaging Server Administrator's Guide* for the steps to configure a specific user to search your directory.

LDAP Issues

The following LDAP issues might arise in a given deployment. Change the LDAP parameters in the `iim.conf` file accordingly.

Issue: Your directory does not permit anonymous bind. By default, iPlanet Instant Messaging server performs an anonymous search of the LDAP directory. However, it is common for sites to prevent anonymous searches in their directory so that any random person cannot do a search and retrieve all the information.

Solution: If your site's directory is configured to prevent such anonymous searches, the iPlanet Instant Messaging server needs to have a user ID and password it can use to bind and do searches. Use the `iim_ldap.usergroupbinddn` and `iim_ldap.usergroupbindcred` parameters to configure the necessary credentials. See the *iPlanet Instant Messaging Server Administrator's Guide* for more details.

Issue: Your site does not use the `uid` attribute for user authentication.

Solution: Use the `iim_ldap.loginfilter` parameter to set the attribute that is used by your directory for authentication. By default, this parameter is set to `uid`. Also, change any "filter" parameters that contains `uid` in its value.

Issue: You want to change how iPlanet Instant Messenger displays contact names from the default.

Solution: The default attribute that iPlanet Instant Messenger uses to display contact names is `cn`. Thus, contact names appear as Frank Smith, Mary Jones, and so on. Edit the `iim_ldap.userdisplay` and `iim_ldap.groupdisplay` parameters to a different attribute, such as `uid`.

Issue: Your directory is indexed to use wildcards.

Solution: Change the `iim_ldap.allowwildcardinuid` parameter to `True`. This parameter determines if the use of wildcards should be enabled for uids while doing a search. As most directory installations have uids indexed for exact searches only, the default value is `False`. Setting this value to `True` can impact performance unless uids are indexed for substring search.

Issue: Your directory uses non-standard object/group classes.

Solution: Change the appropriate `iim_ldap.*` parameters, replacing `inetorgperson` and `groupofuniquenames` with your values.

Issue: Your directory does not use the `mail` attribute for email addresses. If so, iPlanet Instant Messenger will not be able to forward instant messages to offline users as email messages.

Solution: By default, the `iim_ldap.user.mailattr` contains the value `mail`. Change this value to your site's value.

Indexed LDAP Attributes

Index the attributes below as indicated for adequate directory performance when used with iPlanet Instant Messaging Server. If you use iPlanet Delegated Administrator for Messaging, the following lines should appear in the `slapd.ldbm.conf` file.

```
index   cn pres,eq,sub

index   sn pres,eq,sub

index   givenName pres,eq,sub

index   uid eq

index   uniquemember eq
```

If you site permits substring search on `uid`, the index list for `uid` should be:

```
index   uid eq,sub
```

Planning Your Client Configuration

This section describes potential problems and solutions when installing and configuring the iPlanet Instant Messenger client software to work with a web server. It also describes issues associated with running the client with iPlanet Portal Server. See the *iPlanet Portal Server: Instant Collaboration Pack Release Notes* for information on supported web server software.

Web Server Overview

When installing iPlanet Instant Messaging Server with iPlanet Portal Server, you must use the iPlanet Portal Server's web server. When installing iPlanet Instant Messaging Server in a standalone deployment, you supply the web server.

iPlanet Instant Messaging Server depends on a web server to serve up HTML, including:

- An initial `index.html` file, provided by the product, or your own home page, with a link to invoke the iPlanet Instant Messenger. (This applies only to a standalone deployment.)
- The product's client jar files (`iim.jar`, `iimres.jar`, `iimnet.jar`, and `iimjni.jar`).
- The iPlanet Instant Messenger online help.
- Embedded URLs in messages and news channels, to iPlanet Instant Messenger.

Web Server Issue for Both Portal and Standalone Deployments

Location of iPlanet Instant Messenger Software and Web Server

Issue: You must install the iPlanet Instant Messenger client software on the host where the web server is installed. In a portal deployment, this will be the iPlanet Portal Server host (the iPlanet Portal Server's web server).

For standalone installations, some sites might include the web server on the iPlanet Instant Messaging server host, in which case there is no issue. However, if the web server is not on the iPlanet Instant Messaging server host, you will need to install the iPlanet Instant Messenger client software separately on the web server host.

Solution: Run the iPlanet Instant Messaging Server installer, after installing the iPlanet Instant Messaging server software, and install just the client files (the iPlanet Instant Messenger component) on the web server host. See the *iPlanet Portal Server: Instant Collaboration Pack Installation Guide* for more information.

Web Server Issues for Standalone Deployments Only

This section contains web server deployment issues for standalone deployments only.

iPlanet Instant Messenger Software Not Located in Web Server Document Root

Issue: By default, iPlanet Instant Messaging Server expects to find the iPlanet Instant Messenger software installed in the web server document root. However, you might choose to install the iPlanet Instant Messenger software files in a directory other than the web server document root.

Solution: You need to edit iPlanet Instant Messenger's `.html` and `.jnlp` files if iPlanet Instant Messenger software is not located in the web server's document root.

Edit the following files:

- **index.html, iim.html, and iim.jnlp** - The URL that users type in for the `index.html`, `iim.html`, and `iim.jnlp` files needs to reference the iPlanet Instant Messenger installation directory. You either have to configure the web server to enable access to the directory where you installed the iPlanet Instant Messenger files, or create a symbolic link in the web server's document root.

  For example, on iIM Server host `iim.i-zed.com`, if the iPlanet Instant Messenger software is installed in the `/opt/SUNWiim/html` directory, you could create a symbolic link `iim`, which points to `/opt/SUNWiim/html`, in the web server's document root. Users would then type the following URL to access the iPlanet Instant Messenger main page (`index.html`):

  ```
  http://iim.i-zed.com/iim/
  ```

NOTE	By using a symbolic link, you do not need to change the web server's configuration.

- **iim.jnlp, iimres.jnlp, iim.html, iimssl.jnlp, and iimssl.html**- These files have a `codebase` parameter that needs to be changed to reference the web server and path to the iPlanet Instant Messenger software. The line to change is:

  `codebase="http://`*servername*`:`*port*`/`*path*`/"`

You only need to include the port number of the web server if it is not using the default (80).

For example, on iPlanet Instant Messaging server host `iim.i-zed.com`, if the iPlanet Instant Messenger software is installed in the `/opt/SUNWiim/html` directory, you could create a symbolic link `iim`, which points to `/opt/SUNWiim/html`, in the web server's document root. Then you would change the `codebase` parameters in the `iim.jnlp` and `iimres.jnlp` files:

```
codebase="http://iim.i-zed.com/iim/"
```

NOTE The `iim.jnlp` and `iimres.jnlp` files are used for Java Web Start configurations. If you are only using Java Plugin, you do not need to edit these files as they will not be used.

The `iimssl.jnlp` and `iimssl.html` files are used only for SSL. You will not have to edit these files unless you are using SSL.

Web Server Installed on a Port Other than Default (80)

Issue: Your web server might be installed on a port other than the default (80).

Solution: You need to edit the `iim.jnlp` and `iimres.jnlp` files and change the `codebase` parameter to:

`codebase="http://`*webserver*`:`*webserverport*`"`

For example, on iPlanet Instant Messaging server host `iim.i-zed`, if the web server is running on port 8080, `codebase` parameters in the `iim.jnlp` and `iimres.jnlp` files would become:

```
codebase="http://iim.i-zed.com:8080"
```

Launching Java Web Start and MIME Types

Issue: To run iPlanet Instant Messenger using Java Web Start, you might need to edit the web server's MIME types file to include a line for JNLP.

Solution: For iPlanet Web Server, the default location for this file is:

`/usr/netscape/server4/https-`*xxx*`/config/mime.types`

where *xxx* is your web server instance name.

If not already present, add the following line:

```
type=application/x-java-jnlp-file   exts=jnlp
```

For this change to take effect, you must restart the `http-`*xxx* server.

Solution: For Apache Web Server, the `mime.types` file, located in the Apache Web Server configuration directory (its location is site-specific), should be edited to include the line:

```
application/x-java-jnlp-file    jnlp
```

iPlanet Portal Server Issues

This section describes iPlanet Portal Server specific issues with regards to iPlanet Instant Messenger.

Application Channel Links

When installing iPlanet Instant Messaging Server in the iPlanet Portal Server environment, the installer inserts the following three links in the Applications channel of the iPlanet Portal Server Desktop:

- iPlanet™ Portal Server: Instant Messenger Quick Reference (Displays the iPlanet Instant Messaging Server Quick Reference in a new web browser window)
- Launch iPlanet™ Instant Messenger using Java plug-in (Starts iPlanet Instant Messenger using the Java Plug-in)
- Launch iPlanet™ Instant Messenger using Java Web Start (Starts iPlanet Instant Messenger using Java Web Start)

These links are displayed to users in their iPlanet Portal Server Desktop Applications channel only if they have not customized the `iwtAppProvider` component. If users do not automatically receive the iPlanet Instant Messenger links, then they must add them manually from the available Applications channel.

To Manually Add Applications to the Applications Channel

1. Click Edit on the Applications toolbar.
2. Select the iPlanet Instant Messenger applications you want displayed in the Applications channel.
3. Click Finished to return to the Portal Server Desktop page.

Secure Mode vs. Non-Secure Mode

When you install iPlanet Instant Messaging Server in the iPlanet Portal Server environment, users invoke the iPlanet Instant Messenger client from their iPlanet Portal Server Desktop Applications channel. In the iPlanet Portal Server environment, you configure iPlanet Instant Messenger in either secure or non-secure mode. In secure mode, communication is encrypted through the iPlanet Portal Server Netlet (SRAP gateway). A lock icon appears in iPlanet Instant Messenger's Status area when you are running in secure mode. See the iPlanet Portal Server documentation for more information on Netlet at:

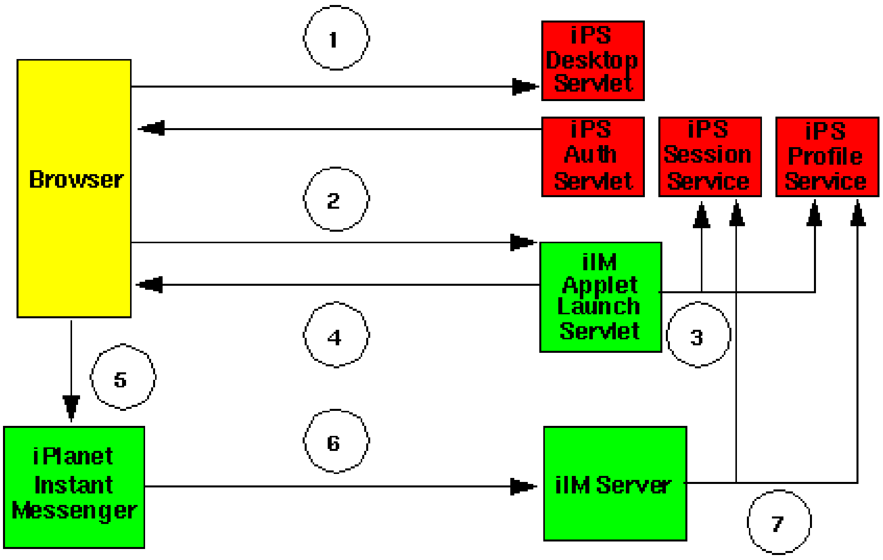
```
http://docs.iplanet.com/docs/manuals/portal/30/ag/netlet.htm#17676
```

In non-secure mode, no encryption takes place between iPlanet Portal Server and the user's machine.

Launching iPlanet Instant Messenger in iPlanet Portal Server Overview

Figure 3 on page 22 shows how iPlanet Instant Messenger functions in the iPlanet Portal Server Single Sign-on (SSO) environment.

Figure 3 iPlanet Instant Messenger Single Sign-on in iPlanet Portal Server



The following describes the above figure:

1. User logs on to the iPlanet Portal Server Desktop. iPlanet Portal Server sets a Single Sign-on (SSO) cookie.
2. User clicks on the Launch iPlanet Instant Messenger link in the Applications Channel.

NOTE If the iPlanet Instant Messenger log on fails, a “logon failed” dialog appears. The user would need to click the Launch iPlanet Instant Messenger link again.

3. The iPlanet Instant Messenger launch servlet validates the user’s session ID and gets the user profile, provided by the iPlanet Portal Server Session Service and Profile Service.
4. The launch servlet returns the iPlanet Instant Messenger applet launch page, which contains the iPlanet Portal Server SSO token as parameter.
5. The iPlanet Instant Messenger applet is launched.
6. iPlanet Instant Messenger talks to iIM Server, passing the SSO token.
7. iIM Server validates the SSO token with the iPlanet Portal Server services.

Notes on Running iPlanet Instant Messenger with iPlanet Portal Server

Note the following conditions when running iPlanet Instant Messenger in the iPlanet Portal Server environment:

- You can run iPlanet Instant Messenger in secure mode using either Java plug-in and Java Web Start to launch the application. (You can configure iPlanet Instant Messenger for secure mode only if the iPlanet Portal Server gateway is configured.) When running in secure mode, iPlanet Instant Messenger displays a lock icon in the Status area at the top of the Main window.
- Secure mode does not work if users launch iPlanet Instant Messenger from a desktop shortcut. In addition, unlike a standalone deployment, when running in a portal deployment Java Web Start does not give the option of creating a desktop shortcut. However, users can still create bookmarks (for both Java Web Start and Java Plug-in) to launch iPlanet Instant Messenger. (Launching by a shortcut should only be done in standalone mode.)

- Single Sign-on (SSO) is not supported with the iPlanet Portal Server Desktop if users launch iPlanet Instant Messenger from an operating system desktop shortcut.
- Auto-logon - Because SSO is used, the Auto-logon feature for iPlanet Instant Messenger cannot be disabled when running in portal mode.

Planning Your Multiplexor Configuration

This section describes the information you need to plan the iIM multiplexor configuration.

The iPlanet Instant Messaging multiplexor component is a connection multiplexor that listens for iPlanet Instant Messenger clients and opens only one connection to the backend iPlanet Instant Messaging server.

In effect, the multiplexor always acts as a frontend component to the iPlanet Instant Messaging server. Any client-server communication must go through the multiplexor; that is, iIM Server architecture is such that it always uses the multiplexor. iPlanet Instant Messenger and iPlanet Instant Messaging server do not talk to each other directly.

You can install multiple multiplexors as needed, depending your configuration. When using multiple multiplexors, you should consider also installing some sort of load balancer product, such as offered by Resonate.

For more information on multiplexor configuration, see “Tuning and Performance Issues,” on page 29.

NOTE Windows NT only supports one multiplexor process per machine. Solaris supports multiple multiplexors per machine.

Planning Security

This section describes the information you need to plan for iPlanet Instant Messenger security, including:

- Access control
- Server-to-server communications
- Secure Sockets Layer (SSL)

- SRAP Gateway and Netlet
- Accessing iPlanet Instant Messenger outside a firewall

Planning Privileges: Access Control

Almost all features of iPlanet Instant Messenger are controlled by a privilege system that limits what a user can see or do. Before deploying iIM Server, determine the privileges you want your users to have from the following list:

- **Administrator privileges** - Enables a user to control all aspects of the system, so should be restricted to the few administrator accounts.
- **Privilege to change client user settings** - Most likely you'll want to permit users to set and save their own preferences. However, for sites that want to standardize on user settings, you can deny this privilege and lock out users from making any preference changes.
- **Privilege to add and delete news channels** - Enables a user to create and delete news channels from iIM Server.
- **Privilege to add and delete conference rooms** - Enables a user to create and delete conference rooms from iIM Server.
- **Privilege to send and forward alerts** - Enables a user to create and send alert messages.
- **Privilege to set up watches on other users** - Enables a user to monitor the status of other users and receive an alert when the status changes.

You set or change user privileges by editing the appropriate ACL file. See *iPlanet Portal Server: Instant Collaboration Pack Administrator's Guide* for more information on how to set privileges for the system.

You cannot disable an iPlanet Instant Messenger user. Because iPlanet Instant Messaging Server authenticates uses the directory for authentication, any existing user has can access to iPlanet Instant Messenger. The only way to prevent users from using iPlanet Instant Messaging Server is to delete them from the directory.

NOTE If you deny users the privilege to set up watches on other users —by editing the `sysWatch.acl` file—they will not be able to display iPlanet Instant Messenger's Main window, effectively denying them the ability to send instant messages. However, users would still be able to see alerts and news channels.

Planning Server-to-Server Communication

You can configure multiple iPlanet Instant Messaging servers to communicate and form a larger instant messaging community. Users on each server can communicate with users on every other server, use conferences rooms on other servers, and subscribe to news channels on other servers (subject to access privileges).

For communication between multiple iPlanet Instant Messaging servers in your network, you need to configure server-to-server communication. When configuring server-to-server communication, you identify your server to the other servers, and identify each *coserver*, or cooperating server, which will have a connection to your server.

When you configure your server to talk to another server, each server is notified of all activities, such as login, watch, conference room creation, etc., which happen on its coservers. This means you must trust all of your coservers with activities happening on your system.

You establish server-to-server communication by editing the appropriate parameters in the `iim.conf` file on each server. See *iPlanet Portal Server: Instant Collaboration Pack Administrator's Guide* for more information on how to configure server-to-server communication.

NOTE You can configure a standalone installation of iIM Server to user server-to-server communication with a portal installation.

Planning Secure Sockets Layer (SSL) For Server to Server Communications

The high-level steps to configure SSL for server to server communications in iPlanet Instant Messaging Server are:

1. Generating a self-signed certificate.
2. Generating a Certificate Signing Request.
3. Sending a Certificate Signing Request to a Certificate Authority (CA) and getting back a signed certificate.
4. Installing the Certificate on the iIM server, and the CA's certificate on other servers; which means you also have to install the other server's CA certificate on your system. (This is much easier when you have the same CA.)

5. Activating SSL

When enabling SSL for use with iPlanet Instant Messaging Server, choose one of the following methods:

- **Using a self-signed certificate** - Put your self-signed certificate in the `iimkeys` file (on Solaris, *im30_install_dir*`/config/iimkeys`; on Windows NT, *im30_install_dir*`\config\iimkeys`)and also export it to other iPlanet Instant Messaging servers so they can put it in their `nlcacerts` file.
- **Using a certificate signed by a CA that is not already in `cacerts`** - Put your certificate and your signing CA's certificate in the `iimkeys` file (on Solaris, *im30_install_dir*`/config/iimkeys`; on Windows NT, *im30_install_dir*`\config\iimkeys`). Also, export your signing CA's certificate to the other servers so they can put it in their `nlcacerts` file.
- **Using a certificate signed by a CA already in `cacerts`** - Put your certificate in the `iimkeys` file only (on Solaris, *im30_install_dir*`/config/iimkeys`; on Windows NT, *im30_install_dir*`\config\iimkeys`), and the other servers already have your signing CA in their `cacerts` file.

NOTE You can run the following command to show all the CAs in your `cacerts` file:

Javahome`/keytool -list -keystore cacerts`

Run this command from the directory that contains the `cacerts` file. Press Return when prompted for password.

In all cases, remember that your iPlanet Instant Messaging server is the "client" of the other server, so you might have to import the CA's certificate for that server.

Other Considerations

The following information is useful if you are going to use SSL:

- The size of the client component increases when you add SSL.
- Use `iimssl.jnlp` for implementing SSL.
- To support both SSL and non-SSL modes, you need to set up two separate multiplexors.

Planning SRAP Gateway and Netlet

iPlanet Portal Server: Instant Collaboration Pack enables users to communicate securely and reliably. It can take advantage of the Netlet technology offered by the iPlanet Portal Server: Secure Remote Access Pack (SRAP) enabling instant messaging to occur over a secure virtual private network (VPN). In the iPlanet Portal Server environment, you configure iPlanet Instant Messenger in either secure or open mode. In secure mode, communication is encrypted through the iPlanet Portal Server Netlet. In open mode, iPlanet Instant Messenger communication is not encrypted.

When installing iPlanet Portal Server: Instant Collaboration Pack in portal mode, you are asked if you want to run iPlanet Instant Messenger in secure or open mode. When you choose during installation to run in secure mode, the installer configures the appropriate Netlet rules for encrypted communications. If you do not choose to run in secure mode, but later want to, you can run the `iimipsadmin` script to configure the Netlet rules.

Planning for Accessing iPlanet Instant Messenger Outside a Firewall

There are two modes to choose from: portal mode, and standalone mode.

Portal Mode

In this mode, the iPlanet Instant Messaging client and iPlanet Portal Server:SRAP (gateway) are outside the firewall and the iPlanet Portal Server, the iPlanet Instant Messaging multiplexor, and the iPlanet Instant Messaging server are inside the firewall. Note that the connection between the multiplexor and iIM server is not encrypted; they should both be inside of the firewall.

The SRAP gateway can be configured to run in either secure or non-secure modes. In non-secure mode, the communication between client, gateway, firewall, and the other components is clear, without encryption.

In secure mode, the individual components communicate via VPN, which provides secure connections by encrypting lower protocol layers in an otherwise non-secure network, such as the internet.

Standalone Mode

In standalone mode, SSL is used to ensure link security between the iIM client, and an iIM multiplexor and server combination on either side of the firewall. This solution may still not provide adequate security since there is an iIM server on the outside of the firewall.

An alternative to this is to have the iIM client outside the firewall, while the iIM multiplexor and server reside only inside the firewall. With this alternative, the firewall is opened only for the SSL port to the iIM multiplexor.

Tuning and Performance Issues

This section describes the information you need to consider for tuning and performance of your iPlanet Instant Messaging system.

Tuning Server Memory

Server memory size can be set using the following `iim.conf` parameter: `iim.jvm.maxmemorysize.` This parameter specifies the maximum number of megabytes of memory that the JVM running the server is allowed to use. The default setting is 256 MB.

This parameter is used to construct the `-mx` argument of the java command. For example, if `iim.jvm.maxmemorysize = 500`, the JVM will be allowed to use up to 500 MB.

On NT, you cannot currently change this value.

Tuning the Multiplexor

A multiplexor consists of one or more multiplexor processes. There are three parameters (found in the `iim.conf` file) used for tuning multiplexor performance:

- `iim_mux.numinstances` - Specifies the number of multiplexor processes.
- `iim_mux.maxsessions` - Specifies the maximum number of clients that one mutliplexor process can handle. The default is 1000.
- `iim_mux.maxthreads` - Specifes the maximum number of threads per multiplexor process. The default is 5.

Figuring Maximum Number of Concurrent Client Connections

To figure the maximum number of concurrent client connections possible, multiply the `numinstances` number by the `maxsessions` number.

Multiplexor Configuration Rules of Thumb

The following suggestions and generalizations might be useful for your planning:

- The number of `iim_mux.maxthreads` should not exceed the number of CPUs on your server.

  This helps maximize resource utilization and optimizes processing speed.
- The `iim_mux.maxsessions` should be high enough to avoid rejecting connections, but it should be reasonable enough so that the multiplexor processes to not get overloaded.
- Be sure that your expected number of concurrent client connections is less than the maximum possible by a safe margin.
- However, do not configure more threads or maximum number of concurrent sessions than you need. Otherwise, you will unnecessarily consume system resources.
- A good starting point is to configure `iim_mux.numinstances` to the number of CPUs on the system.

Concurrent Users and Resource Requirements

Correctly formulating the maximum number of concurrent users that has to be sustained by the system is key to planning your resource requirements. A deployment will have a maximum number of configured users, but the more important planning value is the maximum number of concurrent users (connected and more or less active). A conservative estimate for the number of concurrent users can then be determined based on a 1:10 ratio. Thus, for a deployment of 50,000 configured users, the concurrent users would be 5,000.

Use the following procedure to generate a more precise picture of your resource requirements:

1. Characterize your configured users using three general profiles:
   - Not Connected - Non-connected users consume disk space but no CPU or memory.

- Connected/Inactive - Typical usage consists of having the client up and running and receiving a small amount of presence notification per day. Users rarely use the chat rooms.
- Connected/Active - Typical usage consists of the following:
    - Presence updates equal to or greater than 20 times a day.
    - Contact list contains about 30 contacts.
    - Users subscribe to the presence updates of all the contacts in the contact list.
    - Users set up around 4 conferences/chats per day.
    - Each conference has 3 people in the conference rooms and lasts 10 minutes.
    - A message is added to the conference every 1 -15 seconds.

2. Determine the mix of profiles your system needs to accommodate.

    Divide all of your configured users into these groups.

3. Use Table 2 to determine Server and Multiplexor sizing numbers.

Table 2 Server and Multiplexor Sizing for Concurrent Users *

Server Memory Consumption for Connected/Inactive Users	Server Memory Consumption for Connected/Active Users	Multiplexor Memory Consumption for Connected/Inactive Users	Multiplexor Memory Consumption for Connected/Active Users
100 MB +10 K per User	200 MB + 16 K per User	5 MB + 15 K per User	5MB + 20 K per User
*** Figures generated using a 400MHz UltraSparc II processor.**			

Use Table 3 to help determine the number of CPUs your installation requires for optimum performance.

Table 3 CPU Utilization Numbers*

Server CPU Utilization for Connected/Inactive Users	Server CPU Utilization for Connected/Active Users	Multiplexor CPU Utilization for Connected/Inactive Users	Multiplexor CPU Utilization for Connected/Active Users
Several hundred thousand users per CPU	30 K users per CPU	50 K users per CPU	5 K users per CPU
*** Figures generated using a 400MHz UltraSparc II processor.**			

4. Add a safety buffer of extra capacity.

Small Deployment Sample Resource Requirements Numbers

For a small deployment with the server and multiplexor on a single server having 10,000 users with the following profile:

- 30% connected/active
- 20% connected/inactive
- 50% not connected

The memory requirements are: 1/2 CPU with 300-500 MB RAM.

Large Deployment Sample Resource Requirements Numbers

For a large deployment having 1,000,000 users with the following profile:

- 5% connected/active
- 20% connected/inactive
- 75% not connected

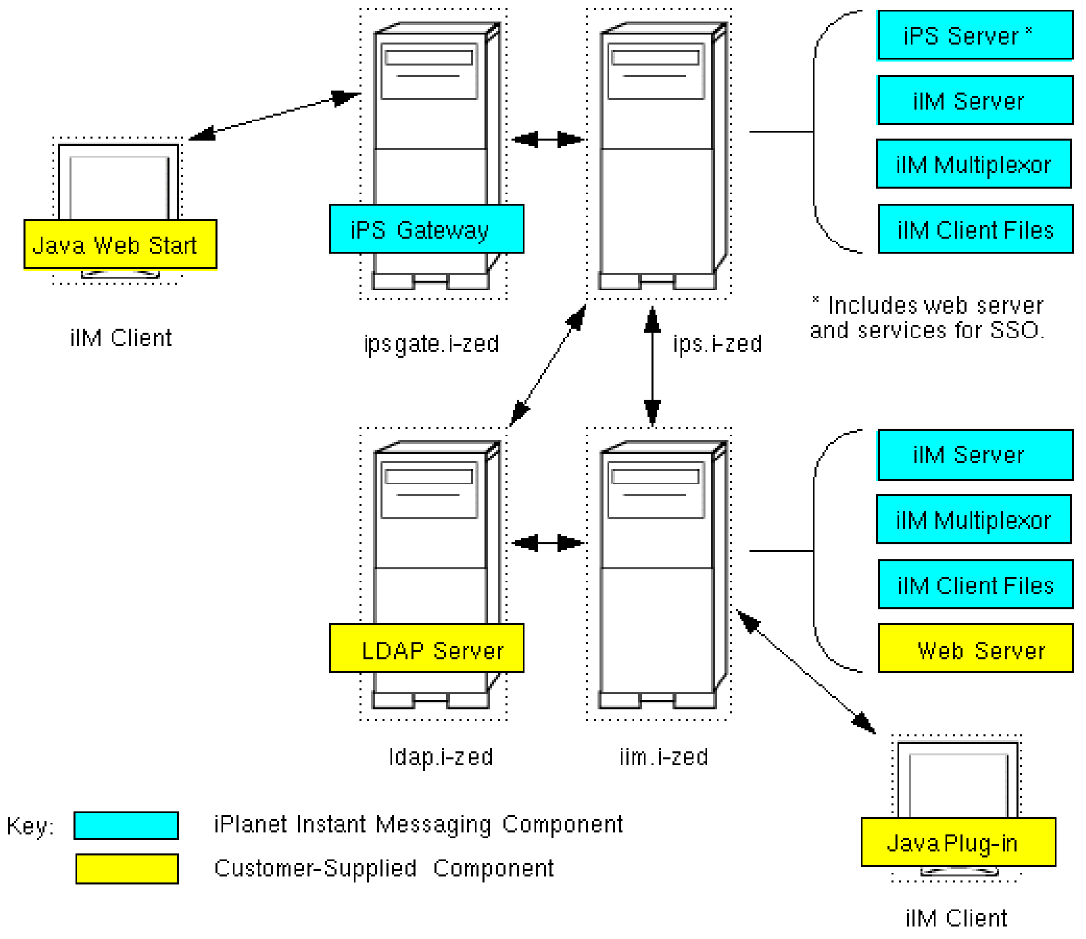
The server memory requirements are 4 GB RAM on 2 CPUs. The multiplexor requirement is 4 GB RAM on 16 CPUs.

NOTE You need to use a provisioning tool to create the profile information on the backend server (LDAP) for each new user.

iPlanet Instant Messaging Server Deployment Example

Figure 4 on page 33 shows a sample deployment, including two iPlanet Instant Messaging servers (one in portal mode and one in standalone mode), and the required software components.

Figure 4 Sample iPlanet Instant Messaging Server Deployment



Software Components Description

Table 4 on page 34 describes the software components deployed on each host.

Table 4 Sample Deployment—Software Components for Hosts

ipsgate.i-zed	ips.i-zed	ldap.i-zed	iim.i-zed
SRAP gateway host: • iPlanet Portal Server: Secure Remote Access Pack	iPlanet Portal Server host: • iPlanet Portal Server (includes web server and services for Single Sign-on) • iIM Server component • iIM Multiplexor component • iIM Client Files component	External LDAP directory host for `iim.i-zed` users. • iPlanet Directory Server	Standalone iPlanet Instant Messaging server host: • iIM Server component • iIM Multiplexor component • iIM Client Files component • iPlanet Web Server

Client Files

Table 5 on page 34 shows the client files that are needed for the two iim hosts.

Table 5 Sample Deployment—Required Client Files

Client File	Used by ips.i-zed?	Used by iim.i-zed?
`index.html`	No. Not necessary for portal deployment.	Yes. Location: ips.i-zed/icp/index.html
`iim.html`	No, as this host's clients are only using Java Web Start.	Yes. Location: ips.i-zed/icp/iim.html
`iim.jnlp`	Yes. Location: ips.i-zed/iim.jnlp	No, as this host's clients are only using Java Plug-in.
`iimres.jnlp`	Yes. Location: ips.i-zed/iimres.jnlp	No, as this host's clients are only using Java Plug-in.

Client Files Content by Server

Each iIM server has its own client component. The `ips.i-zed` host uses Java Web Start, so it has `iim.jnlp`, and `iimres.jnlp` files. The `iim.i-zed` host uses the Java plug-in, so it has `index.html` and `iim.html` files.

In this example, the iIM client component was not installed at the doc root of the web server. It was put in its own `icp` directory. See the *iPlanet Portal Server: Instant Collaboration Pack Installation Guide* for more information on steps to take when the client is not installed at the web server doc root.

How the Sample Deployment Works

From a high-level overview, this sample deployment requires four hosts as follows:

ipsgate.i-zed - Host containing the SRAP gateway.

ips.i-zed - Host containing the iPlanet Portal Server and iPlanet Instant Messaging Server software.

ldap.i-zed - Host containing external LDAP directory server.

iim.i-zed - Host containing iPlanet Instant Messaging Server software, installed in standalone mode.

This sample deployment contains a combination of two iIM server, one in the portal mode, running on `ips.i-zed`, another in standalone mode in `iim.i-zed`. It demonstrates how a company can cooperate with partners to communicate in a controlled and secure manner.

This deployment shows that users can get to the iIM server securely from outside the firewall, using the portal gateway, while at the same time users inside the firewall connect directly to the `iim.i-zed` server.

The outside users can talk with the internal users because the systems, `ips.i-zed` and `iim.i-zed`, are configured for server-to-server communication. If the link between these two systems are within a firewall, they can be connected without using SSL. If the link between them needs to be protected from snooping, the two systems can be set up to communicate using SSL. For simplicity in this example, the outside users are shown using only Java Web Start and the inside users only Java plug-in.

Using the hypothetical case that the outside users are partners of the company I-ZED who need to communicate with people working inside I-ZED, the partners are given access through the secure portal, authenticating themselves as legitimate users. They can then use instant messaging to communicate with users inside I-ZED.

To facilitate secure communications, conference rooms can be set up on ips.i-zed, which allow access by specific partners. For example, you can have a conference room, Nova, which allows only access by users A, B, C, who are partners of I-ZED working on the Nova project. And users X, Y, Z in iim.i-zed who also work on the Nova project are also allowed access. Access to this conference room is private. Non-invited users can't gain access.

The users, A, B, C and X, Y, Z can also watch each other's status so they know when the other goes online or goes away. The users, A, B, C can also subscribe to a news channel called Nova News and the users X, Y, Z can be set up to be able to post to this Nova News channel. Others can be restricted from reading this news channel, so information is limited to only those with specific access.

Users A, B, C can also subscribe to a general access I-ZED News channel, which is accessible to all who have access to the ips.i-zed iIM server. This news channel can contain general news related to I-ZED.

Index