



Insight Server 4.2 Administration Guide

*Copyright © 2005 Bynari Inc.,
All rights reserved.*

*No part of this publication may be reproduced
or transmitted in any form or by any means, electronic
or mechanical, including photocopy, recording, or
any information storage and retrieval system, without
permission in writing from the publisher.*

Trademarks

Bynari Insight products are trademarks of Bynari, Inc.

Microsoft Windows, Outlook and Windows NT logos are trademarks of Microsoft Corporation in the United States, other countries, or both.

All other trademarks are the property of their respective owners.

Technical Support

The Bynari Insight products can be purchased with one of the following technical support options included:

- Without Support – 90 day of free product maintenance and upgrades.
- With Support – 1 year product maintenance, upgrades and unlimited email and telephone support.

Available to customers from anywhere.

To contact technical support

Phone 1-214-350-5772 or email: support@bynari.net

For FAQs: <http://www.bynari.net/faq/>

Table of Contents

<i>Trademarks</i>	6
<i>Technical Support</i>	7
Installation	1
Prerequisites for Insight Server.....	1
RPM Dependencies	2
Port Availability	3
Recovering from conflicting Services	4
New 4.2 Insight Server Installation	5
4.0 to 4.2 Insight Server Upgrade	6
Pre-installation checklist:.....	6
Upgrade from 4.0 to 4.2 on the same hardware server:	6
Upgrade from 4.0 to 4.2 on a new hardware server:.....	6
4.1 to 4.2 Insight Server Upgrade	7
Upgrade from 4.1 to 4.2 on the same hardware server:	7
Upgrade from 4.1 to 4.2 on a new hardware server:.....	8
Insight WebClient 4.2 Installation	8
Administration	9
Accounts	9
Aliases	18
Mail Folders	22
Mail Delivery	25
Configuration	28
Services.....	28
Apache Configuration.....	28
Cyrus IMAP Configuration	31
OpenLDAP Configuration.....	41
Postfix Configuration.....	45
ProFTP Configuration	60
LDAP Replication	68
Distributed Mail.....	70
Tools	73
Migration Wizard	73
Backup & Restore.....	79
Task Scheduler	81
Cyrus Database Recovery.....	83
System	83
Statistics.....	83
Logging.....	86
Registration.....	87
Insight WebClient	88



Insight Server 4.2 Administration Guide

Run WebClient	88
Access Controls	89
Content Filtering	89
AMaViS.....	89
Clam AntiVirus.....	90
SpamAssassin.....	91
SquirrelMail.....	92
Jabber	92
Help Browser	93

Introduction

Insight Server 4.2 offers an enterprise email server that scales from Intel platforms to IBM mainframes, providing world-class reliability for hundreds of thousands of users. Bynari significantly reduces hardware, software, and administrative costs associated with managing email systems by consolidating email servers. Without the need for end-user retraining, Bynari provides seamless interoperability with the latest versions of Outlook and other email clients.

Installation

The insight server installation is an rpm package that is managed by the rpm package handler. However, certain configurations need to be in place for a complete installation.

Before installing Insight Server, please make sure that the minimum requirements for your Linux distribution are met.

Minimum System requirements for Insight Server:

- Minimum 1 GB of free hard drive space for Bynari installation
- Bynari Installation directory is /opt/insight
- User Disk Space - To be determined by user activity (loc: /opt/insight/var/spool/imap)
- Minimum of 512MB swap partition
- Pentium II class or higher i686 based processors
- 256 MB Ram (If SpamAssassin is to be used : Minimum of 512 MB Ram)
- Network Interface Card/Ethernet

Supported Linux Distributions

Bynari supports variety of Linux operating systems. Insight Server will run on major distributions and their latest versions: Red Hat, SuSE, Debian, and Fedora Linux. To determine if your hardware server is supported, please check with the hardware vendor for support of various versions and distributions of Linux. Depending on the hardware manufacturer, they will support certain versions of Linux distributions, only.

If you are running any Red Hat updates, please backup Insight Server prior to the upgrade of your Red Hat Operating system.

If you are UPGRADING any version 4.x (for instance 4.x.1 to 4.x.2 to 4.x.5), there is an upgrade issue with the Red Hat rpm; Red Hat tries to UNINSTALL the old RPM after upgrading the Insight Server. This will remove the /opt/insight directory; to avoid this issue, please upgrade Insight Server using the

" --nopostun" option.

Full command for an upgrade is as follows:

```
# rpm -Uvh --nodeps --nopostun insightserver-x.x-x.i386.rpm
```

Prerequisites for Insight Server

This section discusses the prerequisites for Installing Insight Server onto your newly installed Linux distribution. This section identifies the requirements of the libraries used by Insight Server

as well as the host & domain name configuration. The former being extremely important when generating the configuration files for the base installation of Insight Server. If these entries are not configured properly upon initial installation then Insight Server will not be able to route mail locally.

The following is an initial checklist:

- TCP/IP address of mail server
- Hostname of mail server
- Domain in which the server will reside
- Hard drive space required by mail users (Bynari uses /opt partition)
- Insight Server license key or demo key (30 day free trial)

The following commands can be used on a Linux server to validate that the items above are properly configured:

```
# hostname -a Hostname of the system
# hostname -d Domain name of the system
# hostname -f The Fully Qualified Domain Name (FQDN) of the system
```

Please ensure that the configuration information is correct before starting the installation process of the Insight Server.

If the “hostname -d” doesn’t properly return the domain name then the parameter has not been properly set. Please set the above configuration parameters to a new name that includes the FQDN. To set this option the “hostname” command can also be used for updating the runtime configuration:

```
# hostname mail1.example.com
```

Please refer to your Linux distribution documentation on retaining the changes permanently for the distribution in use.

In addition to the above hostname settings, it may also be necessary to edit the /etc/hosts file. Two entries that are required in the hosts file are localhost as well as the machine name. Below are examples of these entries:

```
127.0.0.1      localhost.localdomain  localhost
192.168.30.131 mail1.example.com mail
```

RPM Dependencies

Insight Server requires the following additional RPM packages beyond a base installation of Linux on some distributions. The two most commonly needed packages beyond the base installation are:

```
libtool-1.5.x-x
gmp-4.2.x-x
```

Port Availability

This is a list of required available ports required by Insight Server:

21: FTP (For Free/Busy Publishing)
22: SSH (Default in Linux)
25: SMTP
80: Apache
110: POP3
143: Cyrus/IMAP
389: LDAP
443: Secure Port for Apache
636: Secure Port for LDAP
993: Secure Port for Cyrus/IMAP

Warning: If you do not turn off sendmail or any other service using a required port listed above, the installation will not complete normally!

Disabling applications using ports needed by Insight Server

The most common applications that cause port conflicts are Sendmail and Apache. To stop and configure Sendmail so that it does not startup at the next reboot time, type the following at the Linux prompt:

For Sendmail:

```
# /etc/init.d/sendmail stop
```

To permanently disable sendmail from startup run the command...

```
# chkconfig sendmail off
```

For Apache:

```
# /etc/init.d/httpd stop
```

To permanently disable apache from startup run the command...

```
# chkconfig httpd off
```

Finding a process currently bound to a port:

To locate which process is currently bound to a given port that is keeping you from completing the installation process use the netstat command from a shell prompt. In the following example, port 389 is already in use and we would like to know which process is currently bound to this port.

```
# netstat -tan|grep 389
tcp    0    0 0.0.0.0:389      0.0.0.0:*        LISTEN  13097/slapd
```

This information can be helpful in tracking down which program is currently a given port. In the above example the process is named slapd which is used by OpenLDAP. This was a SUSE 9.0 SLES installation where OpenLDAP was initially installed on the server. To disable the installed version of OpenLDAP we ran:

```
# /etc/init.d/ldap stop
```

Then to disable the program from the startup sequence:

```
# chkconfig ldap off
```

Recovering from conflicting Services

If the steps above were not taken, then to recover from the installation, follow the below steps to complete the installation process.

Common error message received:

“Error: Can't start until the following ports are available”

1. Once the service currently using the port has been stopped you can continue the setup process by running the command...

```
# /opt/insight/etc/insightserver-setup.sh
```

2. Often when this issue occurs the default password is not displayed at the end of the installation process. To retrieve this information run the following command...

```
# grep rootpw /opt/insight/etc/openldap/slapd.conf
rootpw {default pwd displayed here}
```

Note: Once the password is changed, it is stored in an encrypted format in this directory. You must have a utility called getpw to retrieve this information.

New 4.2 Insight Server Installation

Note: PLEASE MAKE TWO BACKUPS OF YOUR DATA BEFORE STARTING ANY upgrade process.

Installation Steps

1. Start a Shell session.
2. Login as ROOT
3. Type the following to begin the rpm installation;
`# rpm -i insightserver-x.x-x.i386.rpm`
4. Insight Server will automatically start the configuration. When it is complete, (PLEASE WRITE DOWN THE PASSWORD UPON COMPLETION!) a unique manager password will be created. This password is used to login, initially, to the Insight Server.

An example of the final output:

"Your Server has been setup with the administrative account username of 'manager' and the default password of 'CDriaeYZ' -- Please change this immediately!"

Note: Immediately after registering the product the administrator must change the default manager password. This is for security reasons since the password is generated and stored in clear text until it is changed through the web admin interface.

5. To administer the Insight Server, go to the web admin console (open a browser and type `http://yourserveripaddress` [or the Fully Qualified Domain Name (FQDN) that the DNS server will recognize for your Insight Server.]
6. A login screen will appear; user name is "manager" and the default password is the one noted at the end of the installation.
7. The "Registration" section will appear. Read and agree to the End User License Agreement (EULA).
8. Enter your license key or go to 30 day evaluation mode.
9. It is recommended that you change the password for "manager".
10. To change your password, go to the Accounts section, click on manager account.

Congratulations! Your server is now installed and ready for use. See the Server Administrators Guide for further information.

4.0 to 4.2 Insight Server Upgrade

Note: PLEASE MAKE TWO BACKUPS OF YOUR DATA BEFORE STARTING ANY upgrade process.

Pre-installation checklist:

Objects that will not get migrated:

- User-created rules/filters (Sieve rules)
- User-modified/customized configuration for Postfix, Apache, OpenLDAP, ProFTPD, Cyrus.
- SpamAssassin settings
- WebClient user-preferences

Upgrade from 4.0 to 4.2 on the same hardware server:

Download Insight Server 4.2 on the existing server, and run this command to begin the installation:

1. Stop Insight Server 4.0: `# /etc/init.d/insightserver stop`

Note: Ensure that all Insight Server services are stopped.

2. `# rpm -ivh insightserver-4.2.0-*.rpm`

Insight Server 4.2 will now begin installing and will automatically migrate-over the 4.0 accounts and mail to Insight Server 4.2

3. When the installation is complete, login as “manager” with the password that is displayed at the end of the 4.2 installation, and register the 4.2 server with the Insight Server 4.2 license key.

Note: Insight Server 4.2 will not accept the old Insight Server 4.0 license key. Please contact Bynari support to retrieve your 4.2 license key if you have a valid Annual Support and Maintenance contract. For customers without Annual Support and Maintenance, please contact Bynari or your Bynari distributor for pricing information.

Congratulations! Your server is now installed and ready for use. See the Server Administrators Guide for further information.

Upgrade from 4.0 to 4.2 on a new hardware server:

1. Tar the /opt/is4 directory from the current 4.0 server.
`# tar czvf is4.tgz /opt/is4`
2. Un-tar the tar file on the new server into /opt/is4/ directory
`# tar xzvf is4.tgz -C /`

3. Download and install Insight Server 4.2 on the new server, and run this command to begin installation:

```
# rpm -ivh insightserver-4.2.0-*.rpm
```

Insight Server 4.2 will now begin installing and will automatically migrate-over the 4.0 accounts and mail to Insight Server 4.2

4. When the installation is complete, login as “manager” with the password that is displayed at the end of the 4.2 installation, and register the 4.2 server with the Insight Server 4.2 license key.

Note: Insight Server 4.2 will not accept the old Insight Server 4.0 license key. Please contact Bynari support to retrieve your 4.2 license key if you have a valid Annual Support and Maintenance contract. For customers without Annual Support and Maintenance, please contact Bynari or your Bynari distributor for pricing information.

Congratulations! Your server is now installed and ready for use.

4.1 to 4.2 Insight Server Upgrade

Note: PLEASE MAKE TWO BACKUPS OF YOUR DATA BEFORE STARTING ANY upgrade process.

Note: Insight Server 4.2 no longer includes the WebClient as was the case in Insight Server version 4.1. This component must now be installed as a separate rpm package. See the section titled Insight WebClient Installation in this document.

Upgrade from 4.1 to 4.2 on the same hardware server:

Download Insight Server 4.2 on the existing server, and run this command to begin the installation:

1. Stop Insight Server 4.1: `# /etc/init.d/insightserver stop`

Note: Ensure that all Insight Server services are stopped.

2. `# rpm -Uvh insightserver-4.2.0-*.rpm`

Insight Server 4.2 will now begin installing and will automatically migrate-over the 4.1 accounts and mail to Insight Server 4.2

When the installation has completed, login as “manager” and register the 4.2 server with

the Insight Server license key.

Congratulations! Your server is now installed and ready for use.

Upgrade from 4.1 to 4.2 on a new hardware server:

1. In the Web Administrator interface go to Tools and select Backup & Restore then select Create Backup. Create one of each type of available backups Mail, LDAP, and Configuration.
2. Install the same version of Insight Server 4.1 currently running on the new server. Restore the three backups Configuration, LDAP, and Mail in that order. Now see the above section titled Upgrading from 4.1 to 4.2 on the same hardware.

Insight WebClient 4.2 Installation

Note: Insight WebClient is no longer bundled with the Insight Server software. This means that a separate rpm package installation must be performed to use the Insight WebClient software. Please go to the www.bynari.net for download information or contact support@bynari.net for further assistance.

Make sure that the Insight Server package is installed and working properly before installing the Insight WebClient software.

Download and install Insight WebClient onto the server, and run this command to begin installation:

```
# rpm -ivh insightwebclient-4.2.*-*.rpm
```

After the installation is complete, the WebClient will be ready for use. Users may gain access to the WebClient simply by entering the URL to the email server of choice.

The URL for the WebClient is typically `http://youremailserver/groupware/`

The secure page URL is generally `https://youremailserver/groupware/`

Note: In order to use the WebClient, a license key is needed and can be obtained by purchasing WebClient licenses. To activate the WebClient, login as "manager" from the WebClient interface, and enter the license key code.

Administration

All administrative functions for Insight Server are controlled and set within the Web Administration console. This interface has two modes, one for administrators and one for users. In this document we focus on the Administrator portion which includes system configuration, system maintenance, and domain/user administration.

The following options are located on the left side of the screen:

- Accounts
- Aliases
- Mail Folders
- Mail Delivery
- Configuration
- Tools
- System
- Web Client

Accounts

Managers can create and administer domains, organizations, groups, users, or resources. Newly created objects reside in the LDAP server (Open LDAP).



Figure 1 - Account browser screen in the Web Administrator console

After selecting the “Accounts”, clients can view accounts, create an object, or search for a specific account. By selecting “View Accounts”, the main account sections can be accessed (Figure 1).

Default Accounts

By default there are two automatically-created accounts:

1. “manager” account – The mail server default administrator account. It is to be used for most administrative functions, such as creating domains, users, public folders, etc. The password can be changed from the web interface.
2. “service” account – This account can only be seen when upgrading from an Insight Server 4.1 installation. This information no longer applies to new installation of Insight Server 4.2 since this account has been hidden to avoid accidental modification by Administrators unaware of this accounts purpose. Insight Server uses this account when binding for authentication sequences. This read-only account information is stored in various configuration components utilizing the LDAP server for authentication. The password can be changed from the web interface if needed.

View Accounts

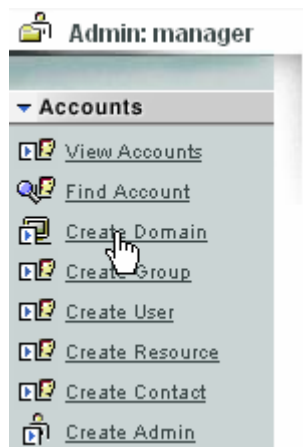


Figure 2 - Account Browser create new

Under the Accounts tab, Insight Server allows the addition of new objects. (Figure 2). Selecting View Accounts permits a review of all accounts on the system.

mail1.example.com



If a user account link is selected, a new screen will appear revealing the user’s attributes. Near the top of the screen another hyperlink will appear named “View Mail Folders”. When this link is followed, a listing of all of the user’s folders currently residing on the server is shown.

Example:

Cathy Marshall, example.com (User)



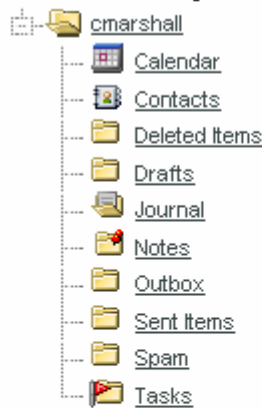
[View Mail Folders](#)

Organization or Group Name

Figure 3 - View Folders

Select “View Folders” for a display of a users folder list when editing the users properties.

mail1.example.com



Total messages: 0
Recent messages: 0
Unseen messages: 0

Reconstruct all mail folders

Figure 4 - Folder View

Once the user connects to the server and the client has synchronized, all data will be moved to the server from the e-mail client.

Find Accounts

Insight Server enables managers to easily manage a large number of users or objects, using the user search function (Figure 5).

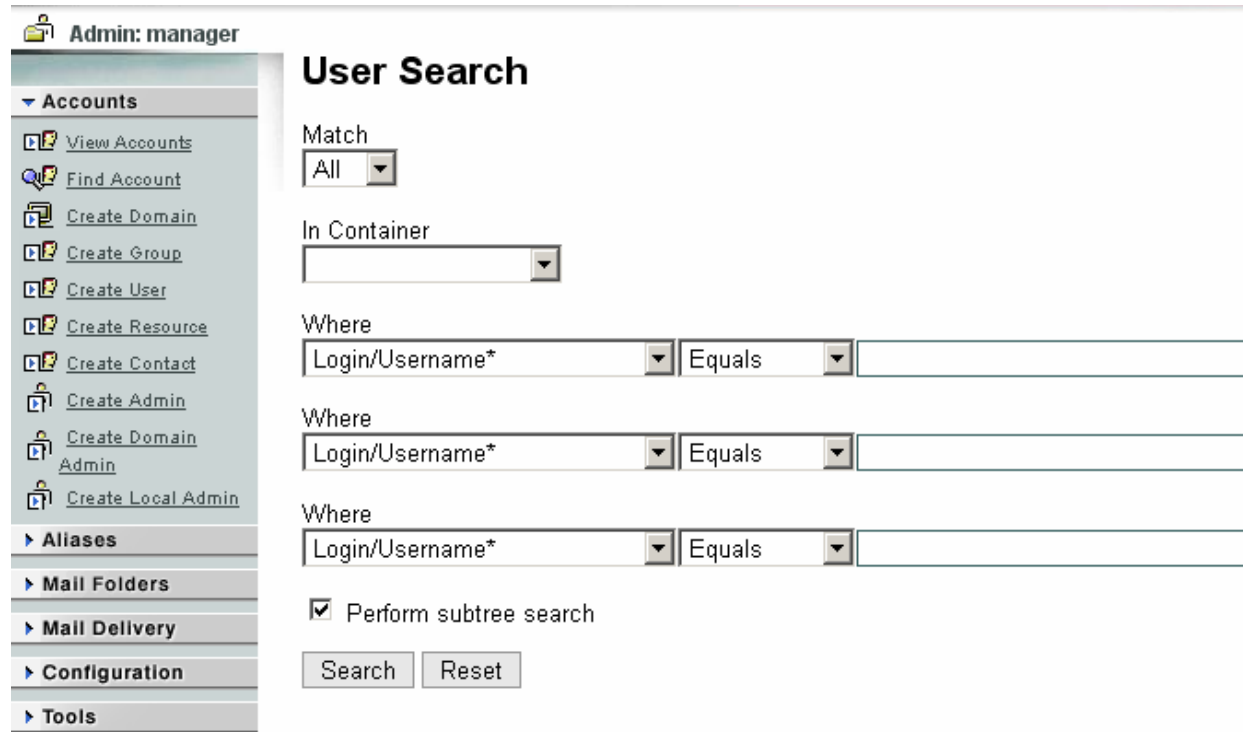


Figure 5 - User search Selection

Create Domain

Insight Server uses the Linux system’s domain name as a default. However, should the use of more than one domain be necessary, Insight Server is capable of supporting multiple domains. If only one domain is used, please skip to the next section, “Creating an organization”.

Many organizations have subsidiaries or host multiple websites. Bynari Insight Server’s successful support of multiple domains allows users to have mail delivered to various domains, using only one server. The Create Domain function enables users to construct several domains.

To create a new Domain, click **Accounts -> Create Domain**

On the “Creating New Domain” screen (Figure 6) fill in the appropriate information. Mandatory fields are designated by an asterisk (*). The Organization name must be identical to the new domain name being created.

Creating new Domain

Basic

Domain*	<input type="text"/>
---------	----------------------

Alias Management

Can users create aliases	<input type="button" value="No"/> ▾
--------------------------	-------------------------------------

General

Organization	<input type="text"/>
Description	<input type="text"/>

Figure 6 -- Creating New Domain

Once the “Create” button is clicked, the new Domain and Organization appear in the LDAP tree. The system will then provide a message regarding the status of the insert. (The letter “O” represents organization).

Private Domains

Insight Server allows certain domains to be private from the rest. When you add or edit a new domain, organization, or group, you have the option to "Make private from rest of directory." If you check this, then only members inside this container sub tree will have access to see the users locally.

Example: There are two domains; bynari.net and private.com. Bynari.net is public and private.com is not. Users in bynari.net domain will not be able see any user in the private.com domain. However, the users in the private.com domain will be able to see the users in the bynari.net domain because it is public.

The option is located above the “Create” buttons on the create-domain page. See figure 6.5.

Make private from rest of directory

Create	Reset
--------	-------



Figure 6.5 - Private Domains

Once the “Create” button is clicked, the new Domain and Organization appear in the LDAP tree. The system will then provide a message regarding the status of the insert.

(The letter “O” represents organization).

Required information for creating a domain: **Domain name and organization.**

Note: If a domain contains objects, it cannot be deleted. To delete the domain, the organizations, groups, users and resources within that domain must first be deleted or moved to another domain.

Create Organization

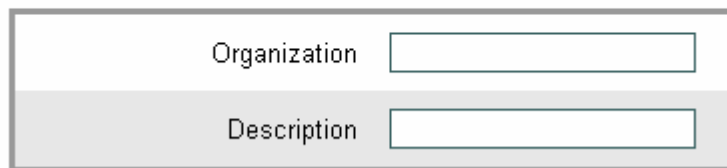
Organizations can be created for ease of managing multiple groups. An organization can contain three types of entries: users, groups, or resources. A group is a collection of multiple users. As such, an organization is a collection of groups. This concept is implemented in the LDAP Server.

To create a new Organization, select **Accounts -> Create Organization**

Complete the fields with the organization’s information (i.e., address and phone number) (Figure 7) and then click “Create”.

Creating new Organization

General



Organization	<input type="text"/>
Description	<input type="text"/>

Figure 7 - Create New Organization

Once created, the user can check the status of the new entry in the LDAP tree. The new organization appears as a folder.

Required information for creating an organization: **organization name.**

Deleting: If an organization contains objects, it cannot be deleted. To delete the organization, groups, users and resources within that organization must first be deleted or moved to another organization.

Create Group

Groups are sub-containers of Organizations and can be created to organize email users in various departments. For example, a manager can create a Sales group for a user in the Sales Department and a Technical Support group for another user in the Technical Support Department. This feature enables users to easily and quickly perform LDAP searches.

To create a group, select **Accounts -> Create Group**

Creating new Group

The screenshot shows a web form for creating a new group. At the top, there is a section titled "Organization or Group Name" which contains a dropdown menu. Below this is a section titled "General" which contains two text input fields: "Group*" and "Description".

Figure 8 -- Create a New Group

The Distinguished Name (DN) must be checked when the window appears. The DN is used for the LDAP to keep an entry unique. Each DN will reflect the name of an organization that was previously created. Two entries are made in the LDAP server and are reflected in the DN option.

Required information for creating a group: **The organization of which the (DN) will be a part, and a group name.**

Deleting: A group cannot be deleted if it contains users or resources. See rule for deleting Domains and Organization.

Create User & User Options

New users may be added once organizations and/or groups have been created. The container (DN) for the user must be selected. Click on the arrow radio button for a list of all organizations and groups that are created on the system. The new user (a specified individual mailbox) can be placed in either an organization or a group.

Under the "General" section, configuration information needs to be entered. (Note: login user name, password, and last name are required entries, as designated by an asterisk [*].)

There are additional options available in this menu (i.e., not creating a mailbox immediately, setting mailbox size (quota), creating Outlook Folders, access to the WebClient, and restricting a user from sending/receiving on the local network only.)

Managers may wish to create user IDs with restricted email functions such as sending and receiving email. See below for the extra options available.

<input checked="" type="checkbox"/>	Create mailbox?
<input type="checkbox"/>	Set quota? <input type="text"/> bytes
<input type="checkbox"/>	Create Outlook Folders? en <input type="button" value="v"/>
<input checked="" type="checkbox"/>	Access WebClient?
<input type="checkbox"/>	Send only local mail?
<input type="checkbox"/>	Receive only local mail?

<input type="button" value="Create"/>	<input type="button" value="Reset"/>
---------------------------------------	--------------------------------------

Figure 9 - User Creation Options

The additional options are:

- **Create mailbox:** This option will automatically generate a mailbox for the new user if checked.
- **Set quota:** This option sets a mailbox size quota for the user. The quota is in bytes and will prevent users from exceeding the mailbox size limit.
- **Create Outlook Folders:** This option will automatically create all the default “Outlook folders”, such as Calendar, Contacts, Tasks, Drafts, Sent Items, etc. The drop dow box denotes which Language to create the folders in.
- **Access WebClient:** This option will allow the user to utilize Insight WebClient (assuming WebClient licenses have been purchased).
- **Send only local mail?:** This option restricts a user from sending email to external email addresses. The user will only be able to send email to other users on the local network.
- **Receive only local mail?:** This option restricts a user from receiving email from external email addresses. The user will only be able to receive email sent from other users on the local network.

Once a new user is created, the LDAP tree will reflect the new ID on the main account browser page. The additional entry of “cn” is shown which stands for Common Name. This information is used by the LDAP server uses this to distinguish the users and resources.

Minimal required information for creating a user is as follows:

Container – This is where the mailbox will be created. The container can be an Organization or group.

Login/User name – Enter the name of the mailbox in this field.

Password – A password must be provided. (The password is set and encrypted using SSHA, thus replacing the older base 64 that was previously used).

Last name – Enter the user’s last name in this field. (The first name or middle initial are not required).

Create Resource

Resources are generally created for very specific reasons. Managers may create resource accounts to represent a resource, such as a conference room or video projector. Insight Server will automatically manage this account, accepting and declining Meeting Requests. Free/Busy information is also available for these accounts.

Create Contact

This option provides administrators the ability to add, remove, and modify external contacts. The external contact information is stored within LDAP similar to that of users, which provides all users access to the external contact listing. The external contacts can be accessed from Insight AddressBook and WebClient as well as SquirrelMail® and IMAP clients such as Thunderbird®. Public Distribution Lists can also be created using the external contact listings.

The screenshot shows the Insight Server administration interface. On the left is a sidebar menu with the following items: Accounts (expanded), Aliases, Mail Folders, Mail Delivery, Configuration, Tools, System, and WebClient. Under 'Accounts', the 'Create Contact' option is highlighted with a mouse cursor. The main content area is titled 'Admin: manager' and contains three sections:

- Organization or Group Name:** A single text input field with a dropdown arrow on the right.
- General:** A section containing four text input fields: 'First Name', 'Middle Initial', 'Last Name*', and 'E-Mail Address'.
- Contact:** A section containing three text input fields: 'Display Name', 'Home Phone', and 'Home Postal Address'.

Figure 10 – Create a new Contact

Create Administrator

The Administrator account has the same authority privileges as the Manager account. Both are allowed full web based access for configurations. These accounts can be used to increase the system's security. The Manager account can also be kept in secret and only used to remove other Administrators.

Create Domain Administrator

When using multiple domains, a Domain Administrator can be created for certain domains under this menu option. This domain administrator ID will only be allowed to create and delete users, groups, resources, and local domain admins only in the particular domains for which it was created. Domain admins can also set quota sizes for users' mailboxes. No other functions can be performed by this administrator ID.

Create Local Administrator

This ID is used to delegate user creation and deletion to other users. It will only allow user creation in the specific GROUP in which the user ID was created.

Aliases

System aliases are created in this section to add a new system alias or user aliases.

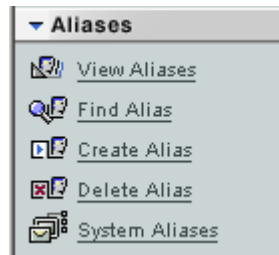


Figure 11 - Aliases Menu

View Aliases

If selected, this option will display a list of all aliases that have been created.



Figure 12 - View Aliases

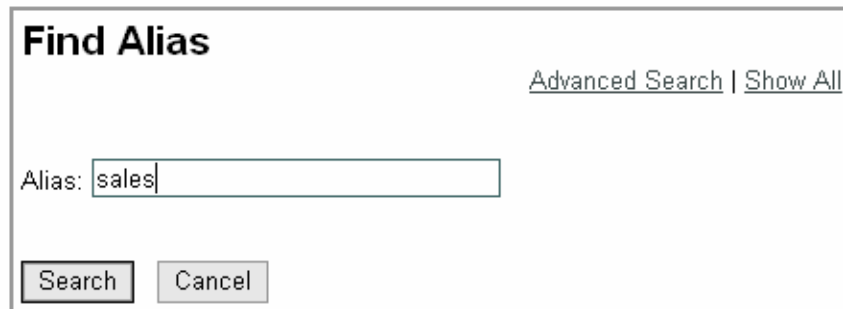
To remove an alias, simply click on the delete icon.

Find Alias

This option allows a user to search for marked aliases in different domains. Options include a basic, simple search and/or an advanced search.

To search for an alias on the system, enter the alias name and click the search button. A list of all aliases found will be displayed.

Simple search:



The screenshot shows a web form titled "Find Alias". In the top right corner, there are two links: "Advanced Search" and "Show All". Below the title, there is a text input field labeled "Alias:" containing the text "sales". At the bottom of the form, there are two buttons: "Search" and "Cancel".

Figure 13 - Find aliases – simple search

The Advanced Search option allows for a selection of criteria for more detailed searching.



The screenshot shows a web form titled "Find Alias". In the top right corner, there are two links: "Advanced Search" and "Show All". Below the title, there is an empty text input field labeled "Alias:". At the bottom of the form, there are two buttons: "Search" and "Cancel".

Figure 14 - Find aliases - Advanced Search Options

The *Show All* option displays all aliases created on the system. To remove an alias, click the Delete icon.

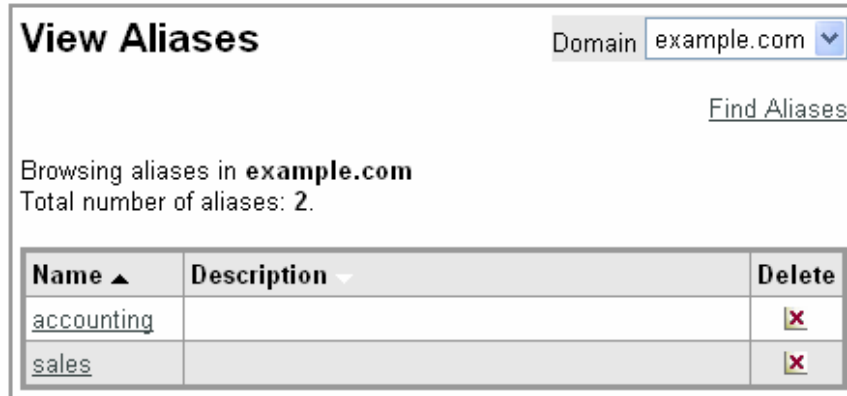


Figure 15 - Find aliases - Show all

Create Alias

To use this function, click on the Create Alias icon to select the domain from the alias list.

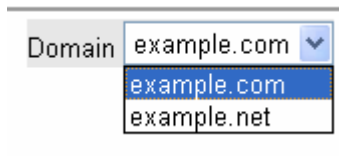


Figure 16 - Create alias

Fill in the appropriate information in each field. (Note: fields marked with an asterisk [*] are required). The Open Membership field allows the user the ability to send to the alias from other domains. The Restricted field allows only users in the same domain to send to the alias created for that domain. Alias owners have permission to modify alias information. Alias members are those who will receive email sent to the alias.

Create Alias Domain **example.net**

* - Indicates a required field

* **Alias:** @example.net

Description:

Membership: Open Restricted

* **Alias Owners:** (DNs separated by commas) [[Browse](#)]

* **Alias Members:** (DNs separated by commas) [[Browse](#)]

Figure 17 - Alias creation

Once the information is entered, select *Create*. *Reset* will reset all the fields to start over, *Cancel* will return to the alias display page.

Delete Alias

To delete an alias, enter the alias name and click “Delete”. A list of all aliases can be viewed by selecting *Show All*.

Delete Alias

Alias:

Figure 18 - Delete Alias

System Aliases

Enter the name required and the email address separated by commas in the "New Alias" section to add a *System Alias*. To change an alias, select the box and change the field, then select *Update All*. To delete an alias, select the alias checkbox and click "Delete".

Note: Caution must be used in multiple domain configuration because System Alias are system wide; thus if created as a system alias, all domains created on the system will be affected.

Select	Mail Alias	Value
<input type="checkbox"/>	MAILER-DAEMON	<input type="text" value="manager@example.net"/>
<input type="checkbox"/>	abuse	<input type="text" value="manager@example.net"/>
<input type="checkbox"/>	apache	<input type="text" value="manager@example.net"/>
<input type="checkbox"/>	postmaster	<input type="text" value="manager@example.net"/>
<input type="checkbox"/>	root	<input type="text" value="manager@example.net"/>
<input type="checkbox"/>	spam.police	<input type="text" value="manager@example.net"/>
<input type="checkbox"/>	uucp	<input type="text" value="manager@example.net"/>
<input type="checkbox"/>	virusalert	<input type="text" value="manager@example.net"/>
<input type="checkbox"/>	webmaster	<input type="text" value="manager@example.net"/>

New Alias

Alias Mail Addresses

Figure 19 - System alias Creation

Mail Folders

Managers can view and manage the system (manager) inbox and subfolders in the Mail Folder, as well as add folders to the account.

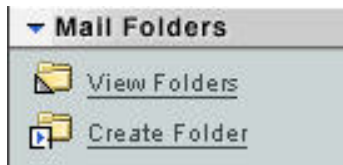


Figure 20 - Mail folders Menu

View Folders

The View Mail Folders option displays the system folders. The folders displayed are for the manager user ID and the shared folders used by the system, including the inbox folder for the manager user ID. The folder display is identical to a user folder display; however, it is for the Manager’s email folders. By default, the inbox is the only folder available following the initial installation. A folder created with this action will create folders that are seen by everyone (unless the default permissions are changed for the specific folder). The folders will show up as “Shared Folders” in each user’s profile. In the example below, the inbox will not be seen by all users; however, the company Calendar folder will.

mail1.example.com



Total messages: 335
 Recent messages: 0
 Unseen messages: 335

Reconstruct all mail folders

View All Users

Figure 21 - System folder view

Note: Only public folders will appear in this section. To view users’ individual folders select “Accounts” > “View Accounts” > select the user in the account listing > select “View Mail Folders” at the top.

Create Folders

To create the folder, type the name of the new folder, select the position in the tree structure where the new folder should be, and select the folder type. If the folder type is incorrectly identified, it will appear as normal mail folders in Outlook with incorrect functionality.

Create a folder

Name

Where

Type

Figure 22 – Create Folder

Any folder created under “Top level” will be a “public folder”, meaning all users will see the folder. The default permissions for top-level folders are lookup, read, and seen, for all users.

Folder Permissions (ACL)

Folder permissions can be added, modified, or deleted by the admin for individual user folders and public folders. Admins can add/remove users and/or user groups to/from user and public folders. This gives the admin control of who has access to specific folders.

To add, modify, or delete a user or user group’s permissions from a folder select ‘View Folders’ from the ‘Mail Folders’ menu, select either a public folder or select ‘View All Users’ to see individual user’s folders and select the appropriate folder, finally add, modify, or delete permissions.

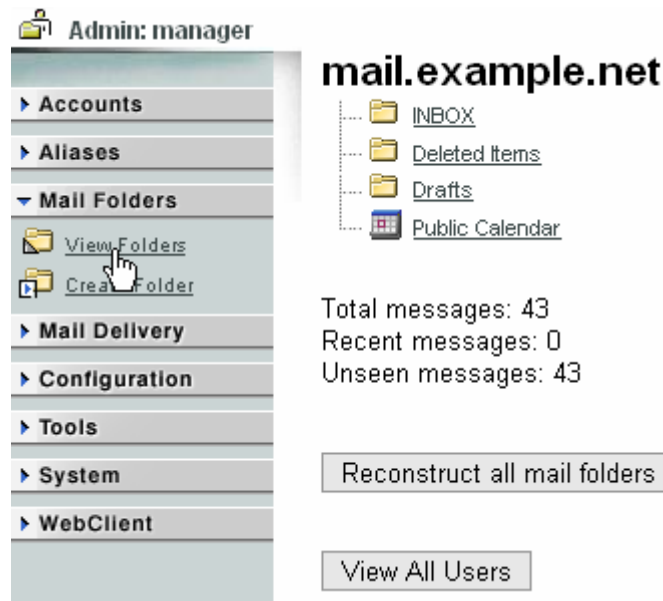


Figure 23 – View Folders

Editing folder: Public Calendar

Current Quota Limit Set quota Kilobytes v

Folder name Rename Delete

Type Appointment Set

Reconstruct

Folder name	User name	lookup	read	seen	write	insert	post	create	delete	admin		
Public Calendar	manager	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Modify	Delete
Public Calendar	user1	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Modify	Delete
Public Calendar	group:ou=examplegroup,o=example.net	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Modify	Delete

o=example.net (group:o=example.net)

ou=examplegroup,o=example.net (group:ou=examplegroup,o=example.net)

Don Tully Jr (thdonjr)

exampleuser1 (exampleuser1)

exampleuser2 (exampleuser2)

exampleuser3 (exampleuser3)

manager (manager)

qa1 (qa1)

qa2 (qa2)

qa3 (qa3)

resource1 (resource1)

user1 (user1)

user2 (user2)

user3 (user3)

lookup	<input checked="" type="checkbox"/>	read	<input checked="" type="checkbox"/>	seen	<input checked="" type="checkbox"/>
write	<input type="checkbox"/>	insert	<input type="checkbox"/>	post	<input type="checkbox"/>
create	<input type="checkbox"/>	delete	<input type="checkbox"/>	admin	<input type="checkbox"/>

Add ACL

Figure 24 –Folder Permissions

Mail Delivery

The mail delivery section contains the mail queue and Global disclaimers.

Mail Queue

The mail queue is managed from this menu. By clicking on the Queue ID, a message will display to determine why it is in the queue. The selected messages can be deleted, put on hold for later delivery, released from the queue, or re-queued to reattempt delivery.

Scrolling over the Queue ID will provide an information box stating the reason why the message is in the queue.

<input type="checkbox"/>	6D540634F	1000b	Wed Oct 6 10:06:08	jdoe@example.com	mrose@example.com
--------------------------	---------------------------	-------	-----------------------	------------------	-------------------

(connect to example.com[192.0.34.166]: Connection timed out)

-- 1 Kbytes i

Figure 25 - Mail queue information box

Only messages that cannot be delivered due to improperly formatted, incorrect addressing, malfunctioning component, etc., will be in the queue. To choose a message, place a check in the box to the left of the Queue ID. Once a message is selected, the following options are available:

Delete: Deletes the selected message(s) from the mail queue. A pop up dialogue box will appear to confirm the deletion request.

Hold: Holds the selected message(s) until they are released (see figure 26). A message will appear near the top of the screen describing the action that transpired. In this example, message 547A816C was placed on hold.

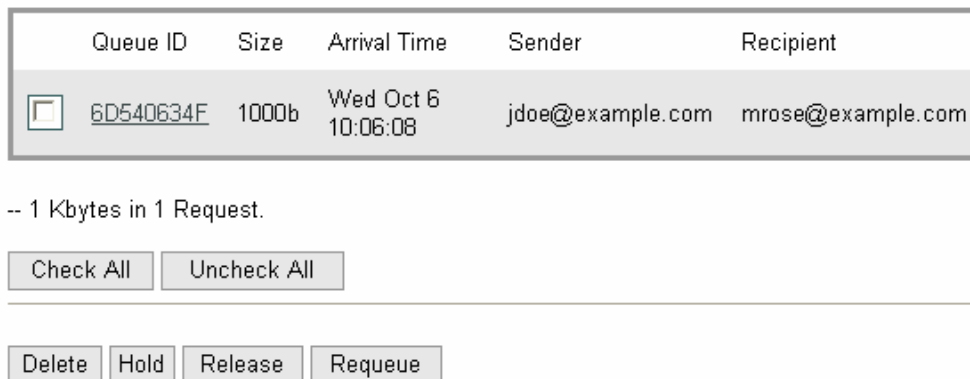


Figure 26 - Mail Management

Release: If a message has been placed on hold by either the manager or another process (such as the header_checks option in postfix) this will release the selected message(s). A message will be displayed as illustrated on Figure 26. In this example, it will state that the message has been released.

Requeue: If the message is stalled, select this option to move it to the beginning of the queue, to be resent.

Global Disclaimers

Disclaimers can be created and attached to emails, either domain wide or only to individual email addresses.

No disclaimers found, please create a default!

Edit disclaimer

Disclaimer name	default
Disclaimer body	<div style="background-color: #cccccc; height: 100px;"></div>

Please select which individuals, groups or whole organizations will be using the current disclaimer.

Organizations	Groups	Individuals and Resources
example.net	Sales	John Doe (jdoe@example.net) ▲ bcc (bcc@example.net) ▼

Update

Figure 27 - User Creation Options

By default the Global Disclaimers are placed on all email (incoming and outgoing) sent to this individual, group, organization or domain. This is inherent since Postfix does not differentiate between incoming and outgoing mail.

To configure Postfix in a manner that this will not occur, the administrator must separate the inbound and outbound mail queues. This is accomplished by configuring multiple IP addresses on the same server. This then provides us the opportunity to configure Postfix to act accordingly based on the IP Address.

Our example will use the address 192.168.1.1 for inbound email (SMTP traffic coming from the internet) and 192.168.1.2 for outbound email (SMTP traffic coming from the clients). The DNS mx records and client configurations would have to be updated accordingly.

Using multiple addresses does not require additional interfaces on the server. See your Linux distributions documentation on multi-homed address configuration for TCP/IP.

When given the above example configuration, we would update the file `/opt/insight/etc/postfix/master.cf` as follows:

Comment out the the line...

```
smtp inet n - n - 100 smtpd -o content_filter=dfilt:
```

Now add two lines at this same location as follows...

```
192.168.1.1:smtp inet n - n - 100 smtpd
```

```
192.168.1.2: smtp inet n - n - 100 smtpd -o content_filter=dfilt:
```

Now save and exit the file and restart the Postfix daemon.

```
# /opt/insight/etc/rc/postfix restart
```

Configuration

Insight Server uses several different components to handle the many functions available to users. List below is a brief description of some of the important configuration components.

Services

These are the services used by the Insight Server to enable collaboration. Individual component configurations can be changed and are described below.

Apache Configuration

The Apache server is the web component of the server for the WEB Administrator Interface and also for the user interface. (This server is used for the Insight Web Client). The configuration can be modified to user requirements.

An additional component now installed in Apache is the WebDAV module. This additional component allows Outlook the ability to publish freebusy information directly to the apache server.

In previous version of Insight Server free busy information was published via ProFTPd (this component is still installed for backward compatibility reasons). However, in the Outlook client configuration under “Tools” > “Options” > “Calendar Options” you can now use the following url to publish and search free busy information.

http://{mail server address}/freebusy/%NAME%.vcf

The {mail server address} can be the IP address for the server or the DNS name.

Further explanation of the Apache configuration parameters can be found by selecting the online help in the Web Administrator Interface.

Navigate to the Apache configuration parameters by logging into the Administrator Web Console → Clicking on the “Services” option under “Configuration” → And clicking the “Apache” Option (Figure 28).

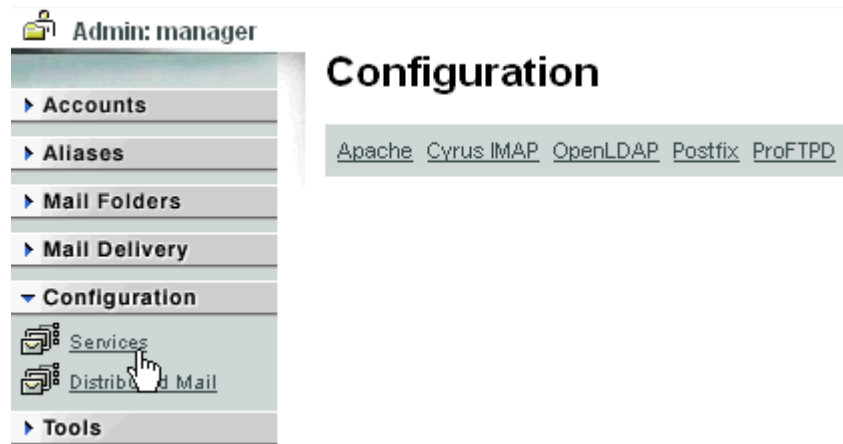


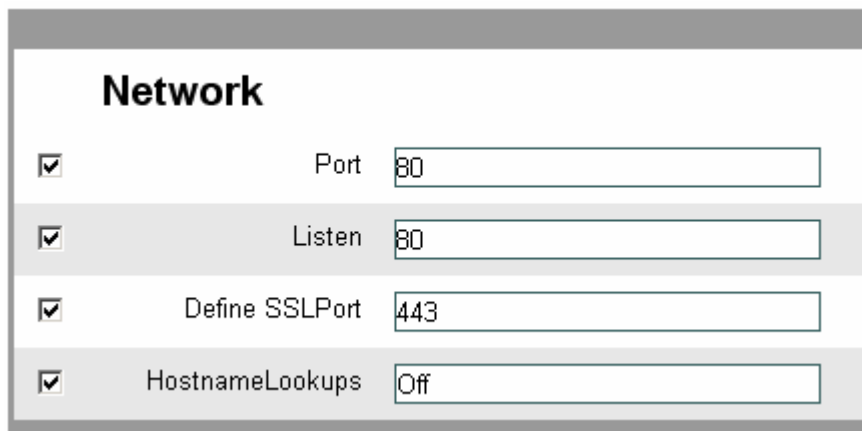
Figure 28 - Navigate to the Apache Configuration Page (apache config.gif)

Settings

Network

The most commonly changed fields are listed below. The Port field is the Port number that Apache uses for allowing connectivity to the web administrator interface which is port 80 by default for web pages; the listen port is used by apache to listen for connectivity. Both of these settings should be set to the same number. By changing this port, the location of accessing the web administrator interface can be changed. If the port is changed to 8080, the listen port must also be changed to 8080. To access the Web Administrator Interface, type <http://servername:8080>.

As shown on Figure 29, HostnameLookups are disabled (off) to prevent Apache from attempting to resolve the server name. If the hostname cannot be found, the Apache web server would time out thus adding delays in displaying the administrator interface.



The screenshot shows a configuration window titled "Network" with four rows of settings. Each row has a checked checkbox on the left, a label, and a text input field. The settings are: Port (80), Listen (80), Define SSLPort (443), and HostnameLookups (Off).

Checkbox	Label	Value
<input checked="" type="checkbox"/>	Port	80
<input checked="" type="checkbox"/>	Listen	80
<input checked="" type="checkbox"/>	Define SSLPort	443
<input checked="" type="checkbox"/>	HostnameLookups	Off

Figure 29 - Apache common Changes (apache2.gif)

The remaining options are:

Port

The Port directive sets the network port on which the server listens.

Listen

The Listen directive instructs Apache to listen to more than one IP address or port. By default, it responds to requests on all IP interfaces, but only on the port indicated by the Port directive.

HostnameLookups

The HostnameLookups directive enables DNS lookups so that host names can be logged.

Performance

Performance		
<input checked="" type="checkbox"/>	MinSpareServers	4
<input checked="" type="checkbox"/>	MaxSpareServers	10
<input checked="" type="checkbox"/>	StartServers	4
<input checked="" type="checkbox"/>	MaxClients	150

Figure 30 - Apache performance Changes

MinSpareServers

The MinSpareServers directive sets the desired minimum number of idle child server processes.

MaxSpareServers

The MaxSpareServers directive sets the desired maximum number of idle child server processes.

StartServers

The StartServers directive sets the number of child server processes created on startup.

MaxClients

The MaxClients directive sets the limit on the number of simultaneous requests that can be supported. This is the maximum number of child server processes that can be created.

Preferences

Preferences		
<input type="checkbox"/>	ServerAdmin	manager@example.net
<input checked="" type="checkbox"/>	ServerSignature	On

Figure 31 - Apache Preference Changes

ServerAdministrator

The ServerAdministrator option allows the user to set the e-mail address to be included in any error messages it returns to the client.

ServerSignature

The ServerSignature directive allows the configuration of a trailing footer line under server-generated documents.

Files

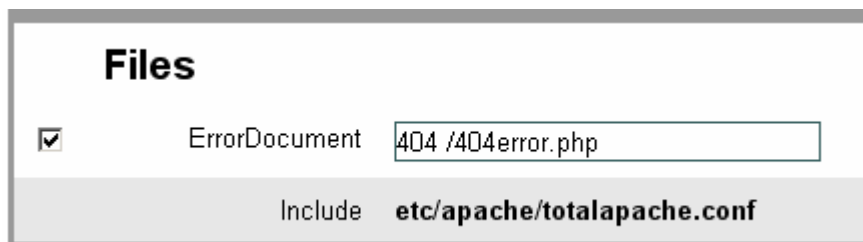


Figure 32 - Apache Files Changes (apache2.gif)

ErrorDocument

The ErrorDocument setting specifies a location for saving the ErrorDocument that can be viewed via the web graphical interface. This file can be located in the logging section.

Include

The Include directive allows inclusion of other configuration files from within the server configuration files.

Log files

The Apache log files are in /opt/insight/logs/

Cyrus IMAP Configuration

Cyrus IMAP is the POP/IMAP component of Insight Server. Cyrus IMAP manages the mail for all the users. Navigate to the Cyrus IMAP configuration parameters by logging into the Administrator Web Console → Clicking on the “Services” option under “Configuration” → And clicking the “Cyrus” Option (Figure 33).

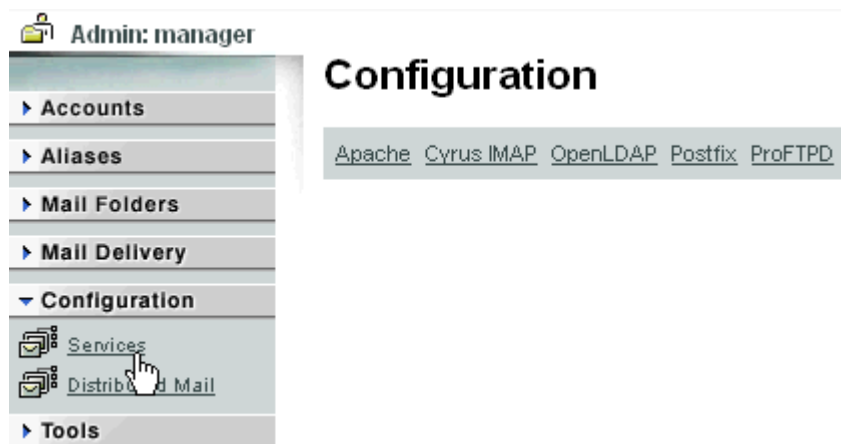


Figure 33 - Navigate to the Cyrus IMAP configuration page (Cyrus config.gif)

A detailed explanation of the configuration parameters can be found in the online help portion of the Web Administrator Interface.

Settings

Files/Permissions

These options allow the administrator to configure the appearance of shared folder names as displayed in Outlook.

<input checked="" type="checkbox"/>	userprefix	<input type="text" value="Other Users"/>
<input checked="" type="checkbox"/>	sharedprefix	<input type="text" value="Shared Folders"/>

Figure 34 - System files Display Name

In Outlook, the folder names are displayed as shown below (Figure 35).

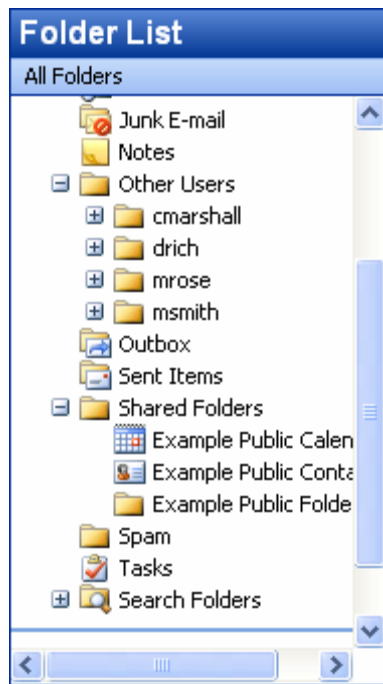


Figure 35 - IMAP folder naming (imap5.gif)

Available Options:

Files/Permissions		
configdirectory		/opt/insight/var/imap
partition-default		/opt/insight/var/spool/imap
sievedir		/opt/insight/var/imap/sieve
sendmail		/opt/insight/sbin/sendmail
unixhierarchysep		yes
altnamespace		yes
<input checked="" type="checkbox"/>	userprefix	Other Users
<input checked="" type="checkbox"/>	sharedprefix	Shared Folders
umask		077

Figure 36 - Cyrus Configuration Files/Permissions

configdirectory

The pathname of the IMAP configuration directory. This field is required.

partition-default

The partition name used by default for new mailboxes (Sievedir). If sieveusehomedir is false, this directory is searched for Sieve scripts.

sievedir

If sieveusehomedir is false, this directory is searched for Sieve scripts.

unixhierarchysep

Use the UNIX separator character '/' for delimiting levels of mailbox hierarchy. The default is to use the netnews separator character '.'

altnamespace

Use the alternate IMAP namespace, where personal folders reside at the same level in the hierarchy as INBOX. This option ONLY applies where interaction takes place with the client/user. Currently, this is limited to the IMAP protocol (imapd) and Sieve scripts (lmtpd). This option does NOT apply to administrator tools such as cyradm (administrators ONLY), reconstruct, quota, etc., NOR does it affect LMTP delivery of messages directly to mailboxes via plus-addressing.

userprefix

If using the alternate IMAP namespace, the prefix for the other users namespace. The hierarchy delimiter will be automatically appended.

sharedprefix

(Shared Folders) If using the alternate IMAP namespace, the prefix for the shared namespace. The hierarchy delimiter will be automatically appended.

umask (077)

The umask value used by various Cyrus IMAP programs.

Preferences

Preferences		
<input type="checkbox"/>	allowallsuscribe	no
<input checked="" type="checkbox"/>	allowanonymouslogin	no
<input checked="" type="checkbox"/>	allowplaintext	yes
<input checked="" type="checkbox"/>	allowusermoves	yes
<input checked="" type="checkbox"/>	quotawarn	90
<input type="checkbox"/>	timeout	30
<input checked="" type="checkbox"/>	imapidlepoll	60
<input checked="" type="checkbox"/>	imapidresponse	yes
<input checked="" type="checkbox"/>	poptimeout	10

Figure 37 - Cyrus Configuration Files/Permissions

allowsubscribe

No information is currently available for this option.

allowanonymouslogin

Permit logins by the user anonymous using any password. Also allows use of the SASL ANONYMOUS mechanism.

allowplaintext

Allow the use of the SASL PLAIN mechanism.

quotawarn

The percent of quota utilization over which the server generates warnings.

timeout

The length of the IMAP server's inactivity autologout timer, in minutes. The minimum value is 30, the default.

imapidlepoll

The interval (in seconds) for polling the mailbox for changes while running the IDLE command. This option is used when idled can not be contacted or when polling is used exclusively. The minimum value is 1. A value of 0 will disable polling (and disable IDLE if polling is the only method available).

imapidresponse

If enabled, the server responds to an ID command with a parameter list containing: version, vendor, support-url, os, os-version, command, arguments, environment. Otherwise the server returns NIL.

poptimeout

Set the length of the POP server's inactivity autologout timer, in minutes. The minimum value is 10, the default.

<input checked="" type="checkbox"/>	popminpoll	<input type="text" value="0"/>
<input checked="" type="checkbox"/>	popexpiretime	<input type="text" value="0"/>
<input checked="" type="checkbox"/>	admins	<input type="text" value="manager"/>
<input checked="" type="checkbox"/>	defaultacl	<input type="text" value="manager lrsiwpcda"/>
<input type="checkbox"/>	autocreatequota	<input type="text" value="2048"/>
<input checked="" type="checkbox"/>	logtimestamps	<input type="text" value="no"/>
<input checked="" type="checkbox"/>	plaintextloginpause	<input type="text" value="0"/>
<input checked="" type="checkbox"/>	loginuseacl	<input type="text" value="no"/>
<input checked="" type="checkbox"/>	singleinstancestore	<input type="text" value="yes"/>

Figure 38 - Cyrus Configuration Files/Permissions

popminpoll

Set the minimum amount of time the server forces users to wait between successive POP logins, in minutes. The default is 0.

popexpiretime

The number of days advertised as being the minimum a message may be left on the POP server before it is deleted (via the CAPA command, defined in the POP3 Extension Mechanism, which some clients may support). %22NEVER%22, the default, may be specified with a negative number. The Cyrus POP3 server never deletes mail, no matter what the value of this parameter is. However, if a site implements a less liberal policy, it needs to change this parameter accordingly.

admins

The list of user id's with administrator rights. Separate each user ID with a space. Sites using Kerberos authentication may use separate "administrator" instances. Note that accounts used by users should not be Administrators. Administrator accounts are not recommended for common mail use, such as with Outlook or the web-client.

defaultacl

(anyone lrs) The Access Control List (ACL) placed on a newly-created (non-user) mailbox that does not have a parent mailbox.

autocreatequota

If nonzero, normal users may create their own IMAP accounts by creating the mailbox INBOX. The user's quota is set to the value if it is positive, otherwise the user has unlimited quota.

logtimestamps

Include notations in the protocol telemetry logs indicating the number of seconds since

the last command or response.

plaintextloginpause

Number of seconds to pause after a successful plaintext login. For systems that support strong authentication, this permits users to perceive a cost of using plaintext passwords. (This does not effect the use of PLAIN in SASL authentications.)

loginuseacl

If enabled, any authentication identity which has a rights on a user's INBOX may log in as that user.

singleinstancestore

If enabled, lmtpd attempts to only write one copy of a message per partition and create hard links, resulting in a potentially large disk savings.

<input checked="" type="checkbox"/>	duplicatesuppression	no
<input checked="" type="checkbox"/>	reject8bit	no
<input checked="" type="checkbox"/>	munge8bit	no
<input type="checkbox"/>	maxmessagesize	10240
<input checked="" type="checkbox"/>	lmtpl_overquota_perm_failure	no
<input checked="" type="checkbox"/>	lmtpl_downcase_rcpt	yes
<input checked="" type="checkbox"/>	sieve_maxscriptsize	32
<input checked="" type="checkbox"/>	sieve_maxscripts	5

Figure 39 - Cyrus Configuration Files/Permissions

duplicatesuppression

If enabled, lmtpl will suppress delivery of a message to a mailbox if a message with the same message-id (or resent-message-id) is recorded as having already been delivered to the mailbox. Records the mailbox and message-id/resent-message-id of all successful deliveries.

reject8bit

If enabled, lmtpl rejects messages with 8-bit characters in the headers. Otherwise, 8-bit characters are changed to `X'. (A proper solution to non-ASCII characters in headers is offered by RFC 2047 and its predecessors.)

maxmessagesize

Maximum incoming LMTP message size. If set, lmtpl will reject messages larger than maxmessagesize bytes. The default is to allow messages of any size.

lmtpl_overquota_perm_failure

If enabled, lmtpl returns a permanent failure code when a user's mailbox is over quota. By default, the failure is temporary. sieve_maxscriptsize Maximum size (in kilobytes) any sieve script can be, enforced at submission by timsieved.

sieve_maxscriptsiz

Maximum size (in kilobytes) any sieve script can be, enforced at submission by tim-sieved.

sieve_maxscripts

Maximum number of sieve scripts any user may have, enforced at submission by tim-sieved. deleteright The right that a user needs to delete a mailbox.

<input checked="" type="checkbox"/>	deleteright	<input type="text" value="a"/>
	virtdomains	userid
	defaultdomain	example.net
	loginrealms	example.net
	sieveusehomedir	false
<input checked="" type="checkbox"/>	lmtp_allowplaintext	<input type="text" value="yes"/>
<input checked="" type="checkbox"/>	rejectnul	<input type="text" value="no"/>
	hashimapspool	yes
	sasl_pwcheck_method	saslauthd

Figure 40 - Cyrus Configuration Files/Permissions

deleteright

The right that a user needs in order to delete a mailbox.

sieveusehomedir

If enabled, lmtpd will look for Sieve scripts in user's home directories: ~user/.sieve.

lmtp_allowplaintext

Allow the use of the SASL PLAIN mechanism for LMTP.

hashimapspool

If enabled, the partitions will also be hashed, in addition to the hashing done on configuration directories. This is recommended if one partition has a very bushy mailbox tree.

sasl_pwcheck_method

The mechanism used by the server to verify plaintext passwords. Possible values also include saslauthd and pwcheck.

Automatically Create Folders

The screenshot shows a configuration panel titled "Automatically create Folders". It contains four rows, each with a checkbox, a label, and a text input field. The first row has the checkbox checked, the label "createonpost", and the input field containing "no". The other three rows have unchecked checkboxes and empty input fields.

Checkbox	Label	Value
<input checked="" type="checkbox"/>	createonpost	no
<input type="checkbox"/>	autocreateinboxfolders	
<input type="checkbox"/>	autosubscribeinboxfolders	
<input type="checkbox"/>	autosubscribesharedfolders	

Figure 41 - Cyrus Automatically create Folders

createonpost

If this is set to yes, when Imtpd receives an incoming mail for an INBOX that does not exist, then the INBOX is automatically created by Imtpd. By default this is set to no.

autocreateinboxfolders

If a user does not have an INBOX created then the INBOX as well as some INBOX subfolders are created under two conditions. 1. The user logs in via the IMAP or the POP3 protocol. (autocreatequota option must have a nonzero value) 2. A message arrives for the user through the LMTPD protocol (createonpost option must yes) autocreateinboxfolders is a list of INBOX's subfolders separated by a "|", that are automatically created by the server under the previous two situations.

autosubscribeinboxfolders

A list of folder names, separated by "|" that the users get automatically subscribed to, when their INBOX is created. These folder names must have been included in the autocreateinboxfolders option of the imapd.conf.

autosubscribesharedfolders

A list of shared folder (bulletin board) names, separated by "|" that the users get automatically subscribed to, when their INBOX is created. These folders must exist before the user mailbox is created and the user must have the appropriate permissions, in order to get subscribed to the shared folder.

Message Parsing

The screenshot shows a configuration panel titled "Message Parsing". It contains three rows, each with a checkbox, a label, and a text input field. All three checkboxes are unchecked and all input fields contain "no".

Checkbox	Label	Value
<input type="checkbox"/>	rfc_ignore_barenewlines	no
<input type="checkbox"/>	rfc_ignore_8bit	no
<input type="checkbox"/>	rfc_ignore_badheader	no

Figure 42 - Cyrus Message Parsing

rfc_ignore_barenewlines

Ignore bare new lines errors within the header. Should be used only for smart migrations, don't use this in production environments.

rfc_ignore_8bit

Ignore 8bit characters in the header. if set to yes the option reject8bit will be ignored, no change to an `X` is done.

rfc_ignore_badheader

Do not reject messages with multiple spaces in headerlines. This function should be used only for smart migrations, and not in production environments.

TLS

TLS		
<input checked="" type="checkbox"/>	tls_cert_file	/opt/insight/etc/ssl/server.pem
<input checked="" type="checkbox"/>	tls_key_file	/opt/insight/etc/ssl/server.pem
<input checked="" type="checkbox"/>	tls_require_cert	0
<input checked="" type="checkbox"/>	tls_ca_file	/opt/insight/etc/ssl/server.pem
<input type="checkbox"/>	tls_ca_path	
<input checked="" type="checkbox"/>	tls_session_timeout	1440
<input type="checkbox"/>	tls_cipher_list	DEFAULT

Figure 43 - Cyrus TLS

tls_cert_file

File containing the global certificate used for ALL services (imap, pop3, lmt, sieve).

tls_key_file File containing the private key belonging to the global server certificate.

tls_key_file

File containing the private key which belongs to the global server certificate.

tls_require_cert

Require a client certificate for ALL services (imap, pop3, lmt, sieve). tls_ca_file File containing one or more Certificate Authority (CA) certificates. tls_ca_path Path to directory with certificates of CAs.

tls_ca_file

File containing one or more Certificate Authority (CA) certificates.

tls_ca_path

Path to directory with certificates of CAs.

tls_session_timeout

The length of time (in minutes) that a TLS session will be cached for later reuse. The maximum value is 1440 (24 hours), the default. A value of 0 will disable session caching.

tls_cipher_list

The list of SSL/TLS ciphers to allow. The format of the string is described in ciphers(1).

Cyrus Murder

Cyrus Murder		
<input checked="" type="checkbox"/>	mupdate_retry_delay	<input type="text" value="20"/>
	proxy_authname	manager
<input checked="" type="checkbox"/>	ldap_bind_dn	<input type="text" value="cn=Insight Service Account"/>
<input checked="" type="checkbox"/>	ldap_password	<input type="text" value="R/BWeXGy"/>
<input checked="" type="checkbox"/>	ldap_filter	<input type="text" value="((login=%u)(login=%u@%d))"/>
<input checked="" type="checkbox"/>	ldap_group_filter	<input type="text" value="(groupName=%u)"/>
<input checked="" type="checkbox"/>	ldap_member_method	<input type="text" value="attribute"/>
<input checked="" type="checkbox"/>	ldap_member_attribute	<input type="text" value="memberOf"/>
<input checked="" type="checkbox"/>	ldap_uri	<input type="text" value="ldap://127.0.0.1/"/>
<input checked="" type="checkbox"/>	ldap_version	<input type="text" value="3"/>
<input checked="" type="checkbox"/>	ldap_sasl	<input type="text" value="0"/>
<input checked="" type="checkbox"/>	ptscache_db	<input type="text" value="skiplist"/>

Figure 44 - Cyrus Murder

mupdate_retry_delay

The time to wait between connection-retries when connecting to the mupdate server.

proxy_authname

This is the SASL username (Authentication Name) to use when authenticating to the mupdate server (if needed). This cannot be changed and is set to “manager” by default.

OpenLDAP Configuration

Insight Server uses an OpenLDAP server and its database to store all user information and is used to authenticate all mail users.

To configure, navigate to the OpenLDAP configuration parameters by logging into the Administrator Web Console → Clicking on the “Services” option under “Configuration” → And clicking the “OpenLDAP” Option (Figure 45).



Figure 45 - Navigate to the OpenLDAP configuration page

Settings

Global

Global	
include	/opt/insight/etc/openldap/schema/core.schema
include	/opt/insight/etc/openldap/schema/cosine.schema
include	/opt/insight/etc/openldap/schema/inetorgperson.schema
include	/opt/insight/etc/openldap/schema/insight.schema
access	to attr=userPassword by self write by anonymous auth by dn="cn=manager" write by * none
access	to attr=objectclass,login,mail,mailalias,webclient,syncServer,syncDN,mailsenderaccess,mailrecipientaccess by self read by dn="cn=manager" write by dn="cn=Insight Service Account" read by users read by * none
access	to * by self write by dn="cn=manager" write by dn="cn=Insight Service Account" read by users read by * none
allow	bind_v2
<input checked="" type="checkbox"/>	idletimeout <input type="text" value="0"/>
	pidfile /opt/insight/var/slaped.pid
	argsfile /opt/insight/var/slaped.args
<input checked="" type="checkbox"/>	password-hash <input style="width: 150px;" type="text" value="{SSHA}"/>
<input checked="" type="checkbox"/>	schemacheck <input style="width: 100px;" type="text" value="on"/>
<input checked="" type="checkbox"/>	sizelimit <input style="width: 100px;" type="text" value="500"/>
<input checked="" type="checkbox"/>	threads <input style="width: 100px;" type="text" value="32"/>
<input checked="" type="checkbox"/>	timelimit <input style="width: 100px;" type="text" value="3600"/>

Figure - 46 Global

include

The openldap schema files that are used by the openldap server.

access

These options are not configurable within the administrator console and listed for informational purposes only. These setting provide the acl's for the LDAP database structure.

allow

Specify a set of features (separated by white space) to allow (default none). bind_v2 allows acceptance of LDAPv2 bind requests. bind_anon_cred allows anonymous bind credentials are not empty (e.g. when DN is empty). bind_anon_dn allows unauthenticated (anonymous) bind whenDN is not empty.

disallow

Specify a set of features (separated by white space) to disallow (default none). bind_anon disables acceptance of anonymous bind requests. bind_simple disables simple (bind) authentication. bind_krbv4 disables Kerberos V4 (bind) authentication. tls_2_anon disables Start TLS from forcing session to anonymous status (see also tls_authc). tls_authc disables StartTLS if authenticated (see also tls_2_anon).

idletimeout

Specify the number of seconds to wait before forcibly closing an idle client connections. An idletimeout of 0 disables this feature. The default is 0.

include

Read additional configuration information from the given file before continuing with the

next line of the current file.

pidfile

The (absolute) name of a file that will hold the slapd server's process ID (see getpid) if started without the debugging command line option.

argsfile

No information is currently available for this option.

password-hash

The hash to use for userPassword generation. One of {SSHA}, {SHA}, {SMD5}, {MD5}, and {CRYPT}. The default is {SSHA}.

schemacheck

{ on | off } Turn schema checking on or off. The default is on.

sizelimit

integer - Specify the maximum number of entries to return from a search operation. The default size limit is 500. threads integer - Specify the maximum size of the primary thread pool. The default is 32.

threads

integer - Specify the maximum size of the primary thread pool. The default is 32.

timelimit

integer - Specify the maximum number of seconds (in real time) slapd will spend answering a search request. The default time limit is 3600.

TLS

The screenshot shows a configuration window titled "TLS" with the following settings:

Option	Value
<input type="checkbox"/> TLSCipherSuite	[Empty text box]
<input checked="" type="checkbox"/> TLSCertificateFile	/opt/insight/etc/ssl/server.pem
<input checked="" type="checkbox"/> TLSCACertificateFile	/opt/insight/etc/ssl/server.pem
<input checked="" type="checkbox"/> TLSCertificateKeyFile	/opt/insight/etc/ssl/server.pem

Figure 47 - LDAP TLS

TLSCipherSuite

cipher-suite-spec Permits configuring what ciphers will be accepted and the preference order. cipher-suite-spec should be a cipher specification for OpenSSL. Example: TLSCipherSuite HIGH:MEDIUM:+SSLv2 To check what ciphers a given spec selects, use: openssl ciphers -v cipher-suite-spec

TLSCertificateFile

Specifies the file that contains the slapd server certificate.

TLSCACertificateFile

Specifies the file that contains certificates for all of the Certificate Authorities that slapd will recognize.

TLSCertificateKeyFile

Specifies the file that contains the slapd server private key that matches the certificate stored in the TLSCertificateFile file. Currently, the private key is not protected with a password, so it is of critical importance that it is protected carefully.

Database

Database	
database	bdb
<input checked="" type="checkbox"/> checkpoint	10
<input checked="" type="checkbox"/> lastmod	on
<input checked="" type="checkbox"/> readonly	off
suffix	""
rootdn	cn=manager
rootpw	{SSHA}VizuGdcze9rc11WI4mh7TommcZmZWuai
<input checked="" type="checkbox"/> cachesize	100000
directory	/opt/insight/var/openldap-data
index	objectClass,login,display-name,mailalias eq
index	cn,sn,mail,givenname,o,ou pres,eq,approx,sub
mode	0600

Figure 48 - LDAP Database Configuration

database

databasesyntax - Mark the beginning of a new database instance definition. databasesyntax should be one of bdb, ldbm, shell, or passwd depending on which backend will serve the database.

lastmod

on | off - Controls whether slapd will automatically maintain the modifiersName, modifyTimestamp, creatorsName, and createTimestamp attributes for entries. By default, lastmod is on. readonly on | off - This option puts the database into read-only mode. Any attempts to modify the database will return an unwilling to perform error. By default, readonly is off.

readonly

on | off - This option puts the database into read-only mode. Any attempts to modify the database will return an unwilling to perform error. By default, readonly is off.

rootdn

dn - Specify the distinguished name that is not subject to access control or administrative

limit restrictions for operations on the LDAP database. This DN may or may not be associated with an entry. An empty root DN (the default) specifies no root access is to be granted. It is recommended that the rootdn only be specified when needed (such as when initially populating a database). If the rootdn is within a naming context (suffix) of the database, a simple bind password may also be provided using the rootpw directive.

rootpw

rootpw password - Specify a password (or hash of the password) for the rootdn. If the rootdn is not within the naming context of the database, the provided password is ignored. This option accepts all RFC 2307 userPassword formats known to the server (see password-hash description) as well as clear text. slapasswd may be used to generate a hash of a password. Cleartext and {CRYPT} passwords are not recommended. If empty (the default), authentication of the root DN is by other means (e.g. SASL). Use of SASL is encouraged.

suffix

dn suffix - Specify the DN suffix of queries that will be passed to this backend database. Multiple suffix lines can be given and at least one is required for each database definition.

updatedn

dn - This option is only applicable in a slave slapd. It specifies the DN allowed to make changes to the replica (typically, this is the DN slurpd binds as when making changes to the replica).

 cachesize

integer - Specify the size in entries of the in-memory cache maintained by the LDBM backend database instance. The default is 1000 entries.

dbcachesize

integer - Specify the size in bytes of the in-memory cache associated with each open index file. If not supported by the underlying database method, this option is ignored without comment. The default is 100000 bytes.

directory

Specify the directory where the LDBM files containing this database and associated indexes live. A separate directory must be specified for each database. The default is /var/db/openldap/openldap-data.

index

{attrlist|default} [pres,eq,approx,sub,special] Specify the indexes to maintain for the given attribute (or list of attributes). Some attributes only support a subset of indexes. If only an attr is given, the indices specified for default are maintained. Note that setting a default does not imply that all attributes will be indexed. A number of special index parameters may be specified. The index type sub can be decomposed into subinitial, subany, and subfinal indices. The special type nolang may be specified to disallow use of this index by language subtypes. The special type nosubtypes may be specified to disallow use of this index by named subtypes. Note: changing index settings requires rebuilding indices, see slapindex.

mode

Integer - Specify the file protection mode that newly created database index files should have. The default is setting 0600.

Postfix Configuration

Postfix is the Mail Transport Agent (MTA) used. This is the component that sends/receives all email for the server. Postfix passes the incoming mail onto Cyrus which in turn delivers the email to the correct mailboxes.

To configure, navigate to the Postfix configuration parameters by logging into the Administrator Web Console → Clicking on the “Services” option under “Configuration” → And clicking the “Postfix” Option (Figure 49).

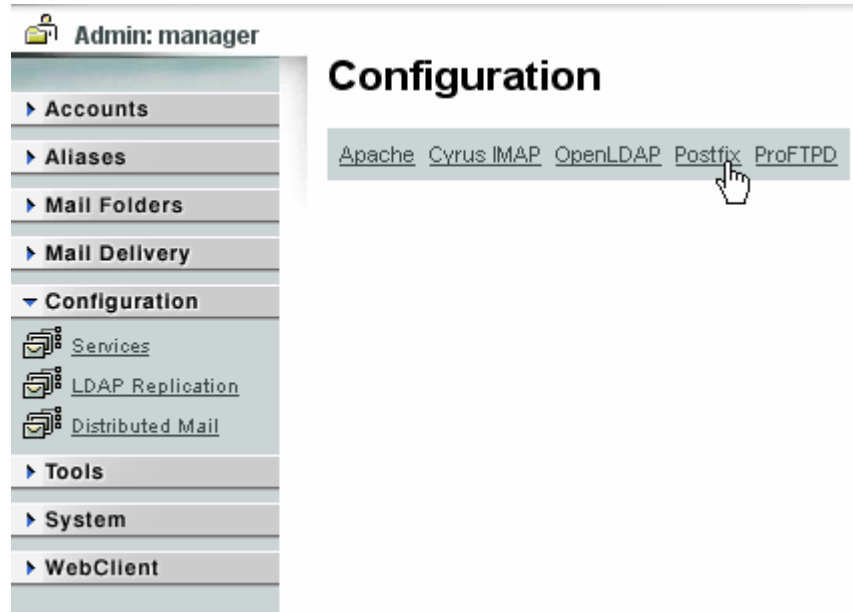


Figure 49 - Navigate to the Postfix configuration page

Settings

Available options include the following:

Networking

Networking		
<input checked="" type="checkbox"/>	myhostname	<input type="text" value="mail2.example.net"/>
<input checked="" type="checkbox"/>	mydomain	<input type="text" value="example.net"/>
<input checked="" type="checkbox"/>	myorigin	<input type="text" value="\$mydomain"/>
<input checked="" type="checkbox"/>	mydestination	<input type="text" value="\$myhostname,\$mydomain"/>
<input checked="" type="checkbox"/>	mynetworks	<input type="text" value="127.0.0.1,127.0.0.1"/>
<input checked="" type="checkbox"/>	relay_domains	<input type="text" value="\$mydestination"/>
<input type="checkbox"/>	relayhost	<input type="text"/>

Figure 50 - Postfix Networking Configuration

myhostname

Describes the fully-qualified domain name of the machine running the Postfix system. `$myhostname` appears as the default value in many other Postfix configuration parameters. `Mydomain` specifies the parent domain of `$myhostname`. By default, it is derived from `$myhostname` by stripping off the first part (unless the result would be a top-level domain).

mydomain

Specifies the parent domain of `$myhostname`. By default, it is derived from `$myhostname` by stripping off the first part (unless the result would be a top-level domain).

myorigin

Specifies the domain that locally-posted mail appears to come from. The default is to append `$myhostname`, which is fine for small sites. If running a domain with multiple machines, the user must change this to `$mydomain` and set up a domain-wide alias database that aliases each user to `user@that.users.mailhost`.

mydestination

Specifies the list of domains that this machine considers itself the final destination for. That includes Sendmail-style virtual domains hosted on this machine. Do not include Postfix-style virtual domains - those domains are specified elsewhere (see `sample-virtual.cf`, and `sample-transport.cf`). The default is `$myhostname + localhost.$mydomain`. On a mail domain gateway, the user should also include `$mydomain`. Do not specify the names of domains that this machine is backup MX host for. Specify those names via the `relay_domains` or `permit_mx_backup` settings for the SMTP server (see `sample-smtpd.cf`). The local machine is always the final destination for mail addressed to `user@[the.net.work.address]` of an interface that the mail system receives mail on (see the `inet_interfaces` parameter). Specify a list of host or domain names, `/file/name` or `type:table` patterns, separated by commas and/or whitespace. A `/file/name` pattern is replaced by its contents; a `type:table` is matched when a name matches a lookup key. Con-

tinue longlines by starting the next line with whitespace.

mynetworks

Lists all networks that this machine somehow trusts. This information can be used by the anti-UCE features to recognize trusted SMTP clients that are allowed to relay mail through Postfix.

relay_domains

Controls the behavior of the reject_unauth_destination and permit_auth_destination restrictions that can appear as part of a recipient address restriction list.

relayhost

Specifies the default host to which mail will be sent when no entry is matched in the optional transport table. When no relayhost is given, mail is routed directly to the destination. On an intranet, specify the organizational domain name. If the user's internal DNS uses no MX records, specify the name of the intranet gateway host instead. In the case of SMTP, specify a domain, host, host:port, [host]:port, [address] or [address]:port; the form [host] turns off MX lookups. If the user is connected via UUCP, see also the default_transport parameter.

Preferences

Preferences		
<input type="checkbox"/>	disable_dns_lookups	<input type="text" value="yes"/>
<input type="checkbox"/>	soft_bounce	<input type="text" value="yes"/>
	queue_directory	/opt/insight/var/spool/postfix
	command_directory	/opt/insight/sbin
	daemon_directory	/opt/insight/libexec
	mail_owner	postfix
<input type="checkbox"/>	in_flow_delay	<input type="text" value="1s"/>
	alias_maps	hash:/opt/insight/etc/mail/aliases

Figure 51 - Postfix Configuration

disable_dns_lookups

yes | no – sets whether or not the dns server should be used to locate account information. Default is set to no.

soft_bounce

Provides a limited safety net for testing. When soft_bounce is enabled, mail will remain queued that would otherwise bounce. This parameter disables locally-generated bounces, and prevents the SMTP server from rejecting mail permanently (by changing 5xx replies into 4xx replies). However, soft_bounce is no cure for address rewriting mis-

takes or mail routing mistakes.

queue_directory

Specifies the location of the Postfix queue. This is also the root directory of Postfix daemons that run chrooted. See the files in `examples/chroot-setup` for setting up Postfix chroot environments on different UNIX systems.

command_directory

Specifies the location of all `postXXX` commands. The default value is `$program_directory`. `daemon_directory` Specifies the location of all Postfix daemon programs (i.e. programs listed in the `master.cf` file). The default value is `$program_directory`. This directory must be owned by root.

daemon_directory

Specifies the location of all Postfix daemon programs (i.e. programs listed in the `master.cf` file). The default value is `$program_directory`. This directory must be owned by root.

mail_owner

Specifies the owner of the Postfix queue and of most Postfix daemon processes. Specify the name of a user account THAT DOES NOT SHARE ITS USER OR GROUP ID WITH OTHER ACCOUNTS AND THAT OWNS NO OTHER FILES OR PROCESSES ON THE SYSTEM. In particular, don't specify `nobody` or `daemon`. PLEASE USE A DEDICATED USER.

local_recipient_maps

Specifies optional lookup tables with all names (not addresses) of users that are local with respect to `$mydestination` and `$inet_interfaces`. If this parameter is defined, then the SMTP server will reject mail for unknown local users. If the default Postfix local delivery agent is used for local delivery, uncomment the definition below. Beware: if the Postfix SMTP server runs chrooted, the user may have to copy the `passwd` (not `shadow`) database into the jail. This is system dependent.

in_flow_delay

Implements mail input flow control. This feature is turned on by default, although it still needs further development. A Postfix process will pause for `$in_flow_delay` seconds before accepting a new message, when the message arrival rate exceeds the message delivery rate. With the default 50 SMTP server process limit, this limits the mail inflow to 50 messages a second more than the number of messages delivered per second. Specify 0 to disable the feature. Valid delays are 0..10.

alias_maps

Specifies the list of alias databases used by the local delivery agent. The default list is system dependent. On systems with NIS, the default is to search the local alias database, then the NIS alias database. See `aliases` for syntax details. If the alias database is changed, run `postalias /etc/aliases` (or wherever the user's system stores the mail alias file), or simply run `newaliases` to build the necessary DBM or DB file. It will take a minute or so before changes become visible. Use `postfix reload` to eliminate the delay.

	alias_database	hash:/opt/insight/etc/mail/aliases
<input checked="" type="checkbox"/>	transport_maps	ldap:/opt/insight/etc/postfix/ldap-mail
	local_transport	lmtp:unix:/opt/insight/var/imap/socket/lmtp
<input type="checkbox"/>	fallback_transport	
<input type="checkbox"/>	error_notice_recipient	manager@example.net
<input type="checkbox"/>	bounce_notice_recipient	\$error_notice_recipient
<input type="checkbox"/>	2bounce_notice_recipient	\$error_notice_recipient
<input type="checkbox"/>	delay_notice_recipient	\$error_notice_recipient
<input checked="" type="checkbox"/>	smtpd_banner	\$myhostname ESMTP \$mail_name
<input checked="" type="checkbox"/>	local_destination_concurrency_limit	5

Figure 52 - Postfix Configuration

alias_database

Specifies the alias database that are built with newaliases or sendmail -bi. This is a separate configuration parameter, because alias_maps may specify tables that are not necessarily all under control by Postfix.

Transport_maps

Specifies a list of transport lookup tables. The optional transport table overrides the default message delivery method (this table is used by the address rewriting and resolving daemon). The transport table can be used to send mail to specific sites via **UUCP**, or to send mail to a mail system that can handle only one SMTP connection at a time.

Note: Transport table lookups are disabled by default.

mailbox_transport

Specifies the optional transport in master.cf to use after processing aliases and .forward files. This parameter has precedence over the mailbox_command, fallback_transport and luser_relay parameters. Specify a string of the form transport:nexthop, where transport is the name of a mail delivery transport defined in master.cf. The :nexthop part is optional. For more details see the sample transport configuration file.

fallback_transport

Specifies the optional transport in master.cf to use for recipients that are not found in the UNIX passwd database. This parameter has precedence over the luser_relay parameter. Specify a string of the form transport:nexthop, where transport is the name of a mail delivery transport defined in master.cf. The :nexthop part is optional.

error_notice_recipient

Recipient of protocol/policy/resource/software error notices.

bounce_notice_recipient

The recipient of single bounce postmaster notices.

2bounce_notice_recipient

The recipient of double bounce postmaster notices.

delay_notice_recipient

The recipient of "delayed mail" postmaster notices.

smtpd_banner

Specifies the text that follows the 220 code in the SMTP server's greeting banner. Some people like to see the mail version advertised. By default, Postfix shows no version.

local_destination_concurrency_limit

How many parallel deliveries are sent to the same user or domain. With local delivery, it does not make sense to do massively parallel delivery to the same user, because mailbox updates must happen sequentially, and expensive pipelines in .forward files can cause disasters when too many are run at the same time. With SMTP deliveries, 10 simultaneous connections to the same domain could be sufficient to raise eyebrows. Each message delivery transport has its XXX_destination_concurrency_limit parameter. The default is \$default_destination_concurrency_limit for most delivery transports. For the local delivery agent the default is 2.

<input checked="" type="checkbox"/>	default_destination_concurrency_limit	20
	debug_peer_level	2
<input checked="" type="checkbox"/>	disable_mime_input_processing	no
<input checked="" type="checkbox"/>	disable_mime_output_conversion	no
	disable_vrfy_command	yes
<input checked="" type="checkbox"/>	mime_boundary_length_limit	2048
<input checked="" type="checkbox"/>	mime_nesting_limit	20
<input checked="" type="checkbox"/>	strict_8bitmime	no
<input checked="" type="checkbox"/>	strict_mime_domain_encoding	no
<input checked="" type="checkbox"/>	always_bcc	bcc@example.com

Figure 53 - Postfix Configuration

default_destination_concurrency_limit

Check help for local_destination_concurrency_limit

debug_peer_level

Specifies the increment in verbose logging level when an SMTP client or server host name or address matches a pattern in the debug_peer_list parameter.

disable_mime_input_processing

While receiving, give no special treatment to Content-Type: message headers; all text af-

ter the initial message headers is considered to be part of the message body.

disable_mime_output_conversion

Disable the conversion of 8BITMIME format to 7BIT format when the remote system does not advertise 8BITMIME support

disable_vrfy_command

This stops some spammers from trying to extract valid email address. By Default is it set to Yes and cannot be changed here.

mime_boundary_length_limit

The amount of space that will be allocated for MIME multipart boundary strings. The MIME processor is unable to distinguish between boundary strings that do not differ in the first \$mime_boundary_length_limit characters.

mime_nesting_limit

The maximal nesting level of multipart mail that the MIME processor can handle. Refuse mail that is nested deeper.

strict_8bitmime

Reject mail with 8-bit text in content that claims to be 7-bit, or in content that has no explicit content encoding information. This blocks mail from poorly written mail software. Unfortunately, this also breaks majordomo approval requests when the included request contains valid 8-bit MIME mail, and it breaks bounces from mailers that do not properly encapsulate 8-bit content (for example, bounces from gmail or from old versions of Postfix).

strict_mime_domain_encoding

Reject mail with invalid Content-Transfer-Encoding: information for message/* or multi-part/*. This blocks mail from poorly written software.

always_bcc

Address to send a copy of each message that enters the system.

<input type="checkbox"/>	hash_queue_depth	2
<input checked="" type="checkbox"/>	hopcount_limit	50
<input checked="" type="checkbox"/>	max_idle	100s
<input checked="" type="checkbox"/>	max_use	100
<input checked="" type="checkbox"/>	delay_warning_time	0h
<input checked="" type="checkbox"/>	initial_destination_concurrency	2
<input type="checkbox"/>	maximal_backoff_time	4000s
<input checked="" type="checkbox"/>	maximal_queue_lifetime	5d
<input type="checkbox"/>	minimal_backoff_time	1000s

Figure 54 - Postfix Configuration

hash_queue_depth

Number of subdirectory levels for hashed queues.

hopcount_limit

Limit the number of Received: message headers.

max_idle

Limit the time in seconds that a child process waits between service requests.

max_use

Limit the number of service requests handled by a child process.

delay_warning_time

The `delay_warning_time` specifies after how many hours a warning is sent that mail has not yet been delivered. By default, no warning is sent.

initial_destination_concurrency

Controls how many messages are initially sent to the same destination before adapting delivery concurrency. Of course, this setting is effective only as long as it does not exceed the process limit and the destination concurrency limit for the specific mail transport channel.

maximal_backoff_time

The maximal amount of time a message won't be looked at after a delivery failure.

maximal_queue_lifetime

The maximal amount of time a message won't be looked at after a delivery failure.

minimal_backoff_time

The minimal amount of time a message won't be looked at, and the minimal amount of time to stay away from a dead destination.

<input type="checkbox"/>	queue_run_delay	1000s
<input checked="" type="checkbox"/>	bounce_size_limit	50000
<input type="checkbox"/>	default_process_limit	50
<input type="checkbox"/>	fork_attempts	5
<input type="checkbox"/>	fork_delay	1a
<input type="checkbox"/>	deliver_lock_attempts	5
<input type="checkbox"/>	deliver_lock_delay	1s
<input type="checkbox"/>	duplicate_filter_limit	1000
<input type="checkbox"/>	header_size_limit	102400

Figure 55 - Postfix Configuration

queue_run_delay

How often the queue manager scans the queue for deferred mail.

bounce_size_limit

How much of an undelivered message is sent back to the sender.

default_process_limit

Default limit for the number of simultaneous child processes that provide a given service

fork_attempts

The number of times to attempt to create a new process before giving up.

fork_delay

The delay between attempts to create a new process.

deliver_lock_attempts

The number of times to try locking a file before giving up.

deliver_lock_delay

How long to wait between attempts to lock a file.

duplicate_filter_limit

Limits the number of envelope recipients that are remembered.

header_size_limit

Limits the amount of memory in bytes used to process a message header.

<input type="checkbox"/>	line_length_limit	2048
<input type="checkbox"/>	message_size_limit	10240000
<input type="checkbox"/>	message_reject_characters	
<input checked="" type="checkbox"/>	message_strip_characters	
<input checked="" type="checkbox"/>	queue_minfree	0
<input checked="" type="checkbox"/>	transport_retry_time	60s
<input type="checkbox"/>	stale_lock_time	500s
<input checked="" type="checkbox"/>	allow_percent_hack	yes
<input type="checkbox"/>	fallback_relay	
<input checked="" type="checkbox"/>	ignore_mx_lookup_error	no
<input checked="" type="checkbox"/>	smtp_connect_timeout	30s
<input checked="" type="checkbox"/>	smtpd_timeout	300s

Figure 56 - Postfix Configuration

line_length_limit

How long a line of text can be before it is broken up into pieces. All Postfix perimeter programs (SMTP server, SMTP client, local pickup and local delivery) enforce this line length limit when reading data from an untrusted source. Long lines are reconstructed upon delivery.

message_size_limit

The maximal size of a Postfix queue file, including envelope information (sender, recipient, etc.).

queue_minfree

How many bytes of free space are needed in the queue file system. The SMTP server declines inbound mail delivery requests when there is insufficient space (the mail will be accepted once enough space becomes available). There is no default limit; however, it seems like a good idea to require at least several times `$message_size_limit` so that the mail system won't get stuck on a single large message.

transport_retry_time

The amount of time between queue manager attempts to contact an apparently defunct Postfix delivery service.

stale_lock_time

How old an external lock file may be before it is forcibly removed.

allow_percent_hack

Changes the percent character to the "at" character and thus rewriting `user%domain` to `user@domain`.

fallback_relay

Hosts to hand off mail to if a message destination is not found or if a destination is unreachable.

ignore_mx_lookup_error

When a name server fails to respond to an MX query, search for an A record instead deferring mail delivery `smtp_connect_timeout` Timeout for completing a TCP connection. When no connection can be made within the deadline, the SMTP client tries the next address on the mail exchanger list.

Smtp_connect_timeout

Timeout for completing a TCP connection. When no connection can be made within the deadline, the SMTP client tries the next address on the mail exchanger list.

Smtpd_timeout

Limits the time to send a server response and to receive a client request.

TLS

TLS		
<input checked="" type="checkbox"/>	smtpd_tls_auth_only	<input type="text" value="no"/>
<input checked="" type="checkbox"/>	smtpd_tls_cert_file	<input type="text" value="/opt/insight/etc/ssl/server.pem"/>
<input checked="" type="checkbox"/>	smtpd_tls_key_file	<input type="text" value="/opt/insight/etc/ssl/server.pem"/>
<input checked="" type="checkbox"/>	smtpd_tls_CAfile	<input type="text" value="/opt/insight/etc/ssl/server.pem"/>
<input checked="" type="checkbox"/>	smtpd_use_tls	<input type="text" value="yes"/>
<input checked="" type="checkbox"/>	smtpd_enforce_tls	<input type="text" value="no"/>
<input checked="" type="checkbox"/>	smtpd_tls_cipherlist	<input type="text" value="DEFAULT"/>
<input checked="" type="checkbox"/>	smtpd_starttls_timeout	<input type="text" value="300s"/>
	smtpd_sasl_auth_enable	yes

Figure 57 - Postfix Configuration

smtpd_tls_auth_only

Setting this option to “no” will prevent passwords used for authentication from being sent on a secure channel.

smtpd_tls_cert_file

Sets the path to the TLS certificate.

smtpd_tls_key_file

Sets the path to the TLS private key.

smtpd_tls_CAfile

Sets the path to the CA Certificate.

smtpd_use_tls

Globally enables/disables TLS.

smtpd_enforce_tls

This is set to “no” by default. If changed to “yes”, the server would not be able to communicate with the clients unless they were using TLS which is configured with the appropriate certificates.

smtpd_tls_cipherlist

Under the default setting, it is the list that provides certificates when a client is authenticating with the server.

smtpd_starttls_timeout

Limits the time in seconds to write and read operations during TLS start and stop handshake procedures.

smtpd_sasl_auth_enable

Enables SASL for SMTP-AUTH checking.

smtpd_recipient_restrictions

Specifies restrictions on recipient addresses that clients can send in RCPT TO commands.

LDAP

```
LDAP

virtual_maps $alias_maps
              ldap:/opt/insight/etc/postfix/ldap-source.cf
```

Figure 58 - Postfix Configuration

virtual_maps

This value is set to the following file contents:

```
mail:/opt/insight/etc/postfix # cat ldap-source.cf
server_host = localhost
server_port = 389
timeout = 10
query_filter = (!(mailalias=%s)(mail=%s))
result_attribute = mailForward,login
special_result_attribute = member
bind_dn = cn=service
bind_pw = SAuz/EOS
```

server_host

Specifies the LDAP server

server_port

Specifies the LDAP server port

timeout

This limits the response time in seconds for search operations during a client query.

query_filter

Sets what results are returned after a query of the OpenLDAP database.

result_attribute

Sets how results are returned after a query of the OpenLDAP database.

bind_dn

This is the dn: used to bind to the LDAP server to perform queries.

bind_pw

This is the password used when binding to the LDAP server to perform queries

UCE Controls (SPAM)

New to version 4.X is the SPAM control feature. By default, none of these directives are enabled. A description of each is provided and managers have the option to enable or leave disabled (A detailed explanation can be found at <http://www.mengwong.com/misc/postfix-uce-guide.txt>).

UCE Controls (SPAM)		
<input type="checkbox"/>	header_checks	<input type="text"/>
<input type="checkbox"/>	body_checks	<input type="text"/>
<input type="checkbox"/>	smtpd_delay_reject	<input type="text" value="no"/>
<input type="checkbox"/>	smtpd_helo_required	<input type="text" value="yes"/>
<input type="checkbox"/>	maps_rbl_domains	<input type="text"/>
<input type="checkbox"/>	smtpd_helo_restrictions	<input type="text" value="permit_mynetworks, reject_invalid_h"/>
<input type="checkbox"/>	strict_rfc821_envelopes	<input type="text" value="yes"/>
<input checked="" type="checkbox"/>	smtpd_sender_restrictions	<input type="text" value="permit_sasl_authenticated"/>
<input checked="" type="checkbox"/>	smtpd_recipient_restrictions	<input type="text" value="check_sender_access ldap:/opt/insig"/>
<input type="checkbox"/>	smtpd_client_restrictions	<input type="text" value="permit_sasl_authenticated, permit_m"/>
<input type="checkbox"/>	content_filter	<input type="text" value="smtp-amavis:[127.0.0.1]:10024"/>
<input checked="" type="checkbox"/>	smtpd_restriction_classes	<input type="text" value="local_sender_only, local_recipient_of"/>
<input checked="" type="checkbox"/>	local_sender_only	<input type="text" value="check_recipient_access ldap:/opt/insig"/>
<input checked="" type="checkbox"/>	local_recipient_only	<input type="text" value="check_sender_access ldap:/opt/insig"/>

Figure 59 - Postfix Configuration

header_checks

The header_checks variable defines a regexp lookup table map. This will tell Postfix to look for the header checks file. A location of the header_checks file must be given. To enable header checks in the Postfix configuration file open the web administrator console of the Insight Server. Go to **Configuration -> Postfix -> UCE Controls (Spam)** and place a check mark on Header Checks.

In the Header_checks' open field, add the path to the map that will be used as the header check file (this is similar to hosts file in that the map does not have an extension). For example:

regexp:/etc/postfix/maps/header-checks

(Use a text editor to modify the Header Check file).

The format to follow for each line in the header-checks file is as follows:

^/HEADER: .*content_to_act_on/ ACTION.

The HEADER listed can be any header available in an email. The Subject header is the most popular way to find key words, phrases or values on which rejections will be based; however, others can be very useful as well. The X-Mailer header can be used to identify some software or mail clients that are used almost exclusively for spam.

The value that the manager wishes to filter is preceded by a period, then an asterisk. This instructs postfix to ignore everything preceding the specified characters. The following ACTION options are available:

REJECT is the most common. This will cause the email to be rejected by Postfix. The incoming email will be blocked before it can enter the user's server. As an option, text can be added after the word REJECT, whereas that text will appear in both the user's log and the bounce message to the sender of the email. A good practice is to number the lines in any check file, as the user may sometimes have difficulty identifying which rule it was that caused a particular email to be rejected. A sample reject is as follows:

`/^Subject .*Hi There/ REJECT Spam Header Rule #42`

This specifies that any email containing the words "Hi There" in the subject line will be rejected. The bounce message to the sender and user's mail log will both have the text "Spam Header Rule #42" in them. This will allow the user to more efficiently find what rule is causing problems or false rejects.

IGNORE will cause that particular header to be removed from the email, and will continue to process the email as normal.

WARN can be very useful when testing new header_check filters. An entry will be made into the mail log with a warning on the header, as well as any text that the user places after the word "WARN", just as with REJECT. It is often advisable to test new filters for a day or two with WARN before implementing them fully. This especially applies to complex rules that could have errors.

HOLD will hold the email in a hold queue, so that the system Administrator can later take action (delete or release the email). See Mail Management for instructions on how to release mail from the mail queue.

DISCARD will cause the sending server to think that the email was sent properly, but the user's Postfix server will silently discard (delete) the email. This option is for instances where the user do not want the remote person or server to know that the email was deleted.

FILTER will allow for the specification of another instance of postfix, filter, or server where to send the email. After the word FILTER, add an entry like in the transport map file of transport:nextthop. Please see the transport map documentation for more information.

As spammers have become a lot more devious in finding ways to slip emails past filters, header_checks has become much more useful in defining complex filtering schemes. Following are a few examples.

`/^Subject: .* / REJECT Spam Header Many Spaces 1`

In this example, any subject with more than eight spaces will be rejected. In normal circumstances, there are very few reasons for someone to put eight spaces in a subject. Many automated spam-sending tools and systems will add spaces at the end of a subject, and then place a code identifying the message or some other details.

```
/^Date: .* 200[0-2]/ REJECT Spam Header Past Date 1  
/^Date: .* 19[0-9][0-9]/ REJECT Spam Header Past Date 2[/b]
```

In the above examples, emails that appear to have been sent in the past (it is currently 2003 as of the time of this writing) will be rejected. Many spammers use dates far in the past (or the future) to make emails appear at the top of incoming mails list.

```
/^Subject: .*s[ _\*\-]+p[ _\*\-]+a[ _\*\-]+m/ REJECT Hidden Word 1
```

The above example shows how some spammers use different characters in between words to bypass filters. In this case, the word "spam" can be disguised with various characters in between the letters, and the header check will still reject it.

Header checks not only filter words in the subject line. They can be detailed and granular enough to catch even the strangest subject line.
(See Appendix A for an example of a Header-Check file)

body_checks

The `body_checks` variable defines a regexp lookup table map.

smtpd_delay_reject

If the client has been rejected but insists on sending mail, setting this option to NO will minimize Postfix logging.

smtpd_helo_required

Yes or No, If the smtp client fails either of these variables, it's thrown out.

smtpd_helo_restrictions

Specifies a set of restrictions that the smtp client must meet or mail will be rejected.

strict_rfc821_envelopes

Set to either Yes or No. If the smtp client fails either of these variables, mail will be rejected.

smtpd_sender_restrictions

Specifies a set of restrictions that the smtp client must meet or mail will be rejected.

smtpd_recipient_restrictions

Specifies a set of restrictions that the smtp client must meet or mail will be rejected.

ProFTP Configuration

ProFTPD is used to receive the free/busy information published by Outlook. Clients must authenticate to ProFTPD using their Insight Server uid/pwd combination to publish the free/busy information via the ftp protocol. The free/busy is saved in a directory `/opt/insight/var/ftp/freebusy` which in turn gets published via Apache for Outlook clients to retrieve using http:.

Settings

To configure ProFTPD, navigate to the ProFTPD configuration parameters by logging into the Administrator Web Console → Clicking on the "Services" option

under “Configuration” → And clicking the “ProFTPD” Option (Figure 60).

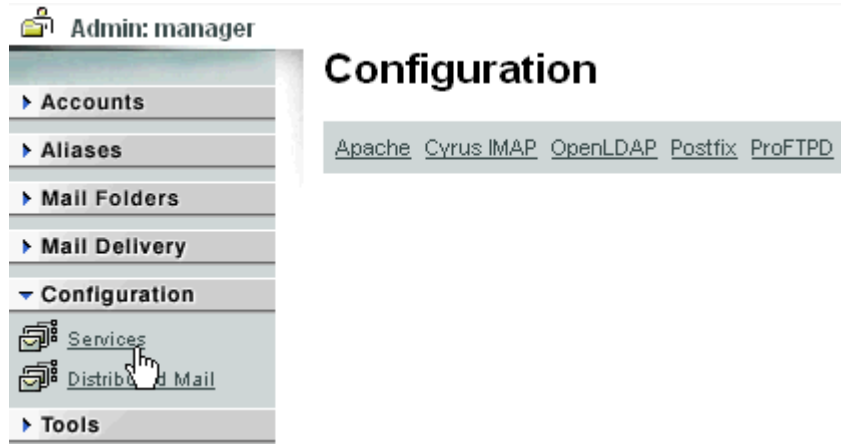


Figure 60 - Navigate to the ProFTPD configuration page (proftpd config.gif)

Settings

The following options are available:

Settings	
<input checked="" type="checkbox"/>	ServerName <input type="text" value="ProFTPD"/>
	ServerType standalone
	DefaultServer on
	RequireValidShell off
<input checked="" type="checkbox"/>	Port <input type="text" value="21"/>
<input checked="" type="checkbox"/>	Umask <input type="text" value="022"/>
	User proftpd
	Group proftpd
	DefaultRoot /opt/insight/var/ftp
	AllowOverwrite on

Figure 61 - ProFTPD Settings

ServerName

Configures the name displayed to connecting users.

AuthPam

This directive determines whether PAM is used as an authentication method by ProFTPD. By default, this feature is enabled in order to fit in with the design policy of using PAM as the primary authentication mechanism.

AuthPamConfig

This directive allows the specification of the PAM service name used in authentication. A specific service name to use when authenticating is also allowed under this option, enabling the user to configure different PAM service names to be used for different virtual hosts. The directive was renamed from PAMConfig post 1.2.0 pre10.

ServerType

Set the mode proftpd runs in.

DefaultServer

Set the default server.

RequireValidShell

Allow connections based on /etc/shells.

Port

Setup and Configuration Guide

Set the default port to listen.

Umask

Set the default Umask.

User

Set the user the daemon will run as.

Group

Set the group the daemon will run in.

DefaultRoot

Sets default chroot directory.

AllowOverwrite

Enable files to be overwritten.

Performance

Performance		
<input checked="" type="checkbox"/>	MaxInstances	<input type="text" value="30"/>
<input checked="" type="checkbox"/>	UseReverseDNS	<input type="text" value="off"/>
<input type="checkbox"/>	IdentLookups	<input type="text" value="on"/>
<input type="checkbox"/>	TimeoutLogin	<input type="text" value="120"/>
<input type="checkbox"/>	TimeoutIdle	<input type="text" value="600"/>
<input type="checkbox"/>	TimeoutNoTransfer	<input type="text" value="900"/>
<input type="checkbox"/>	TimeoutStalled	<input type="text" value="300"/>
<input checked="" type="checkbox"/>	MaxClients	<input type="text" value="10"/>
	Include	<input type="text" value="/opt/insight/etc/proftpd.inc ldap"/>
	Include	<input type="text" value="/opt/insight/etc/proftpd.inc standard"/>
<input checked="" type="checkbox"/>	Include	<input type="text" value="/opt/insight/etc/proftpd.inc anonymous"/>

Figure 62 - ProFTPD Performance

MaxInstances

Sets the maximum number of child processes to be spawned.

UseReverseDNS

Toggle rDNS lookups.

IdentLookups

Toggle ident lookups.

TimeoutLogin

Sets the login timeout.

TimeoutIdle

Sets the idle connection timeout.

TimeoutNoTransfer

Sets the connection without transfer timeout.

TimeoutStalled

Sets the timeout on stalled downloads MaxClients Limits the number of users that can connect.

LDAP

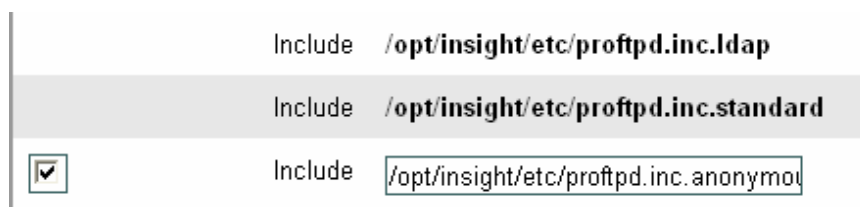


Figure 63 - ProFTPD LDAP

Include

This value is set to the following file contents:

```
mail:/opt/insight/etc # cat proftpd.inc.ldap
LDAPServer localhost
LDAPUseTLS off
LDAPDoAuth on "" (login=%v)
LDAPDNInfo "cn=service" "SAuz/EOS"
LDAPDefaultUID 400
LDAPDefaultGID 400
LDAPDefaultAuthScheme clear
LDAPAuthBinds on
LDAPDoUIDLookups off
LDAPForceDefaultGID on
LDAPForceDefaultUID on
LDAPHomedirOnDemand off
LDAPHomedirOnDemandPrefix /opt/insight/var/ftp
#LDAPNegativeCache on
```

LDAPServer

LDAPServer allows the user to specify the hostname(s) and port(s) of the LDAP server(s) to use for LDAP authentication. If no LDAPServer configuration directive is present, the default LDAP servers specified by the user's LDAP API will be used.

LDAPUseTLS

By default, mod_ldap connects to the LDAP server via a non-encrypted connection. Enabling this option causes mod_ldap to use an encrypted (TLS/SSL) connection to the LDAP server. If a secure connection to the LDAP server fails, mod_ldap will not authenticate users (mod_ldap will *not* fall back to an unsecured connection).

LDAPDoAuth

This configuration directive activates LDAP authentication. The second argument

to this directive is the LDAP prefix to use for authentication. The third argument is a template to be used for the search filter; %v will be replaced with the username that is being authenticated. By default, the search filter template "((&(uid=%v)(objectclass=posixAccount))" is used. Search filter templates are only supported in mod_ldap v2.7 and later versions.

LDAPDNInfo

This directive specifies the LDAP DN and password to use when binding to the LDAP server. If this configuration directive is not specified, anonymous binds are used.

LDAPDefaultUID

This directive is useful primarily in virtual-user environments common in large-scale ISPs and hosting organizations. If a user does not have a LDAP uidNumber attribute, the LDAPDefaultUID is used. This allows a user to have a large number of users in an LDAP database without uidNumber attributes; setting this configuration directive will automatically assign those users a single UID.

LDAPDefaultGID

This directive is useful primarily in virtual-user environments common in large-scale ISPs and hosting organizations. If a user does not have a LDAP uidNumber attribute, the LDAPDefaultUID is used. This allows a user to have a large number of users in an LDAP database without uidNumber attributes; setting this configuration directive will automatically assign those users a single UID.

LDAPDefaultAuthScheme

Specifies the authentication scheme used for passwords with no {prefix} in the LDAP database. For example, if the user uses userPassword: mypass in the LDAP database, the LDAPDefaultAuthScheme should be set to clear.

LDAPAuthBinds

By default, the DN specified by LDAPDNInfo will be used to bind to the LDAP server to obtain user information, including the userPassword attribute. If LDAPAuthBinds is set to on, the DN specified by LDAPDNInfo will be used to fetch all user information except the userPassword attribute. Then, mod_ldap will bind to the LDAP server as the user who is logging in via FTP with the user-supplied password. If this bind succeeds, the user is considered authenticated and is allowed to log in. This method of LDAP authentication has the added benefit of supporting any password encryption scheme supported by the LDAP server.

LDAPDoUIDLookups

This configuration directive activates LDAP UID-to-name lookups in directory listings. The second argument to this directive is the LDAP prefix to use for UID-to-name lookups. The third argument is a template to be used for the search filter; %v will be replaced with the UID that is being looked up. By default, the search filter template "((&(uidNumber=%v)(objectclass=posixAccount))" is used. Search filter templates are only supported in mod_ldap v2.7 and later.

LDAPForceDefaultGID

Even with a LDAPDefaultGID configured, mod_ldap will allow individual users to have gidNumber attributes that will override this default GID. With LDAPForceDefaultGID enabled, all LDAP-authenticated users are given the default GID. GIDs may not be overridden by gidNumber attributes.

LDAPForceDefaultUID

Even with a LDAPDefaultUID configured, mod_ldap will allow individual users to have uidNumber attributes that will override this default UID. With LDAPForceDefaultUID enabled, all LDAP-authenticated users are given the default UID. UIDs may not be overridden by uidNumber attributes.

LDAPHomedirOnDemand

LDAPHomedirOnDemand activates on-demand home directory creation. If a user logs in without a created home directory, one is created automatically.

In mod_ldap <= 2.7.6, the home directory will be owned by the same user and group that ProFTPD runs as (see the User and Group configuration directives). mod_ldap >= 2.8 can create home directories for users with any UID/GID, not just those with the same UID/GID as the main ProFTPD server.

The second argument allows a user to specify the mode (default permissions) to use when creating home directories on demand, subject to ProFTPD's umask (see the Umask directive). If no directory mode is specified, the default of 0755 is used. Directory mode setting is only supported in mod_ldap v2.7 or later.

LDAPHomedirOnDemandPrefix

LDAPHomedirOnDemandPrefix enables a prefix to be specified for on-demand home directory creation. This is most useful if mod_ldap is being used to authenticate against an LDAP directory that does not return a homeDirectory attribute, either because it cannot (Microsoft Active Directory, for example) or because the user does not wish to extend the existing directory schema. For example, setting this directive to "/home" and logging in as the user "joe" would result in his home directory being created as "/home/joe". The directory will be created with the mode specified in LDAPHomedirOnDemand. To use this directive, LDAPHomedirOnDemand must be enabled.

LDAPNegativeCache

LDAPNegativeCache specifies whether or not to cache negative responses from the LDAP server when using LDAP for UID/GID lookups. This option is useful if the user also uses (or is in transition from) another authentication system; if there are many users in the old authentication system who are not in the LDAP database, there can be a significant delay when a directory listing is performed as the UIDs not in the LDAP database are repeatedly accessed in an attempt to present usernames instead of UIDs in directory listings. With LDAPNegativeCache set to on, negative ("not found") responses from the LDAP server will be cached and speed will improve on directory listings that contain many users who are not present in the LDAP database.

Include

This value is set to the following file contents.

```
mail:/opt/insight/etc # cat proftpd.inc.standard
<Directory /*>
  <Limit WRITE>
    DenyAll
  </Limit>
</Directory>
<Directory /opt/insight/var/ftp/freebusy>
  <Limit READ WRITE>
    DenyAll
  </Limit>
  <Limit STOR>
    AllowAll
  </Limit>
</Directory>
```

These entries set the permissions for users authenticated against the LDAP server.

Include

This value is set to the following file contents.

```
mail:/opt/insight/etc # cat proftpd.inc.anonymous
<Anonymous /opt/insight/var/ftp>
  User proftpd
  Group proftpd
  UserAlias anonymous proftpd
  UserAlias ftp proftpd
  RequireValidShell off
<Directory *>
  <Limit WRITE>
    DenyAll
  </Limit>
</Directory>
<Directory freebusy>
  <Limit READ WRITE>
    DenyAll
  </Limit>
  <Limit STOR>
    AllowAll
  </Limit>
</Directory>
</Anonymous>
```

These entries provide anonymous access to the ftp server which is often used by Outlook 2000 Clients. To disable anonymous access to the ftp server deselect this option. You would then need to configure the Outlook 2000 clients to use the appropriate uid/pwd combination. Please refer to the Insight Connector documentation for these settings.

LDAP Replication

Insight Server now supports the authentication of accounts against third party LDAP servers like Active Directory for authentication. These accounts are also replicated into Insight Servers local OpenLDAP instance so that the users can gain full access to all available features. The accounts that are created are read only and can not be modified through the web admin interface.

It is important to note that although the account information is replicated locally the password information is not. Passwords are not extracted and replicated between servers. When ever an incoming authentication request is made against a replicated account, the SASL Auth Daemon redirects the authentication attempt to the third party LDAP server. Successful authentication is determined via the success of an LDAP bind using the credentials provided.

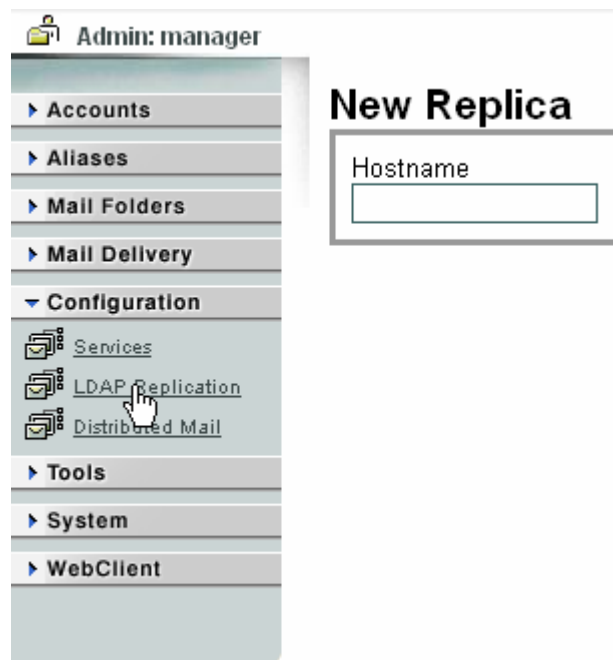


Figure 64 – LDAP Replication

When setting up the replication sequence an account must be specified for use when binding to the LDAP service. This account must have access to the full schema for Insight Server to perform an ldapsearch of the entire server. In the following example we will use the Administrator account for this purpose.

Let's examine the information needed when adding an Active Directory server as a New Replica.

New Replica

Hostname <input type="text"/>	Port <input type="text"/>	Administrative DN <input type="text"/>	Password <input type="text"/>	LDAP Suffix <input type="text"/>	<input type="button" value="Add"/>
----------------------------------	------------------------------	---	----------------------------------	-------------------------------------	------------------------------------

Figure 65 – New Replica

Hostname	IP Address or Fully Qualified Domain Name (FQDN)
Port	Default of 389 for LDAP and 3268 for Active Directory
Administrative DN	This is the Bind DN used during replication
Password	This is the Bind Password used during replication
LDAP Suffix	Default search string used during replication

Now let's examine the steps we use to determine the information used for the New Replica entry. The Hostname must be the IP Address or FQDN and in our case it will be "192.168.30.123". Since we are adding an Active Directory server as our Replica we will be using port "3268" for our example. If we were setting up an LDAP server using a Samba schema as our New Replica partner we would most likely be using port 389.

Now that we have our connection information, we will determine our Administrative DN and LDAP Suffix to complete our example New Replica entry. To do this, open a shell on the server as root. The following command is used to determine administrator accounts full DN as well as the LDAP Suffix.

```
# /opt/insight/bin/ldapsearch -x -h [ip address of the ldap server] -p 3268|more
```

Here is the initial result listing of this command in our example configuration.

```
[root@mail2 root]# /opt/insight/bin/ldapsearch -x -h 192.168.30.123 -p 3268|more
# extended LDIF
#
# LDAPv3
# base <> with scope sub
# filter: (objectclass=*)
# requesting: ALL
#
# example.net
dn: DC=example,DC=net
...

```

Given the 'dn:' results from our example configuration we now know that our LDAP Suffix will be "CN=Users, DC=example,DC=net".

Using the LDAP Suffix we can then determine the administrator accounts full DN by pre-pending "CN=Administrator," to the LDAP Suffix.

The Administrator DN is now "CN=Administrator,CN=Users, DC=example,DC=net". To validate the information gleaned from these results you can use the following command.

```
# /opt/insight/bin/ldapsearch -x -h [ip address of the ldap server] -p [port] \
-D "[Bind DN]" -w [Bind Password] -b '[LDAP Suffix]'
```

This command will produce a user listing from LDAP that will be used by the replication routine for creating the accounts. Below is the command line from our example configuration and the initial results.

```
[root@mail2 root]# /opt/insight/bin/ldapsearch -x -h 192.168.30.123 -p 3268 \
> -D "CN=Administrator,CN=Users,DC=example,DC=net" -w password \
> -b 'CN=Users,DC=example,DC=net'|more
# extended LDIF
#
# LDAPv3
# base <CN=Users,DC=example,DC=net> with scope sub
# filter: (objectclass=*)
# requesting: ALL
#
# Users, example.net
dn: CN=Users,DC=example,DC=net
cn: Users
description: Default container for upgraded user accounts
dSCorePropagationData: 20050411163721.0Z
dSCorePropagationData: 16010101000001.0Z
instanceType: 4
distinguishedName: CN=Users,DC=example,DC=net
objectCategory: CN=Container,CN=Schema,CN=Configuration,DC=example,DC=net
```

We can now populate the fields in the New Replica entry with this information then select Add.

Distributed Mail

Insight Server can be configured for load sharing and limited redundancy by creating a slave server (or servers). The slave server(s) will have a copy of the original configuration from the master. In the event of the master failing, the slave will continue to be functional. A master server has to be established by selecting the role in the selection screen. The slave server communicates with the master when a user account is created on the slave to prevent duplication. The order in which the master/slave configuration is set is critical. If a step is missed or if a mistake is made during configuration, it may not be readily apparent but may manifest itself at a later time as an error. If events are not proceeding normally during this process, it may be best to make a backup of all user data and reinstall the servers.

Single Role

All user email data and login information reside on a single server. This is Insight Server's default role upon installation.

Master Role

In the master/slave roll all the accounts (LDAP database) are stored on the master server and all the email data on the slave server. The master maintains user information in the LDAP directory which is for email authentication. The master server accepts the logon and redirects the request to the slave to retrieve email data. Users can log into the slave server but will not be able to share contacts with every one listed on the master server, only users on the slave server. The master server can have multiple slave servers and the user load distributed among the slaves. When adding a user a choice is given to which slave server the user account must be created.

Slave Role

The Slave server maintains all the email data that is directed from the master. The slave server polls the master server for all the data and user accounts created. The master polls the slave when user accounts are created on the master.

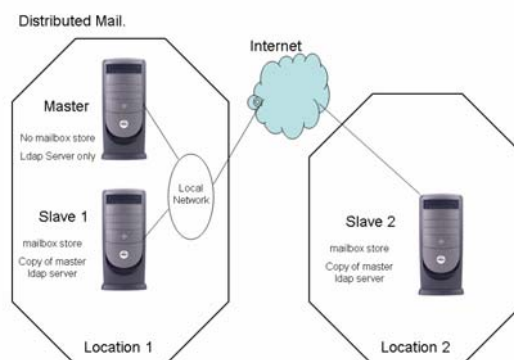


Figure 66 - Distributed Mail

Steps for creating a Master/Slave with a **fresh installation** of Insight Server on all mail servers (domains, organizations, or users have NOT been created) include:

N.B: The first location will use 2 servers to setup master/slave distributed mail system; the master is the LDAP server where all the account information is kept which distributes the LDAP information to the slaves and vice versa if an account is setup on the slaves.

1. Install each server normally as if it is a stand alone server.
2. Before creating any organizations or domains, perform the following steps:
 - a. On the server that will serve as the master, click distributed mail.
 - b. In the box that specifies "type", change this to master and click "set".
 - c. On the server that will be the slave, click distributed mail.
 - d. In the box that specifies "type", change this to slave and click "set".
 - e. On the master server, type in the name (this must be the Fully Qualified Domain Name [FQDN]) of the slave server in the host name box. Type in "manager " in

the username box and enter the password in the “password” box, then click “add”. (A screen appears which shows that the slave is set and instead of an “add” button it will have “modify” and “delete”. There will also be the option to add more slave servers.)

- f. On the slave server, type in the name (FQDN) of the master server in the host name box, type in “manager “ in the username box and enter the password in the “password” box, then click “add”. (A screen appears which shows that the slave is set and instead of an “add” button it will have “modify” and “delete”. There will not be an option to add any more master servers.)
3. Perform normal administrator functions.

Steps to create a Master/Slave with an **existing installation** of Insight Server on all mail servers (domains, organizations, or users have been created) include:

1. Backup the configuration, LDAP and Mail on all servers.
2. Download the LDAP and Mail backups of the Master Server to the user’s workstation.
3. Upload the LDAP and Mail backup files to the slave server(s).
4. Restore the LDAP and Mail backups on the slave server(s).
5. Perform the following steps as in the first scenario;
 - a. On the server that will be the master, click “distributed mail”.
 - b. In the box that specifies “type”, change this to master and click “set”.
 - c. On the server(s) that will be the slave(s), click “distributed mail”.
 - d. In the box that specifies “type”, change this to slave and click “set”.
- e. On the master server, type in the name (this must be the Fully Qualified Domain Name [FQDN]) of the slave server in the host name box, type in “manager “ in the username box and enter the password in the “password” box, then click “add”. (A screen appears which shows that the slave is set and instead of an “add” button it will have “modify” and “delete”. There will also be the option to add more slave servers.)
- f. On the slave server, type in the name (FQDN) of the master server in the host name box, type in “manager “ in the username box and enter the password in the “password” box, then click “add”. (A screen appears which shows that the slave is set and instead of an “add” button it will have “modify” and “delete”. There will not be an option to add any more master servers.)
6. Perform normal administrator functions.

Tools

This section contains the system tools.

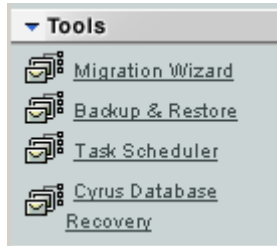


Figure 68 - Tools Menu

Migration Wizard

This section explains how to migrate users and their mail from Insight Server 4.0 or from Microsoft Exchange Server. For instructions on upgrading Insight Server from 4.0 to 4.2 on a machine please refer to the Installation and Upgrade document for Insight Server 4.2.

Note: Before performing any migration or upgrade, it is recommended to have two verified and viable backups of both MAIL and LDAP.

Note: When migrating the mail store from a previous installation of Insight Server 4.0 not on the same server messages receive a new IMAP message id in the new installation if IS 4.2. This means that you must have all clients create a clean PST file in Outlook to avoid duplication of message store contents.

Note: If migrating from Exchange 5.5, ensure that the Administrator or Service Account for Exchange does not have a blank password.

Network Migration from Insight Server 4.0 to Insight Server 4.2

1. Install the new version of Insight Server (Refer to Installation Chapter).

Note: Ensure that the server is registered with your new license and set the password for the manager account.

2. Login to the Web Admin interface as manager and navigate to 'Tools' then 'Migration Wizard' as shown in figure 68 above.

Migration Wizard

Option 1

Specify Existing Server Type Bynari Insight Server 4

Hostname/IP or Full Path For example, mail.domain.com, or /opt/insight

Next

Figure 69 –Migration Wizard Option1

3. In the Migration Wizard under Option 1 we start with Step 1 of the Network Migration. Specify the existing server type of 'Bynari Insight Server 4' as show in Figure 69 above.
4. Enter the IP address or FQDN (i.e.: 192.168.1.5 or mail1.example.com) of the original IS 4.0 server then select 'Next'.
5. In Step 2 provide the manager account name and password for previous installation of Insight Server4.0. The LDAP Search Base Country Code should be left blank in most circumstances. Select 'Next' once completed.
6. The migration wizard will then list all Organizational Units, Groups and Accounts found in the LDAP database as shown below in Figure 70.

Migration Wizard

Step 3

Please make sure what you want to migrate is checked.

- Import all Top Level Shared folders

- o=example.com
- cn=John Doe,o=example.com (jdoe)
- cn=Mark Smith,o=example.com (msmith)
- cn=Cathy Marshall,o=example.com (cmarshall)
- cn=David Rich,o=example.com (drich)
- cn=Mary Rose,o=example.com (mrose)
- cn=Nancy Cane,o=example.com (ncane)

Migrate

Figure 70 –Migration Wizard

7. By default all check boxes are checked. At this time you can deselect any Accounts or Organizations you do not wish to migrate. Once completed select the "Migrate" button at the bottom of the page.

Note: If you deselect the organizational unit and not the users in that Organization then you will receive errors after proceeding to the next page. These errors will state that the users could not be created on the new server. If you do not wish to migrate a specific Organizational Unit also deselect the users belonging to that unit as well.

8. A successful operation will result in a list of accounts created migrated and once completed "Done" will appear at the bottom of the page. Shared Folders, Organizational Units, Groups, and Accounts should now be migrated to the new server.

Server to Server Migration from an installation of Exchange Server

1. Install the new version of Insight Server (Refer to Installation Chapter).

Note: Ensure that the server is registered with your new license and set the password for the manager account.

2. Login to the Web Admin interface as manager and navigate to 'Tools' then 'Migration Wizard' as shown in figure 70 above.

Option 1

Specify Existing Server Type	Microsoft Exchange	
Hostname/IP or Full Path	<input type="text"/>	For example, mail.domain.com, or /opt/insight

Next

Figure 71 –Migration Wizard

3. The Migration Wizard will start now with Step 1. Specify the existing server type (Refer to Figure 71 above) as Microsoft Exchange Server.
4. Enter the IP address or FQDN of the Microsoft Exchange server then select 'Next'

Step 2

Migrating from server 192.168.3.145	
Administrative DN	Administrator
Administrative password	<input type="text"/>
Confirm password	<input type="text"/>
LDAP Suffix	<input type="text"/>

Next

Figure 72 –Migration Wizard: Exchange Step 2

5. Provide the Administrative DN which is generally Administrator or service account name and password for Exchange Server.

Note: The Exchange Server must have a password in order for Insight Server Migration Wizard to work. It will reset back to Step 1 if no password is supplied during this step.

The final field to be entered is the LDAP Suffix. When migrating from an Exchange 5.5 server this field can be left blank. This field is generally only during Exchange 2000 server migrations.

To find out what LDAP Suffix should be used for an Exchange 2000 Server, open a shell on the Insight Server and login as root to run the following commands. The example shown here assumes that the IP address of the Exchange server is 192.168.3.155.

```
# /opt/insight/bin/ldapsearch -x -h 192.168.3.155 -p 3268|more
```

```
// this returns the following output...
```

```
# extended LDIF
#
# LDAPv3
# base <> with scope sub
# filter: (objectclass=*)
# requesting: ALL
#
# exchsvr.example.com
dn: DC=exchsvr,DC=example,DC=com
...
```

Now take above dn: information and add CN=Users, to the beginning of this line. You now have the LDAP Suffix entry to be used for the migration process.

```
CN=Users,DC=exchsvr,DC=example,DC=com
```

6. Click "Next".

Migration Wizard

Step 3

Please make sure what you want to migrate is checked.

- CN=jdoe,CN=Users,DC=exchsvr,DC=example,DC=com
- CN=Administrator,CN=Users,DC=exchsvr,DC=example,DC=com
- CN=TsInternetUser,CN=Users,DC=exchsvr,DC=example,DC=com
- CN=cmarshall,CN=Users,DC=exchsvr,DC=example,DC=com
- CN=mrose,CN=Users,DC=exchsvr,DC=example,DC=com
- CN=drich,CN=Users,DC=exchsvr,DC=example,DC=com

Migrate

7. The migration wizard will import all LDAP entries into Insight Server and then provide instructions on how to use EXMerge (available from Microsoft) to export the user's Exchange mailboxes to .PST files.

Note: This step will create a PST for each user that will be imported using the Insight Server Migration Wizard using ExMerge provided by Microsoft. This is not the same PST that the user may be using on the workstation in Outlook. The user must start with a NEW PST after migrating to Insight Server. If the user continues with the previous Outlook PST, there is a possibility of duplicate or lost e-mail.

8. Browse to the location of the zip or tar file with the PST files to be uploaded (imported) and click next.
9. A successful operation will result in "Done" shown at the bottom of the page.

Option 2

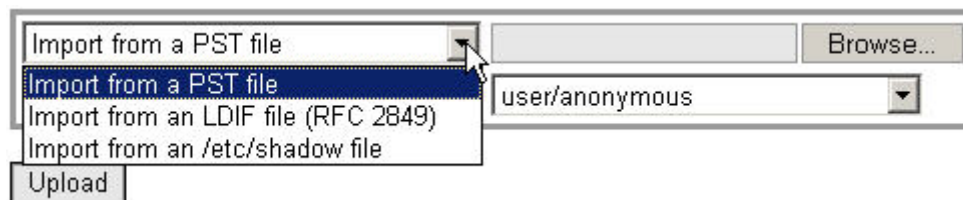


Figure 73 - Option 2 format Selection

Importing from a PST file

To import a PST file from Outlook, click on browse and pick this file from the hard drive, then select which IMAP folder in which the contents of the PST file will go. Click the Upload button to continue.

Importing from an LDIF file (RFC 2849)

To import LDAP entries from an LDIF file, simply click on browse and pick this file from the hard drive. Click *Upload* afterwards to continue. There is no need to pick an IMAP folder as it does not apply to an LDIF import.

An example of the LDIF format for the Insight Server follows. (This is the minimum information required to create the user):

```
# FirstName MiddleName LastName, LDIF
dn: cn=FirstName MiddleName LastName, o=LDIF
cn: FirstName MiddleName LastName
objectClass: insightPerson
login: user-idlogin
sn: LastName
mail: emailaddress@domain.com
userPassword: password
```

All the fields used in the LDIF format are:

```
# FirstName MiddleName LastName, LDIF
dn: cn=FirstName MiddleName LastName, o=LDIF
cn: FirstName MiddleName LastName
objectClass: insightPerson
login: login
givenName: FirstName
initials: MiddleName
sn: LastName
mail: emailaddress@domain.com
mailalias: mailAlias@domain.com
mailForward: Emailforwarding@otherdomain.com
display-name: DisplayName
homePhone: HomePhone 555-555-5555
homePostalAddress: HomePostalAddress
postalAddress: PostalAddress
postOfficeBox: PostOfficeBox
street: Street
l: City
st: State
postalCode: PostalCode
telephoneNumber: TelephoneNumber
facsimileTelephoneNumber: FacsimileTelephoneNumber
mobile: MobileNumber
pager: PagerNumber
businessCategory: BusinessCategory
departmentNumber: DepartmentNumber
employeeNumber: EmployeeNumber
employeeType: EmployeeType
title: Title
roomNumber: RoomNumber
physicalDeliveryOfficeName: PhysicalDeliveryOfficeName
registeredAddress: RegisteredAddress
labeledURI: LabeledURI
```

preferredLanguage: PreferredLanguage
userSMIMECertificate: UserSMIMECertificate
userPKCS12: UserPKCS12
destinationIndicator: DestinationIndicator
telexNumber: TelexNumber
description: Description
userPassword::
e1NTSEF9NnRFZIJGVS9xb0dCVzAvaHd3MnA2Z3hPWjVKQUMwazY

To learn more about LDIF: LDAP Data Interchange Format please follow this link [more...](#)

Importing from an /etc/shadow file

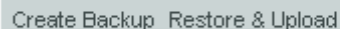
If there are e-mail users set up as system users on a previous mail server, grab the /etc/shadow file from that machine as the user root and put it somewhere on the hard drive. Then select the file by clicking browse and click Upload. Picking an IMAP folder is not required for this type of import.

Backup & Restore

Creating a Backup

When placing the cursor on the Backup and Restore hyperlink, a “floating” choice box will appear to enable the creation of a backup or restore a backup. Click on *Backup & Restore* to go to the main “backup” section (Figure X). A description of each choice follows.

Backup & Restore



[Create Backup](#) [Restore & Upload](#)

Figure 74 - Backup & Restore

Place the cursor on either the *Create Backup* or *Restore & Upload* hyperlink to see a description box, as illustrated below.

Create Backup File

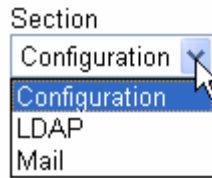


Figure 75 - Selecting the section to backup

The user can select which section of the server to backup: Configuration, LDAP database or the Mail store.

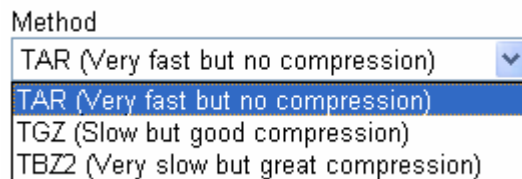


Figure 76 - Selecting the method when backing up

Select the section to backup and then select the type of file format Then click the Backup button.

A list of all the files that were backed up will be displayed when the backup procedure is selected, allowing the user to select which files need to be restored.

The different files that are created include the following:

Configuration (files of Apache, ProFTP, Postfix)

The file name listed is *cfg_date_time.compressiontype*

LDAP (files which are the used by the LDAP server)

The file name listed is *ldap_date_time.compressiontype*

Mail Data file (all the mailboxes used by the server)

The name listed in *mail-date_time.compressiontype*

To list all of the files that are available to restore after creating a backup, proceed to the next section.

Restoring

List of backup files

Filename	File Size	File Date	File Time			
cfg-051106_0615.tgz	13564	Nov 6	06:15	Delete	Download	Restore
cfg-051105_0615.tgz	13564	Nov 5	06:15	Delete	Download	Restore
mail-051105_0430.tgz	74093	Nov 5	04:30	Delete	Download	Restore
cfg-051104_0615.tgz	13564	Nov 4	06:15	Delete	Download	Restore
ldap-051104_0530.tgz	74866	Nov 4	05:30	Delete	Download	Restore
cfg-051103_0615.tgz	13564	Nov 3	06:15	Delete	Download	Restore

Figure 77 - List of files for Restore

To restore the configuration, LDAP or Mail store, click on Restore and Upload. A list of all backup files will appear. There are three available options: delete, download and restore.

Delete: Allows the user to purge older backups that are no longer need and free up disk space for new backups.

Download: Allows the user to save or transfer backup files to another location or computer. This may be done for purposes of archiving, rebuilding or setting up a slave.

Restore: Restoring configuration files will over write the existing files on the system. When restore is selected and the files are displayed that were created to select for restoration. The files are the configuration files for Apache, LDAP, Proftpd, and Postfix.

When restoring the mail store, a list box appears displaying all users that can be restored. The users' mailbox will be restored as a whole; individual file cannot be selected by the web interface. After mail has been restored, Insight Server automatically reconstructs the users' folders. The system message is returned, stating that the mailbox has been reconstructed. (This is the Cyrus command to rebuild the databases used by Cyrus.)

Uploading

Below the list of backup files is a button and a file field for uploading backup files. These files can be uploaded to the server for the purpose of restoring. Select "browse" to select the file to upload and it will be displayed and then select the file in the restore screen to restore, and click "Upload". A message will display to confirm file restoration.

Task Scheduler

Scheduled tasks can be set under this option to backup the server configuration, the LDAP configuration, and the mail store. Scheduled times to rotate the apache authentica-

tion logs and clean up any temporary files can also be established.

Server - 6 jobs

Disabled	Minute	Hour	Day of Month	Month	Day of Week	File location
<input type="checkbox"/> Remove old backups	15	4	15	Every	Every	/opt/insight/htdocs/is4web/cron/serve

Custom	Minute	Hour	Day of Month	Month	Day of Week	File location
<input type="checkbox"/> Resource Manager	0,10,20,30,40,50 * * * *					/opt/insight/bin/resourcemgr.sh

Daily	Minute	Hour	Day of Month	Month	Day of Week	File location
<input type="checkbox"/> Backup Configuration	15	6	Every	Every	Every	/opt/insight/htdocs/is4web/cron/run-s
<input type="checkbox"/> Run AD/LDAP Synchronization/Replication	45	6	Every	Every	Every	/opt/insight/htdocs/is4web/bin/ldapsy

Weekly	Minute	Hour	Day of Month	Month	Day of Week	File location
<input type="checkbox"/> Backup LDAP Accounts	30	5	Every	Every	Fri	/opt/insight/htdocs/is4web/cron/run-s
<input type="checkbox"/> Backup User Mailboxes	30	4	Every	Every	Sat	/opt/insight/htdocs/is4web/cron/run-s

Figure 78 - Scheduled Tasks

Here an administrator is able to set how often a given task runs. The format used here is the same format used in creating scheduled tasks through the Linux crontab.

The concept to understand here is that until a field is set then “every” is assumed. This means when the minute field is set then the task becomes an hourly event occurring each time that minute passes. When the hour field is set then that task becomes a daily event occurring each time that hour passes.

You can continue this process for each field remaining. Day of Week becomes weekly, Day of Month becomes monthly, and finally setting the Month makes the event yearly.

To see an example of an event that occurs every 10 minutes see the task titled Custom.

Occurrence	Minute	Hour	Day of Month	Month	Day of Week	File location
Disabled						
Name	Every	Every	Every	Every	Every	
<input type="button" value="Create"/>						

Figure 79 – Create Scheduled Tasks

Available options include Disabled, Hourly, Daily, Weekly, or Monthly. Simply set the interval for each option and then click “update”.

Cyrus Database Recovery

Cyrus database recovery will reconstruct the entire Cyrus database. This option will be used when users and or the system appears to have folders that cannot be deleted or removed by the user, and efforts to reconstruct the email is not successful. **Please note the warnings below in performing this function as to prevent the possible deletion of emails.**

Warning!

Please backup your mail data before continuing. This operation is not undoable.

This operation performs the following

- Recreate mailbox database
- Remove old site-wide database files
- Reconstruct all mailboxes



Figure 80 - Cyrus Warning

Select Continue to rebuild the database and restart Cyrus. A message will appear to confirm task completion.

Stopping Cyrus IMAP...

Performing recovery operations...

- Recreate mailbox database
- Remove old site-wide database files
- Reconstruct all mailboxes

... list of Cyrus IMAP folders appears here ...

Starting Cyrus IMAP...

Done

Figure 81 - Database Recovery

System

Statistics

The feature enables the Administrator/Manager to check statistics regarding Insight Server and can be helpful with planning and maintenance activities. The statistics page is illustrated in the table below.

Statistics

Metrics are available for Insight Server Inventory as well as both the Postfix and Cyrus IMAP services. Select the appropriate item from the Statistics page to view additional details.

Statistics

[Inventory](#) [Postfix](#) [Cyrus IMAP](#)

Figure 82 – Statistics

Inventory

The initial load page for statistics is the Insight Server Inventory. Total number of user, administrator, and resource accounts are displayed as well as the total number of mailboxes complimented by the listing of account mailboxes without activity for the last 30 days.

Inventory

Number of entries in user directory	9
Number of administrator accounts	1
Number of user accounts	7
Number of resource accounts	1
Number of mailboxes on system	9
Mailboxes with no activity over the last 30 days	alluser cmarshall drich exampleuser jdoe mrose msmith ncane user1

Figure 83 - Inventory

Postfix

The following metrics are tracked for the Postfix service and displayed in Daily, Weekly, Monthly, and Yearly Graphs.

Sent – Total number of messages successfully sent through the SMTP process.

Received – Total number of messages successfully received for local delivery by the SMTP agent.

Rejected – Total number of messages rejected by the server. Reasons that email might be rejected include message size limit exceeded or matching rules in header checks or body checks.

Bounced – Total number of bounce messages sent by the server. Bounce messages are generated when the server is unable to deliver an email message. The most common bounce is generated when a user account is unknown.

Viruses – Total number of emails containing a virus identified by ClamAv via the Amav-

isd-New content filters.

Spam – Total number of email messages identified as Spam by either Spamassassin or Razor used by the Amavisd-New content filter.

Postfix

Day Graphs



Figure 84 - Postfix

Cyrus IMAP

The primary metrics tracked for the Cyrus services are logins for the various services and displayed in Daily, Weekly, Monthly, and Yearly Graphs. The service tracked are POP3, IMAP, POP3-SSL, and IMAP-SSL

Cyrus IMAP

Day Graphs

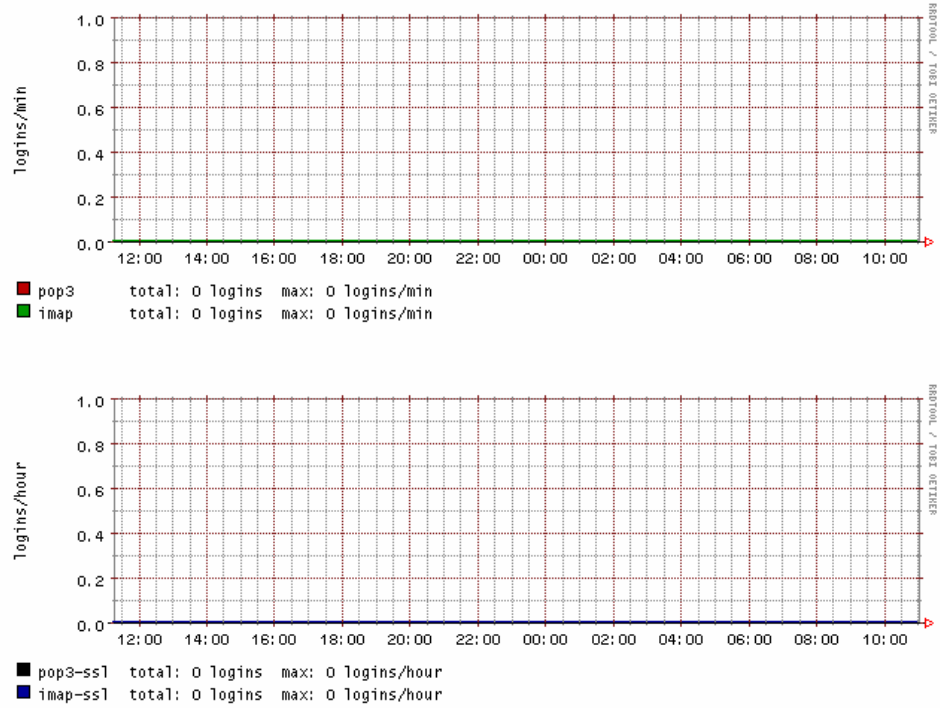


Figure 85 – Cyrus IMAP

Logging

This feature assists the Administrator/manager in efforts to troubleshoot components and attain an understanding of which. To access the logging menu, click on the logging hyperlink (Figure 85). A list of the log files will be shown. A description of each log file is provided below.

Admin: manager

- ▶ Accounts
- ▶ Aliases
- ▶ Mail Folders
- ▶ Mail Delivery
- ▶ Configuration
- ▶ Tools
- ▼ System
 - Statistics
 - Logging
 - Registration
 - Connector Access
- ▶ WebClient

	Log file	Lines	Size
<input type="checkbox"/>	/opt/insight/logs/access_log	31452 lines	7468142b
<input type="checkbox"/>	/opt/insight/logs/current	114716 lines	7446183b
<input type="checkbox"/>	/opt/insight/logs/error_log	1670 lines	69012b
<input type="checkbox"/>	/opt/insight/logs/ssl-access_log	0 lines	0b
<input type="checkbox"/>	/opt/insight/logs/ssl-error_log	0 lines	0b
<input type="checkbox"/>	/opt/insight/logs/ssl_engine_log	45 lines	4107b
<input type="checkbox"/>	/opt/insight/logs/ssl_request_log	0 lines	0b

View Selected

Search Case insensitive

Figure 86 - Logging

To view a log file, select the file to be displayed, select 'View Selected' and the file will display on the web browser. A search can be performed on the selected log file(s) by entering key words to look for in the open field at the bottom of the display and clicking "search".

One primary difference between IS 4.2 and previous versions is that we no longer log to syslogd. This means that administrators look to the log files located in /opt/insight/logs. The primary log file for Insight Server is /opt/insight/logs/current.

Registration

This screen appears when Insight Server is installed for the first time. A license key is required for this process. Enter the license key, or chose the 30-day evaluation mode if a license key is not available. If the product fails to register, manual validation may be required.

Normally, the license key is verified via the Internet, through port 80 or 3080, to the Bynari Key Validation Servers. The key is verified and if valid, the product is registered. (User can ping <http://register.bynari.net> to check for connectivity).

If the server resides behind a proxy server, the user has the option to configure the following settings in order to register properly. (See Figure 86).

- I hereby acknowledge that this license contains the complete and exhaustive list of the terms of the agreement concerning the software struck between you, the licensor, and the other owners, and that it replaces any previous agreement or any written or oral exchange or any other communication pertaining to the object of this license.

Insight Server has to register the installation. For that it has to connect to the key server. Only data relevant for registration will be sent.

Which port would you like to use for registration?

License Key

Please enter your key

If you're using a proxy to connect to the web, please enter the information below:

* Proxy IP address * Proxy port
Username Password

* - Required values if using a proxy

Figure 87 - Proxy Registration

Note: If the server resides behind a firewall and port 80 is blocked, port 3080 can be configured for automatic registration and validation of the license key.

To manually validate a license key (Non-demo systems):

1. Ensure that the registration page is open.
2. After "Manually validate the key" is selected, a string of letters and numbers are displayed. Email this information to a Bynari Support representative.

A Bynari representative will contact the user as soon as possible and provide validation information to enter into the "Line 1" and "Line 2" fields.

Insight WebClient

Note: In order to use the WebClient, a license key is needed and can be obtained by purchasing WebClient licenses. To activate the WebClient, login as "manager" from the WebClient interface, and enter the license key code.

Run WebClient

This link opens the web client login screen.

Access Controls

This link opens the web client administrator screen where access permissions are changed for each user to allow access to the web client. To change a user's status, select or deselect a check box and click on "Change Access", as illustrated below.

Access	Username	Distinguished Name
<input checked="" type="checkbox"/>	cmarshall	Cathy Marshall, example.com
<input checked="" type="checkbox"/>	drich	David Rich, example.com
<input checked="" type="checkbox"/>	jdoe	John Doe, example.com
<input checked="" type="checkbox"/>	msmith	Mark Smith, example.com
<input checked="" type="checkbox"/>	mrose	Mary Rose, example.com
<input checked="" type="checkbox"/>	ncane	Nancy Cane, example.com
<input checked="" type="checkbox"/>	exampleuser	user, example.com

Figure 88 - WebClient access

Content Filtering

For our customers convenience we have included several open source products already integrated into Postfix's content filter. All messages are passed through Postfix's content_filter before being delivered locally via Imtp to Cyrus.

There are a number of contents filters available both through open source as well as commercially. These products for the most part are for virus scanning and spam filtering. Since a wide variety of products exist and often a number of them may want to be used, we've integrated AMaViS content filter into Postfix. This product passes the message between multiple content filters and virus scanners.

We have also included ClamAV for anti virus and SpamAssassin for spam filtering which AMaViS is configured to utilize. In a default installation the administrator must enable the content_filtering entry in the Postfix configuration if you wish to take advantage of these additional features.

AMaViS



Setup and Configuration Guide

AMaViS (A Mail Virus Scanner) scans e-mail attachments for viruses using third-party virus scanners available for UNIX environments (such as ClamAV, F-Prot, Sophos, etc). It resides on a UNIX (Linux) machine and scans the attached files arriving via e-mail, generates reports when a virus is found and sets the delivery on hold. AMaViS is built into Insight Server 4.2, together with ClamAV and SpamAssassin.

This software is integrated into our product for the convenience of our customers. We assume no responsibility for its use within our product.

AMaViS configuration settings can be adjusted by updating this file:

```
/opt/insight/etc/amavisd.conf
```

Here are some common entries which may need to be adjusted on a per installation basis depending on your requirements.

To bypass either virus scanning or spam checking uncomment the appropriate line shown below.

```
# @bypass_virus_checks_maps = (1); # uncomment to DISABLE anti-virus code  
# @bypass_spam_checks_maps = (1); # uncomment to DISABLE anti-spam code
```

The following entry is helpful when you would like to configure multiple domains residing on the same server as local traffic.

```
@local_domains_maps = ( [ ".$mydomain" ] );
```

Log level adjustments can be made using the line shown below.

```
$log_level = 2;          # verbosity 0..5
```

The following lines adjust the Spam Assassin tag level behavior. These entries control when headers are updated, the subj. line is updated to include *****SPAM*****, and finally when known spam is bounced back to the originator. The last two entries are the same so if you would like more aggressive spam tagging on the subject line then lower the `sa_tag2_level_deflt` to lower than 5.0 and leave the kill level at 5.0.

```
$sa_tag_level_deflt = 2.0; # add spam info headers if at, or above that level  
$sa_tag2_level_deflt = 5.0; # add 'spam detected' headers at that level  
$sa_kill_level_deflt = 5.0; # triggers spam evasive actions
```

For more information about the (open-source) AMaViS project, please visit their website: <http://www.amavis.org>

Clam AntiVirus

Clam AntiVirus is an open-source anti-virus toolkit for Unix/Linux that has been integrated into Insight Server 4.2. The main purpose of this software is the integration with mail servers (attachment scanning). The package provides a flexible and scalable multi-threaded daemon, a command line scanner, and a tool for automatic updating via Internet. The programs are based on a shared library distributed with the Clam AntiVirus package which can be used in the user's own software. Most importantly, the virus data-



Setup and Configuration Guide

base is kept up to date.

This software is integrated into our product for the convenience of our customers. We assume no responsibility for its use within our product.

This GPL scanner features:

- command-line scanner
- fast, multi-threaded daemon
- database updater with support for digital signatures
- virus scanner C library -on-access scanning (Linux)
- detection of over 20000 viruses, worms and trojans
- built-in support for RAR (2.0), Zip, Gzip, Bzip2 -built-in support for Mbox, Maildir and raw mail files

[also remember that Clam was "plugged into" AMaViS]

ClamAV can be configured in this directory:

```
/opt/insight/etc/clamav.conf
```

Other directories used by clamav:

```
/opt/insight/bin/clamscan  
/opt/insight/bin/clamscan  
/opt/insight/etc/rc/clamd  
/opt/insight/include/clamav.h  
/opt/insight/man/man1/clamscan.1  
/opt/insight/man/man1/clamscan.1  
/opt/insight/man/man5/clamav.conf.5  
/opt/insight/man/man8/clamav-milter.8  
/opt/insight/man/man8/clamd.8  
/opt/insight/sbin/clamd  
/opt/insight/share/clamav  
/opt/insight/var/amavis/clamd.log  
/opt/insight/var/amavis/clamd
```

More information and configuration options can be found in the ClamAV manual on our website.

SpamAssassin

SpamAssassin is a mail filter which attempts to identify spam using a variety of mechanisms including text analysis, Bayesian filtering, DNS blocklists, and collaborative filtering databases.

Using its rule base, it uses a wide range of heuristic tests on mail headers and body text to identify "spam", also known as unsolicited commercial email.

This software is integrated into our product for the convenience of our customers. We assume no responsibility for its use within our product.

The primary configuration file for SpamAssassin is:

```
/opt/insight/etc/mail/spamassassin/local.cf
```

To view the man pages for the local.cf configuration file from a shell prompt run the

command:

```
# /opt/insight/bin/perldoc Mail::SpamAssassin::Conf
```

For more information about the SpamAssassin project, please visit their website:

<http://spamassassin.apache.org/>

SquirrelMail

SquirrelMail is a free, standards-based, open-source webmail package written in PHP4, and has been integrated into Insight Server. It includes built-in pure PHP support for the IMAP and SMTP protocols, and all pages render in pure HTML 4.0 (with no JavaScript required) for maximum compatibility across browsers. It has very few requirements and is easy to configure and install. SquirrelMail is great for clients needing a simple web-based email client for email only; it will not synch/read "special folders" such as contacts, calendar items, tasks. To access special folders, use either Insight Connector for Outlook or our web based groupware client, Insight WebClient.

SquirrelMail can be accessed by entering "squirrelmail/" after the mail server name or IP address; ie "<http://mail.company1.com/squirrelmail/>"

This software is integrated into our product for the convenience of our customers. We assume no responsibility for its use within our product.

Any user on Insight Server can utilize SquirrelMail.

Jabber

Jabber is an open source alternative to Instant Messaging services like AIM, ICQ, MSN, and Yahoo. This allows companies to provide Instant Messaging capabilities to users without opening their internal networks to the potential risks of external connections. In addition, it will require no additional administrative overhead since users are authenticated against the Insight Server Open LDAP database using our schema.

The Jabber server can be accessed by using an appropriate client and their Insight Server user id and password combination.

Configuration files for Jabber can be found in the directory `/opt/insight/etc/jabberd`.

Additional information regarding the customization of this product can be found at <http://www.jabber.org>.

This software is integrated into our product for the convenience of our customers. We assume no responsibility for its use within our product.

Help Browser

Administrator Help Browser

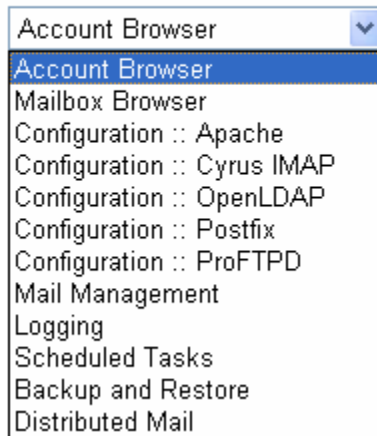


Figure 89 – Help Browser

The help browser is intended for online help facility for configuration parameters for the different components of the Insight Server. These parameters can be found on the actual product help pages.