

Directory Sync Server Edition

Administration Guide

Release 1.2.22

- **Google Message Filtering**
- **Google Message Security**
- **Google Message Discovery**
- **Postini Email Security**

Google

powered by postini

Google, Inc.
1600 Amphitheatre Parkway
Mountain View, CA 94043
www.google.com

Part number: DSS_614_03

14 April 2008

© Copyright 2008 Google, Inc. All rights reserved.

Google, the Google logo, Google Message Filtering, Google Message Security, Google Message Discovery, Postini, the Postini logo, Postini Perimeter Manager, Postini Threat Identification Network (PTIN), Postini Industry Heuristics, and PREEMPT are trademarks, registered trademarks, or service marks of Google, Inc. All other trademarks are the property of their respective owners.

Use of any Google solution is governed by the license agreement included in your original contract. Any intellectual property rights relating to the Google services are and shall remain the exclusive property of Google, Inc. and/or its subsidiaries ("Google"). You may not attempt to decipher, decompile, or develop source code for any Google product or service offering, or knowingly allow others to do so.

Google documentation may not be sold, resold, licensed or sublicensed and may not be transferred without the prior written consent of Google. Your right to copy this manual is limited by copyright law. Making copies, adaptations, or compilation works, without prior written authorization of Google. is prohibited by law and constitutes a punishable violation of the law. No part of this manual may be reproduced in whole or in part without the express written consent of Google. Copyright © by Google, Inc.

Google, Inc. provides this publication "as is" without warranty of any either express or implied, including but not limited to the implied warranties of merchantability or fitness for a particular purpose. Google, Inc. may revise this publication from time to time without notice. Some jurisdictions do not allow disclaimer of express or implied warranties in certain transactions; therefore, this statement may not apply to you.

This software uses the JGoodies Forms, JGoodies Validation, and JGoodies Looks.

Copyright (c) 2002-2008 JGoodies Karsten Lentzsch. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

o Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

o Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

o Neither the name of JGoodies Karsten Lentzsch nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT OWNER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This software uses Apache Derby.

Apache Derby

Copyright 2004-2007 The Apache Software Foundation

This product includes software developed by

The Apache Software Foundation (http://www.apache.org/).

Portions of Derby were originally developed by International Business Machines Corporation and are licensed to the Apache Software Foundation under the "Software Grant and Corporate Contribution License Agreement", informally known as the "Derby CLA".

The following copyright notice(s) were affixed to portions of the code with which this file is now or was at one time distributed and are placed here unaltered.

(C) Copyright 1997,2004 International Business Machines Corporation. All rights reserved.

(C) Copyright IBM Corp. 2003.

The portion of the functionTests under 'nist' was originally developed by the National Institute of Standards and Technology (NIST), an agency of the United States Department of Commerce, and adapted byInternational Business Machines Corporation in accordance with the NIST Software Acknowledgment and Redistribution document at

http://www.itl.nist.gov/div897/ctg/sql_form.htm

About This Guide 7
What This Guide Contains 7
Related Documentation 7
How to Send Comments About This Guide 8
Introduction 9
About Directory Sync Server Edition 9
Features and Benefits 9
Comparison with Directory Sync Hosted Edition 10
Architecture 11
Components 13
Installation 15
About Installation 15
System Requirements 16
Install Directory Sync 16
Upgrade Directory Sync 17
Uninstall Directory Sync 18
Configuration 19
About Configuration 19
Configuration Files 20
Settings 20
Server 21
Orgs 23
Exclusion Filters 24
LDAP Settings 28
LDAP Authentication 29
LDAP Attributes 32
Search Rules 34
Mail Lists 41
Notifications 45
Delete Limits 47
Log Files 48
Test 49
Simulate Sync 50
Synchronization 53
About Synchronization 53
Command Line Synchronization 53
Synchronization options 54
Scheduling Synchronization 54
Microsoft Windows: Scheduled Tasks 55
Linux and Solaris: cron 55
Troubleshooting 57
About Troubleshooting 57
Common Issues 57
System Tests 58
Escalating Problems 59



About This Guide

What This Guide Contains

The *Directory Sync Server Edition Administration Guide* provides information about:

- Directory Sync Server Edition features.
- Basic steps for installing the directory sync utility on your mail server.
- Configuration for the directory sync utility.
- Synchronizing users.
- Troubleshooting the directory sync utility.

This guide is intended for mail server administrators who are already familiar with mail server configuration and the message security service.

This guide is a supplement to the *Message Security Administration Guide*. For details about using the features and components of the message security service, see the *Message Security Administration Guide*.

Related Documentation

For additional information about the message security service and related products, refer to the following related documents.

Document	Description
Message Security Administration Guide	Administration Guide for the message security service. This includes information on users and organizations, message filtering, and other features. The Directory Sync chapter in this guide covers only Directory Sync Hosted Edition.

Document	Description
Directory Sync Configuration Guide	Instructions for setting up your network environment and directory server for Directory Sync Hosted Edition. Directory Sync Hosted Edition is a different feature, that runs on the message security service and requires special configuration on your network to use.

How to Send Comments About This Guide

Postini values your feedback. If you have comments about this guide, please send an email message to:

`doc_comments@postini.com`

Please specify in your email message the section to which your comment applies. If you want to receive a response to your comments, ensure that you include your name and contact information.

Chapter 2

Introduction

About Directory Sync Server Edition

Directory Sync Server Edition is a utility that adds, deletes, and moves your users in the message security service to match your LDAP server. When you synchronize, any changes on your LDAP server are reflected in the message security service.

The directory sync utility runs on a server machine in your network environment. You can use any machine that is able to connect to your LDAP server and the message security service.

Features and Benefits

Directory Sync Server Edition offers the following features and benefits:

- Updates registered users in the message security service to match your LDAP user list.
- A local on-site utility that runs in your server environment. Your LDAP information never leaves your perimeter.
- Can be configured to track user primary address changes, keeping quarantines and settings intact even with user address changes.
- Runs on any Windows (tested on XP), Linux or Solaris server.
- Installs with all needed components.
- Allows sophisticated rules to handle mailing lists, aliases, and exceptions.
- Allows complex mapping for your org hierarchy.
- Extensive tests and simulation to ensure correct synchronization.

Comparison with Directory Sync Hosted Edition

Directory Sync Server Edition is a separate utility run on your server, and is different from the Directory Sync Hosted Edition feature found in the Administration Console.

Because of the functional advantages and ease of use, Directory Sync Server Edition is recommended over Directory Sync Hosted Edition for most administrators.

Both Directory Sync Server Edition and Directory Sync Hosted Edition synchronize your LDAP server with your user list in the message security service, but they work in very different ways.

WARNING: Directory Sync Server Edition and Directory Sync hosted Edition are two distinct ways to synchronize. They are not designed to work together. Using both at the same time could cause unexpected or contradictory results.

This table compares these two methods:

	Directory Sync Server Edition	**Directory Sync Hosted Edition**
Location	Runs on a server in your network.	Runs on the message security service.
Configuration	Configure on your server with the Configuration Manager utility provided.	Configure in the Administration Console.
Direction of Data Flow	Pushes changes to the message security service.	Pulls changes from your DSML server.
Installation Needed	Installation includes all needed components.	Requires complex installation of third party DSML server on your network.
Firewall Settings	Your firewall must allow outgoing HTTPS connections to the message security service.	Your firewall must allow incoming HTTP connections to your DSML server.
Connection	Connects directly to your LDAP server.	Connects to your DSML server, which then connects to your LDAP server.
Authorization	Requires administration access on the message security service, and read and execute permissions on your LDAP server. Uses basic authentication.	Requires administration access on the message security service, and read and execute permissions on your LDAP server. Uses basic authentication or anonymous access.
Complexity	Allows advanced LDAP queries, sophisticated organization mapping, and exception handling.	Allows advanced LDAP queries, simple organization mapping, and some exception handling.

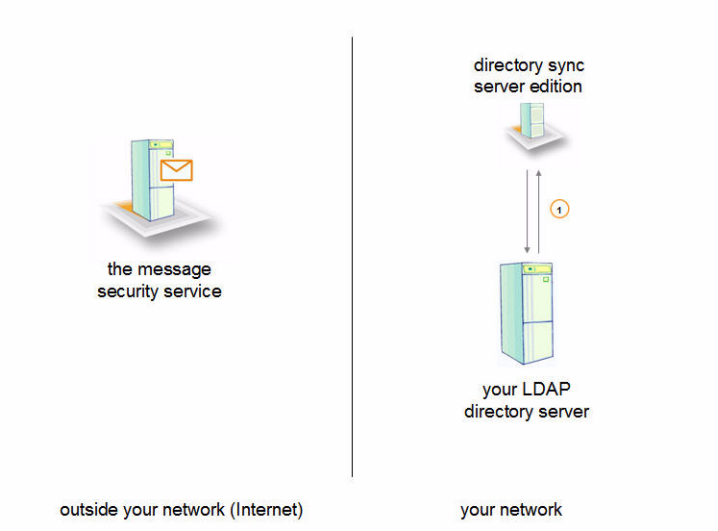
This guide details Directory Sync Server Edition. For more information about Directory Sync Hosted Edition, see *About Directory Sync* in the Message Security Administration Guide and the *Configuration Guide for Postini Directory Sync*.

Architecture

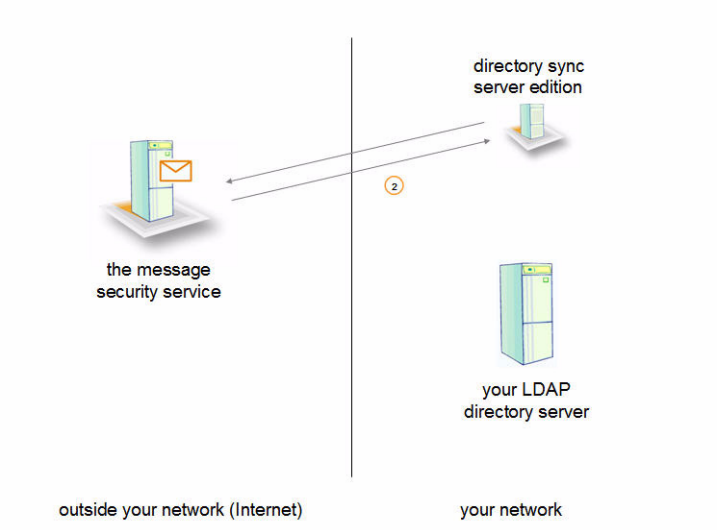
Directory Sync Server Edition runs on your server and updates the message security service to match your LDAP server. The directory sync utility never updates or changes your LDAP server.

The following graphs and steps describe how the data flow of directory sync works.

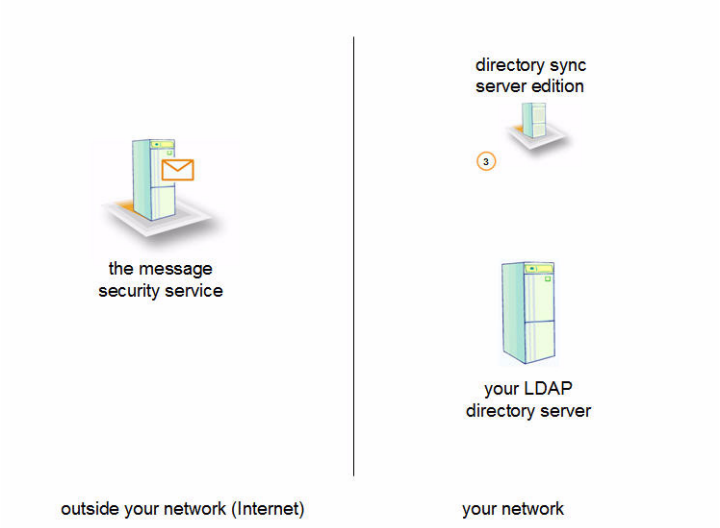
1. The directory sync utility connects to your LDAP server and generates a list of users on your directory server. You can set up rules to specify how this user list is generated.



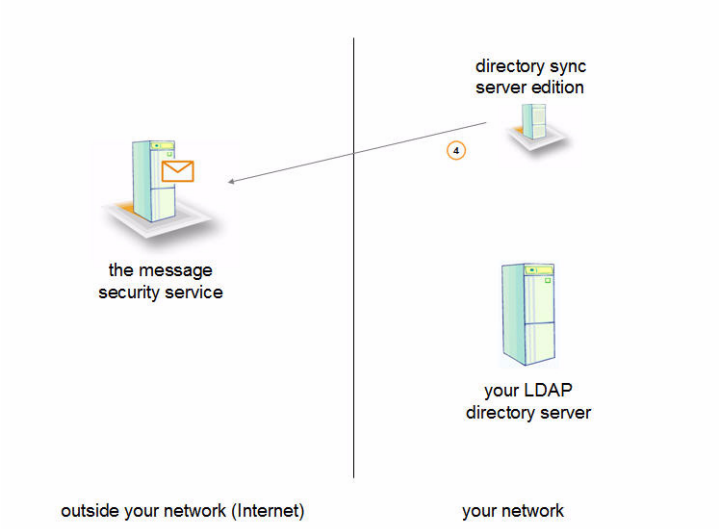
2. The directory sync utility connects to the message security service and generates a list of registered users in the message security service. You can set up rules to specify how this user list is generated.



3. The directory sync utility compares the two lists, and generates a list of changes.



4. The directory sync utility then updates the message security service to match your LDAP server settings.



Components

The directory sync utility includes the following components:

- **Configuration Manager.** Use this graphical UI to configure how the directory sync utility will connect to the message security service and to your LDAP server. You can also create rules for user lists, search queries, organization mapping, aliases, distribution lists and exceptions. See “Configuration” on page 19.
- **XML Configuration File.** An XML file containing connection and configuration information. This XML file is created in the configuration manager and used by the synchronization command line.
- **Synchronization Command Line.** The command-line utility `sync-cmd.exe` performs actual synchronization. This utility connects to the message security service and your LDAP server, using settings in the XML file you configure, then updates your registered user list in the message security service. See “Synchronization” on page 53.
- **Scheduling.** The directory sync utility is designed to work with your server’s scheduling utility for a scheduled synchronization. Depending on the synchronization you use, this might be a `cron` job, a Windows Scheduled Service utility, or any other scheduling tool. See “Synchronization” on page 53.

These components are designed to work together. A typical setup for Directory Sync Server Edition involves the following steps:

1. Install the directory sync utility.
2. Step through Configuration Manager to configure synchronization.
3. In Configuration Manager, simulate a synchronization.
4. In Configuration Manager, revise your configuration based on the simulation. This could take several revisions for complex environments.
5. When the simulation is successful, save your final copy of the configuration file and exit Configuration Manager.
6. In the command line, run a manual synchronization with the configuration file you created to update the message security service.
7. Using your server’s scheduling tools, set up automatic scheduled synchronization.

Chapter 3

Installation

About Installation

To run Directory Sync Server Edition, install the directory sync utility on your server. The directory sync utility is designed to run on Windows, Linux or Solaris machines.

The installer is an executable program that installs all needed components on the server, including managing libraries, classpath variables, and other components. The installer also uninstalls any existing version of the directory sync utility in the same directory.

The sections below contain instructions on how to install, upgrade and uninstall the directory sync utility on your server.

System Requirements

To use Directory Sync Server Edition requires the following:

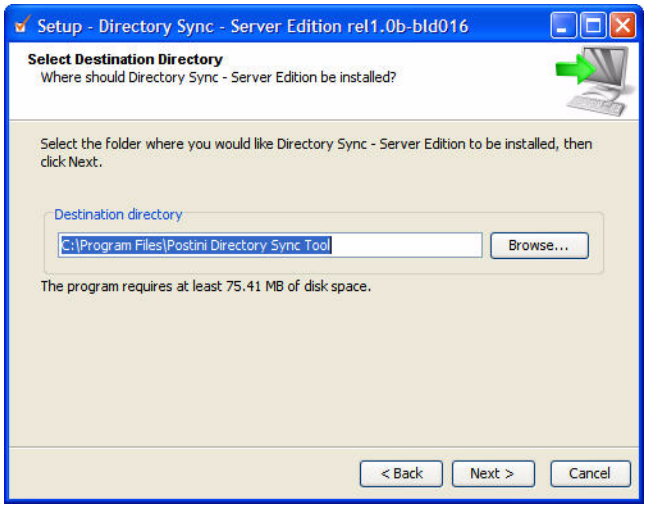
- A server on which to install Directory Sync Server Edition, running Microsoft Windows (tested on XP), Linux or Solaris.
- Sufficient disk space on the server. You should have at least 5G of disk space for log files and data. If you are running with DEBUG or INFO level of logging, you may need more free space than this for additional log data.
- Sufficient memory enough the server. The minimum amount of RAM needed to run the tool is 256MB free. Suggested is 1G free if you have less than 10,000 users, 2G free if you have more than 10,000 users. For very large organizations (over 250,000) further tuning may be needed.
- An LDAP server with user information, accessible to the directory sync utility. All versions of the LDAP protocol are supported.
- Read and execute administrative access on the user section of the LDAP server.
- Network access to the message security service through HTTP, directly or through a proxy server.
- An administrator account on the message security service.
- A mail server able to accept and relay notifications from the directory sync utility.

Install Directory Sync

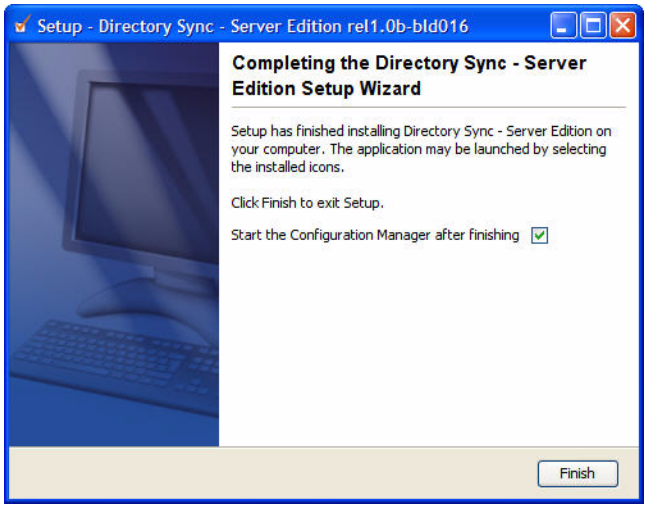
To install the directory sync utility:

1. In a web browser, go to `http://www.postini.com/dir_sync`.
2. Choose the operating system of the server where you plan to run the directory sync utility.

3. Download and run the installer.



4. When you have completed all the steps of the installer, the directory sync utility has been installed.



The installer contains all needed components and can be run offline without any outside connection.

Upgrade Directory Sync

The latest version of the directory sync utility is always accessible on the Directory Sync Server Edition website. To upgrade to the latest version, go to this site, and download and run the directory sync utility.

Configuration files are backward-compatible. Future versions of the directory sync utility cans run configuration files created in earlier versions.

The installer wizard automatically detects and uninstalls previous versions of the software in the same directory.

To reinstall the utility.

1. In a web browser, go to `http://www.postini.com/dir_sync`.
2. Choose the operating system of the server where you plan to run the directory sync utility.
3. Download and run the installer.
4. Select a directory on your server to install the directory sync utility.
5. Complete the installer wizard.

Uninstall Directory Sync

The directory sync utility also includes an uninstaller.

To remove the directory sync utility:

1. Open a command line interface and go to the directory that contains directory sync utility
2. Run the following command:

   ```
   uninstall
   ```

3. In the Uninstaller, click Next to uninstall the directory sync utility.
4. Once uninstallation has completed close the uninstaller.

All directory sync utility files and all libraries not used by other programs will be removed. Log files and XML configuration files will not be deleted.

Chapter 4

Configuration

About Configuration

Configuration Manager is a step-by-step graphical user interface that walks you through creating and testing an XML configuration file for Directory Sync Server Edition.

In Configuration Manager, you can:

- Set up and test a connection to the message security service.
- Configure which users and orgs in the message security service to synchronize.
- Set up and test a connection to your LDAP server.
- Configure LDAP search criteria for synchronization.
- Set up notifications and logging.
- Run a simulated synchronization to verify your settings.

Once you have set up your configuration in Configuration Manager, run your actual synchronization from the command line. See “Synchronization” on page 53.

Configuration Manager does not change your data in your LDAP directory server or the message security service. It is strictly used to configure and simulate synchronization.

Directory Sync Server Edition settings are stored as XML configuration files. Configuration Manager can also load and edit existing configuration files for Directory Sync Server Edition.

Note: All configuration settings, including accounts and passwords, are stored in an unencrypted XML file. Be careful when allowing access to this file.

Configuration Manager walks you through each step of configuring Directory Sync Server Edition. Once you have finished each page, click Next to go to the next step. You can also go back to previous steps with the Previous button, or jump directly to any step using the left side navigation menu.

The directory sync utility includes several ways to customize search rules and filters. When collecting information from your LDAP server, you can define LDAP queries to extract information. The directory sync utility supports RFC 2254, the International Standard on LDAP Filters. For the details, see RFC 2254:

```
http://www.ietf.org/rfc/rfc2254.txt
```

The directory sync utility also includes some non-LDAP filters. In these, you can use regular expressions to filter for patterns of text. Regular expressions use standard Java regular expression syntax, which is similar to most standard regular expression syntax standards.

Configuration Files

In Configuration Manager, you can save or load configuration files to manage multiple configuration files and store settings for later. All configuration files are XML files.

To save configuration settings under a new name, select File->Save As from the top menu and specify the directory and filename you wish to use. If you overwrite an existing file, Configuration Manager will save the existing file as a copy with the timestamp in the file name.

To save configuration settings under the existing name, select File->Save from the top menu. If you haven't saved yet, this option will be greyed out. If you overwrite an existing file, Configuration Manager will save the previous file as a copy with the timestamp of when the file was overwritten.

To open a configuration file, select File->Open from the top menu and choose the configuration file. The user interface will then show the settings for that configuration file. To open a recent configuration file, select File->Open Recent and choose the configuration file.

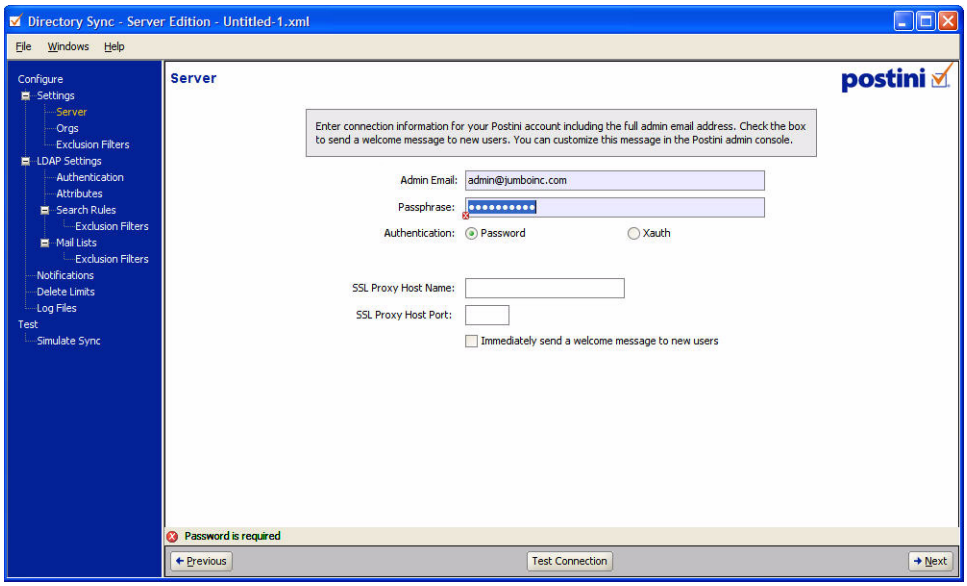
To start a new configuration file, select File->New from the top menu. Configuration Manager will load a new file with no configuration rules specified.

Settings

The Settings section governs how Directory Sync connects to the message security service, and how Directory Sync generates your message security service user list for comparison.

Server

Enter your message security service login and connection information in this section.



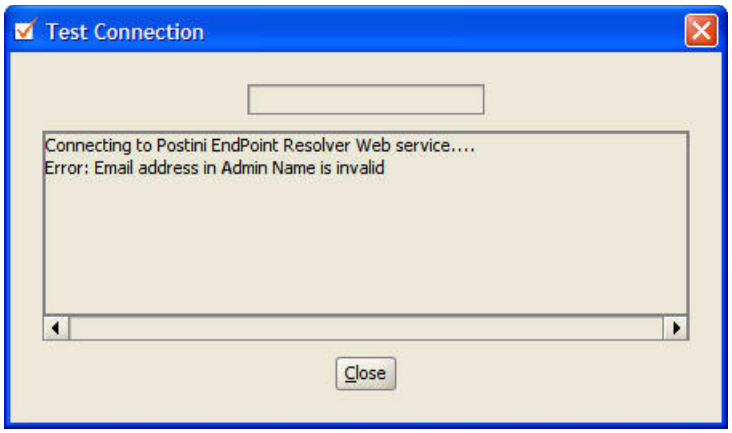
Specify the following:

Setting	Description
Admin Email	The email address used to log into the Administration Console. This address should be a valid user on the Administration Console with administrative privileges over the user organizations you want to synchronize. Example: `admin@jumboinc.com`
Passphrase	The password (if using passwords) or XAuth shared secret (if using XAuth) for the Admin Email. Example: `swordFISH23` **Note:** Like all configuration settings, passwords are stored in an unencrypted XML file.

Setting	Description
Authentication	The authentication method used. If you have set up XAuth (cross-authentication) with the Administration Console, and you wish to use XAuth to connect, select XAuth. Otherwise, leave this setting as Password. Example: Password
SSL Proxy Host Name	If your server is running behind a firewall that requires an SSL Proxy to connect to an outside server, enter the proxy host name here. If you can connect directly to the internet from this machine, leave this field blank. Example: `httpproxy.jumboinccorp.com`
SSL Proxy Host Port	If your server is running behind a firewall that requires an SSL Proxy to connect to an outside server, enter the proxy host port here. Otherwise, leave this field blank. Example: `8080`
Welcome Message	Typically, the message security service sends welcome notifications to new users within 24 hours, but not immediately. This is to prevent a flood of welcome that may overload your mail server. If you want to send all the notifications immediately, check the box labelled "**Immediately send a welcome notification to new users.**"

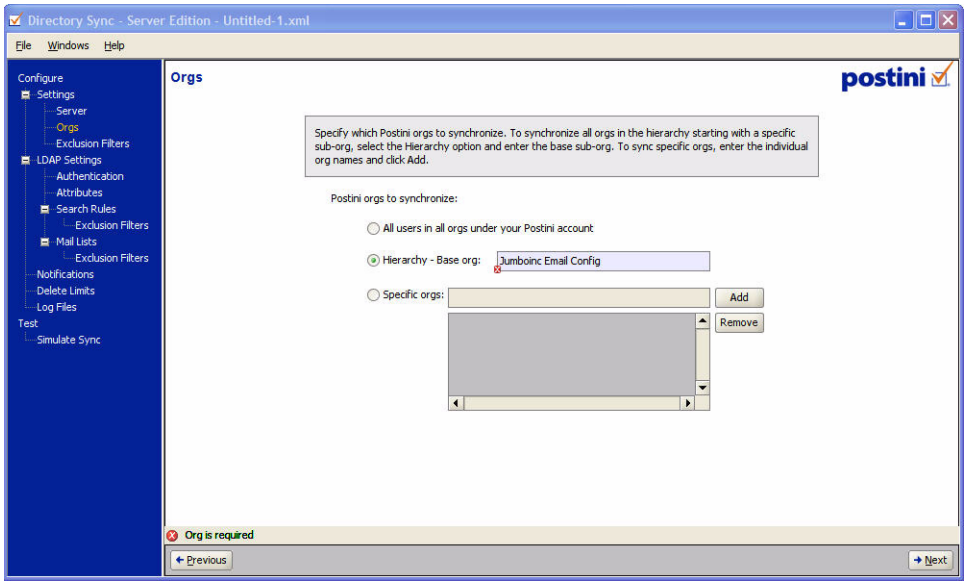
Test Connection

Once you have configured Server settings, click **Test Connection**. Configuration Manager will connect to the message security service and attempt to log in.



Orgs

On this page, specify which orgs in the message security service to synchronize. The directory sync utility will use these orgs to generate user lists as a basis for comparison with your LDAP user list.



By default, any user in the specified orgs will be deleted if they are in the user list generated from your LDAP server, and any users not in these orgs will be added (or moved from another org) if they in the user list generated from your LDAP server. You make exceptions to this behavior by using exclusion filters.

Choose which orgs to synchronize:

- **All users in all orgs under your Postini account:** All organizations visible to the administrator account (specified in the Server section) are included in synchronization.
- **Hierarchy:** All organizations under an organization you specify here are included in the synchronization. Enter the org name (not IID) here. The org name is case sensitive. Match the same case as the org name in the message security service.
- **Specific orgs:** Only the specified organizations are included in the synchronization. Enter each org name (not IID) and click Add to add it to the list. To remove an organization from synchronization, select that organization on the list and click Remove. Org names are case sensitive. Match the same case as the corresponding org name in the message security service.

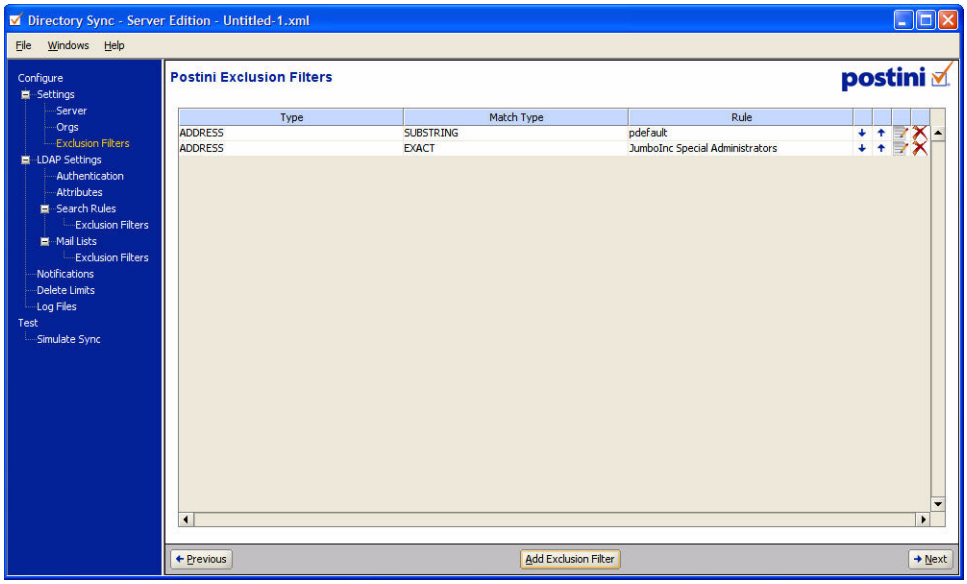
Exclusion Filters

If you have any users on your message security service user list who should not be deleted or moved by the synchronization, add an exclusion filter to protect those users.

Important: If you include your top-level message security service account organization in the synchronization, you must add an exclusion filter for your default user. See Add Exclusion Filter for details.

Other exclusion filters you may want to might include:

- Default users
- Administrators who are not in your LDAP system in the OUs you specify
- Mailing list administrators
- Users in the message security service who are listed on a different LDAP server



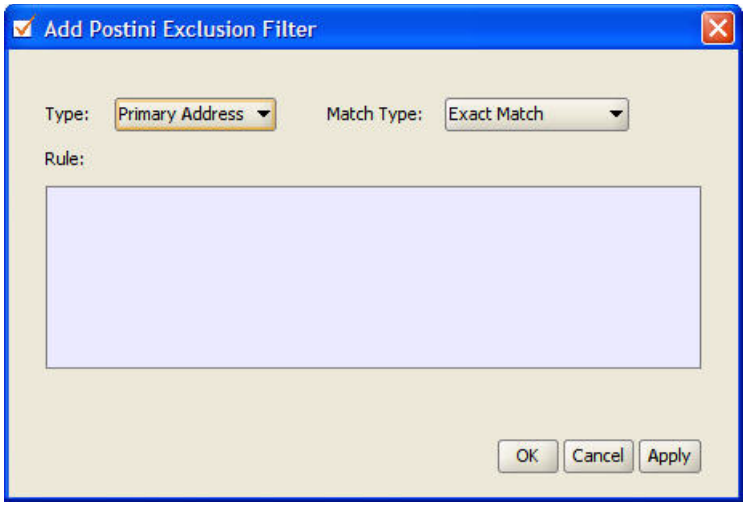
This page shows the list of exclusion filters. In a new configuration, this will be an empty list. To add new exclusion filters, click the Add Exclusion Filter button at the bottom of the screen.

On the list of Exclusion Filters, you can change existing filters:

- Reorganize: Click the up arrow or down arrow icon to change the order of exclusion filters.
- Edit: Click the notepad icon to edit the settings of an exclusion filter.
- Delete: Click the X icon to delete the exclusion filter.

Add Exclusion Filter

Click the Add Exclusion Filter at the bottom of the page to exclude a user or organization from synchronization.



Specify the following:

Setting	Description
Type	Sets what type of exclusion filter to create, Primary Address or Postini Org. • Primary Address: Check the user's primary address and excludes any users that match. • Postini Org: check the organization name on the message security service and exclude all users in organizations that match.

Setting	Description
Match Type	The type of rule of match for the filter. • **Exact Match:** The address or organization name must match the rule exactly. User Example: For a user, `user1@jumboinc.com` would exclude that single user. Org Example: For an org, “Jumboinc Florida Sales” would exclude all users in that single org. • **Substring Match:** The address or organization name must contain the text of the rule as a substring. User Example: For a user, `pdefault` would exclude `pdefaultsales55@jumboinc.com` and `pdefault@sales.jumboinc.com`. Org Example: For an org, “Sales” would exclude all users in “Jumboinc Florida Sales” and “Sales Teams”. • **Regular Expression:** The address or organization must match the regular expression in the rule. User Example: For a user, the regular expression `team[3-9]@jumboinc.com` would exclude `team3@jumboinc.com` through `team9@jumboinc.com`. Org Example: For an org, the regular expression `Local Group - [A-Z][A-Z]` would exclude all users in the “Local Group - NJ” and “Local Group - AZ” organizations.
Rule	The text of the match or regular expression to compare. See above for examples for these rules. Users that meet the requirements for an exclusion filter will not be deleted or moved. If they are listed on the LDAP server, the directory sync utility will attempt to add the user and fail

Default Users

If your search includes your pdefault users, the directory sync utility will try to delete these users unless they are in your LDAP server. This will cause an error.To fix this, add an exclusion filter. Click Add Exclusion Filter and use the following settings:

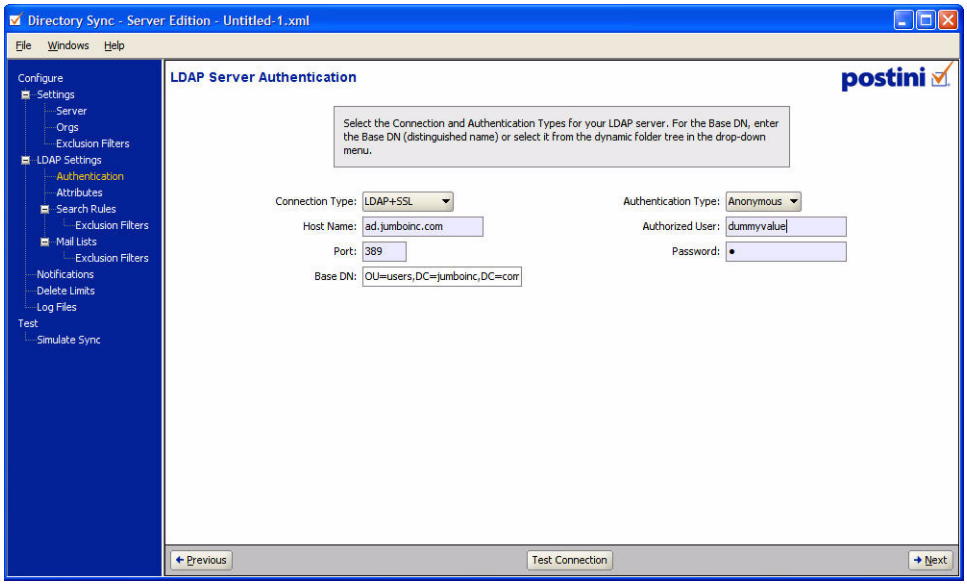
- **Type:** Primary Address
- **Match Type:** Substring Match
- **Rule:** `pdefault@`

LDAP Settings

The LDAP Settings section configures how the directory sync utility connects to your LDAP directory server and generates your LDAP user list for comparison.

LDAP Authentication

Specify your LDAP Authentication settings in this page.

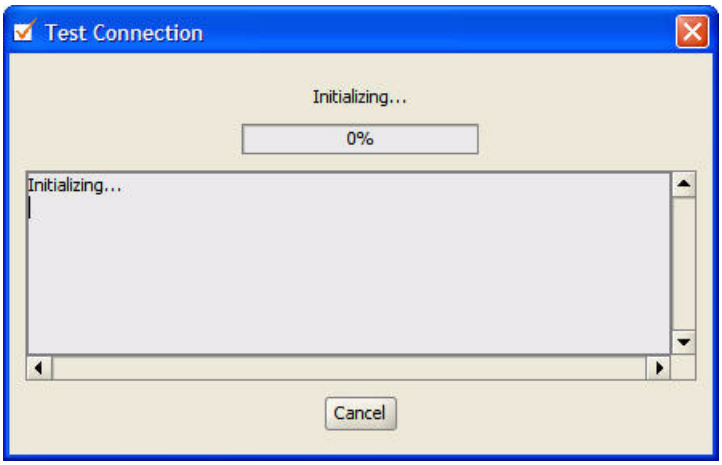


Setting	Description
Connection Type	Choose whether to use an encrypted connection. If your LDAP server supports an SSL connection and you wish to use it, choose LDAP + SSL. Otherwise, choose Standard LDAP. Example: Standard
Host Name	Enter the domain name or IP address of your LDAP directory server. Example: `ad.jumboinc.com`, or 10.22.1.1.
Port	Specify the host port. The default is 389. Example: 389
Base DN	Enter the Base DN for the subtree to use. Do not include spaces between commas. If you don't know the Base DN, consult your LDAP administrator. Example: `ou=test,ou=sales,ou=melbourne,dc=ad,dc=jumboinc,dc=com.`

Setting	Description
Authentication Type	The authentication method for your LDAP server If your LDAP server allows Anonymous connections and you want to connect anonymously, select Anonymous. Otherwise, select Simple. Example: Simple
Authorized User	Enter the user to use when connecting to the server. This user should have read and execute permissions for the whole subtree. If needed, include the domain for the user as well. **Note:** This field is always required. If you are using an Anonymous connection, enter any value here. Example: `admin1`
Password	Enter the password for the authorized user. **Note:** This field is always required. If you are using an Anonymous connection, enter any value here. Example: `swordfish` **Note:** Like all configuration settings, passwords are stored in an unencrypted XML file.

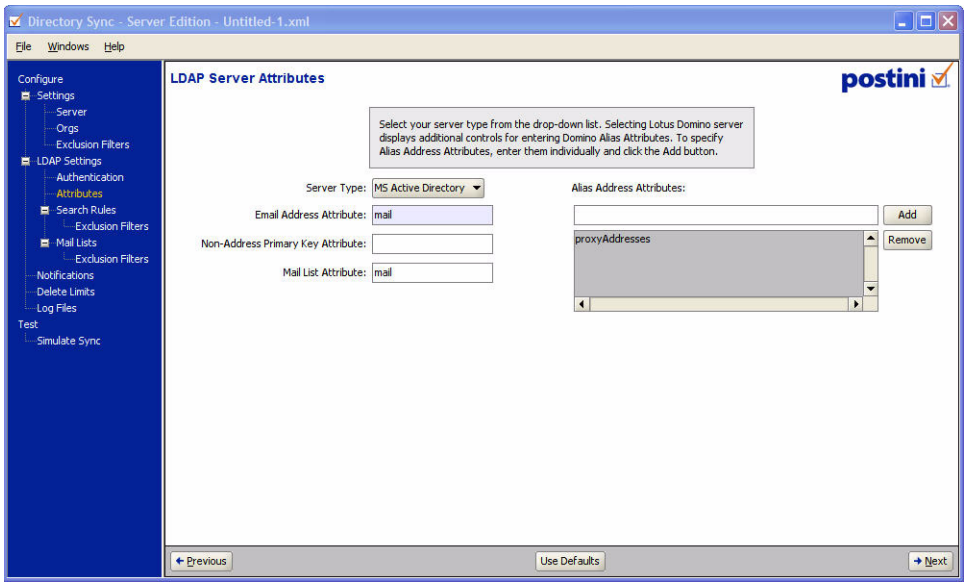
Test Connection

Once you have configured LDAP Authentication settings, click Test Connection. Configuration Manager will connect to your LDAP server and attempt to log in, to verify the settings you entered.


Test Connection
Initializing...
0%
Initializing...
Cancel

LDAP Attributes

Specify what attributes Directory Sync will use when generating the LDAP user list.



Setting	Description
Server Type	The type of LDAP server that you are using with the directory sync utility. If you are using a Lotus Domino, Microsoft Active Directory, or Open LDAP directory server, select that Server Type. Otherwise, select Other. Example: Microsoft Active Directory
Email Address Attribute	The LDAP attribute that contains a user's primary email address. Example: The default is `mail`.
Non-Address Primary Key Attribute	An LDAP attribute with a unique key other than an email address. This is optional, but provides a benefit: if a user's email address on your LDAP server changes, Directory Sync will rename the user in the message security service without losing any quarantined mail or user settings.

Setting	Description
Mail List Attribute	An LDAP attribute that specifies the address of a mailing list. The directory sync utility will use this attribute to look up the email address for any mailing lists detected with Mail List rules. For most servers, this value will be the same as the Email Address attribute. Example: `mail`
Alias Address Attributes	One or more attributes used to hold alias addresses. These addresses will be placed as aliases to the primary address listed in the Email Address Attribute field. Example: `proxyAddresses`
Domino Alias Address Attribute	Only for Lotus Domino servers. One or more attributes used to hold internal Domino alias attributes, which are stored as usernames without domain information. These addresses will be formatted as email addresses and placed as aliases to the primary address listed in the Email Address Attribute field. If you are using a Lotus Domino server but your alias address attribute stores full SMTP email addresses, list the attribute in Alias Address Attributes, not Domino Alias Address Attributes. Example: `uid`
Domino Replacement Character	Only for Lotus Domino servers. If an address contains a space, Directory Sync will substitute this character instead. Example: The most common values are dot (“.”) and underscore (“_”).

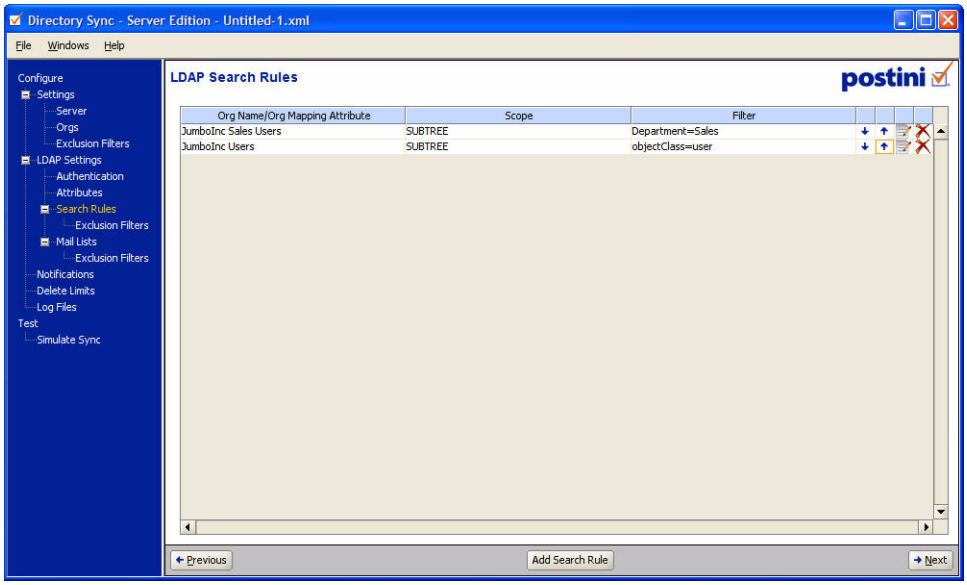
Use Defaults

Click this button to use the default values for your Server Type, as follows:

- Lotus Domino: Email Address Attribute `mail`, Domino Alias Address Attribute `uid`.
- MS Active Directory: Email Address Attribute `mail`, Alias Address Attribute `proxyAddresses`.
- OpenLDAP: Email Address Attribute `mail`.
- Other: Email Address Attribute `mail`.

Search Rules

This shows a list of rules used when generating the LDAP user list.



By default, all users that match these search rules will be added to the message security service user list (or moved if they are in a different organization) and all users that do not match these search rules will be removed. You can change this behavior with exclusion filters.

This page shows the list of search rules. In a new configuration, this will be an empty list. To add a search rule, click the Add Search Rule button at the bottom of the screen.

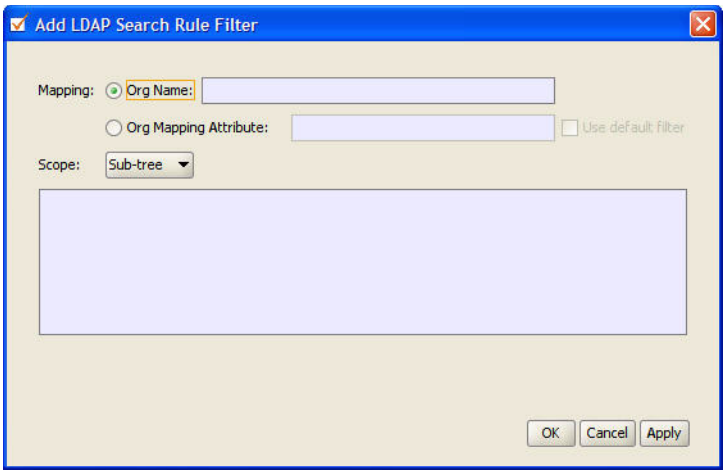
On the list of Search Rules, you can change existing rules:

- Reorganize: Click the up arrow or down arrow icon to change the order of search rules.
- Edit: Click the notepad icon to edit the settings of a search rule.
- Delete: Click the X icon to delete a search rule.

Search rules are processed in the order listed. If you would like one search rule to take priority over another, move that search rule up using the up arrow icon on this page. If two rules contradict each other, the first rule takes precedence.

Add Search Rule

To add a new search rule, click Add Search Rule.



Specify the following:

Setting	Description
Org Name	Select Org Name or Org Mapping Attribute for Mapping. For Org Name, all users that match this rule will be added to the message security service in the specified org. The org must exist in the message security service, but need not exist on your LDAP server. Example: “jumboinc-com users” Example: Org Mapping, “Department”

Setting	Description
Org Mapping Attribute	Select Org Name or Org Mapping Attribute for Mapping. For Org Mapping Attribute, the directory sync utility looks up the value of the attribute specified under Org Mapping Attribute, and adds users to this org on the message security system. For instance, if the Org Mapping Attribute is “Department” the directory sync utility will look up each user’s Department attribute. If that attribute is set to “jumboinc-com sales” then the directory sync utility will attempt to add the user to “jumboinc-com sales” in the message security service. If the value of the Org Mapping Attribute is blank, the directory sync utility will not add the user, and will attempt to delete the user from the message security system if it is there. The Org Mapping Attribute must be set up on your LDAP server. The value of that attribute must be the exact name of an org in the message security service. Example: Department The “use default filter” check box sets the scope to “Subtree” and the rule to `objectclass=*`.

Setting	Description
Scope	This determines where in the LDAP directory this rule applies. This could be an entire subtree, one level, or a single object. • Subtree: All objects matched by the search, and anything under those objects. (recursive) • One-level: All objects matched by the search, and anything one level underneath them. Does not look further than one level. • Object: Only objects directly matched by the search. No recursion of any kind. Choosing which option to use: Subtree gives the broadest search, but for very large organizations this can be load-intensive and cause system problems. One-level provides a limited search that will avoid causing load for very large organizations. Object is rarely used except with very complex searches. In most cases, Example: Subtree

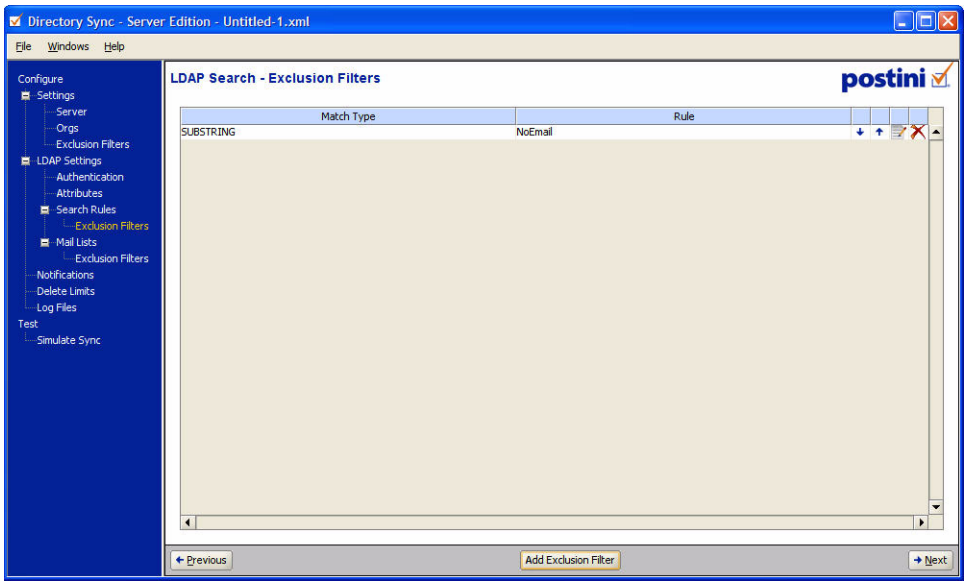
Setting	Description

Rule	This field is not labelled. This is the search rule used. This rule uses standard LDAP filtering language, and allows sophisticated logic and complex rules for searching. For more information about LDAP search filters, consult your LDAP documentation.
	
	Example 1: To match all objects (this may cause load problems):
	
	`objectclass=*.`
	
	Example 2: To match all human users:
	
	• For OpenLDAP:
	
	`(objectClass=inetOrgPerson)`
	
	• For Active Directory:
	
	`(objectClass=person)`
	
	• for Lotus Domino:
	
	`(objectClass=dominoPerson)`
	
	Example 3: Another way to detect only human email users in Active Directory:
	
	`(&(objectclass=user)(objectcategory=person))`

Exclusion Filters

If you have any users on your LDAP directory server that match your search rules but should not be added, add an Exclusion Filter here. This might include:

- Internal users who do not have outside email addresses
- Printers, conference rooms, and other non-user resources
- Users who should not receive mail filtering



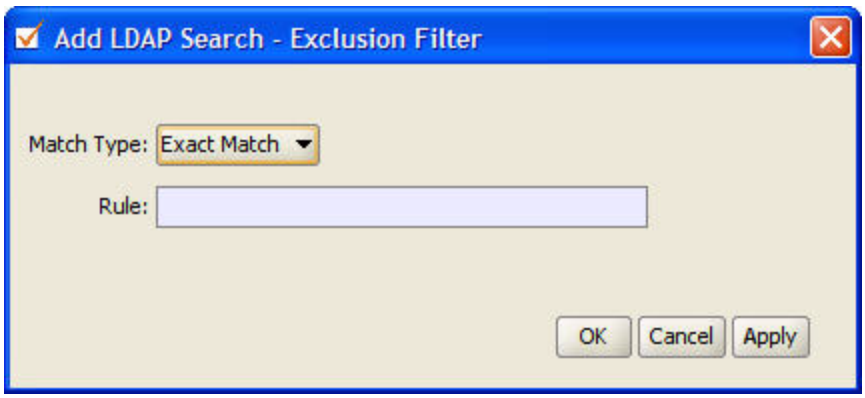
This page shows the list of exclusion filters. In a new configuration, this will be an empty list. To add exclusion filters, click the Add Exclusion Filter button at the bottom of the screen.

On the list of Exclusion Filters, you can change existing filters:

- Reorganize: Click the up arrow or down arrow icon to change the order of exclusion filters.
- Edit: Click the notepad icon to edit the settings of an exclusion filter.
- Delete: Click the X icon to delete the exclusion filter.

Add Exclusion Filter

Click the Add Exclusion Filter at the bottom of the page to exclude a user or organization in your LDAP server from synchronization.

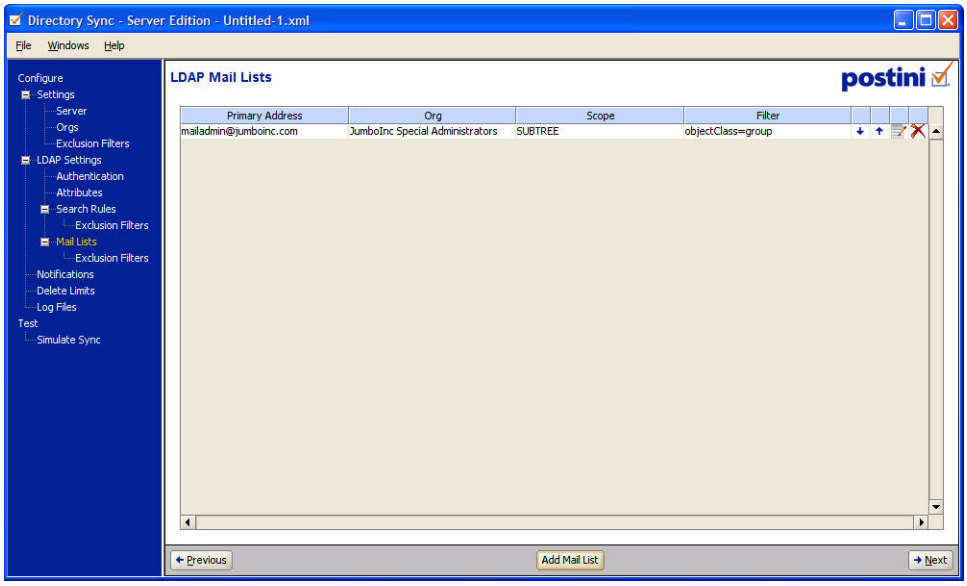


Specify the following:

Setting	Description
Match Type	The type of rule to use for the filter. • **Exact Match:** The address must match the rule exactly. Example: `maria@jumboinc.com` would exclude only the user `maria@jumboinc.com`. • **Substring Match:** The address or organization name must contain the text of the rule as a substring. Example: “test” would exclude `testadmin@jumboinc.com` and `salestest1@jumboinc.com`. • **Regular Expression:** The address or organization must match the regular expression specified. Example: `internal*@jumboinc.com` would exclude `internalhelpdesk@jumboinc.com` and `internal@jumboinc.com`.
Rule	The text of the match or regular expression to compare. See above for examples. Users that meet the requirements for an exclusion filter (or users in orgs that meet the requirements) will not be added as users in the message security service, and will be removed if they are listed there.

Mail Lists

Mailing lists are a special kind of email address that direct mail to many addresses at once. Most administrators prefer to create mailing lists as aliases to a separate user in the message security service, to avoid administrative notifications and quarantine summaries going out to all the members of a mailing list.



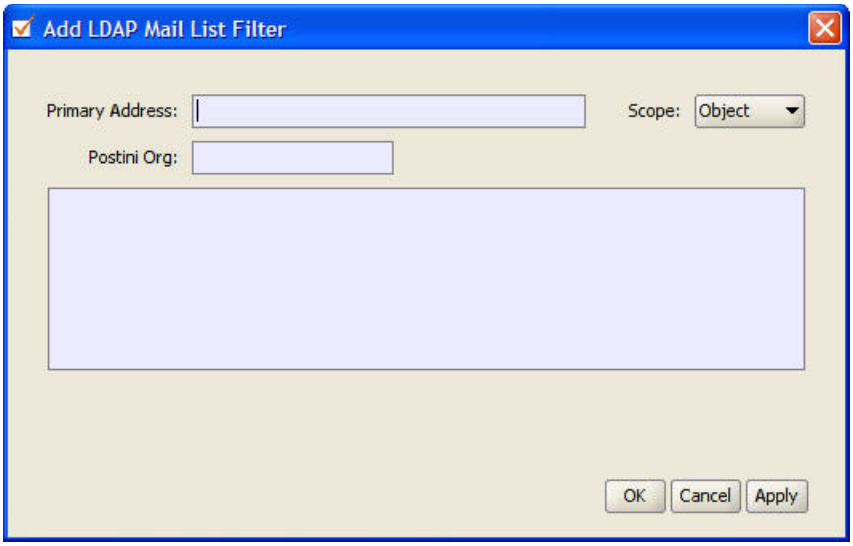
This page shows the list of LDAP Mail List rules. In a new configuration, this will be an empty list. To add mail lists, click the Add Mail List button at the bottom of the screen.

On the list of Mail List rules, you can change existing filters:

- Reorganize: Click the up arrow or down arrow icon to change the order of exclusion filters.
- Edit: Click the notepad icon to edit the settings of an exclusion filter.
- Delete: Click the X icon to delete the exclusion filter.

Add Mail List

Click the Add Mail List at the bottom of the page to mark one or more addresses as mailing lists.



Specify the following:

Setting	Description
Primary Address	The email address of the user who will manage the Mail List. If this user is not a user in the message security service, the directory sync utility will add this user in the specified Postini Org. Example: `admin@jumboinc.com`
Postini Org	If the Primary Address does not exist on your LDAP server, the directory sync utility will add it to this organization. If the Primary Address already exists this field is not used. Example: JumboInc Special Administrators

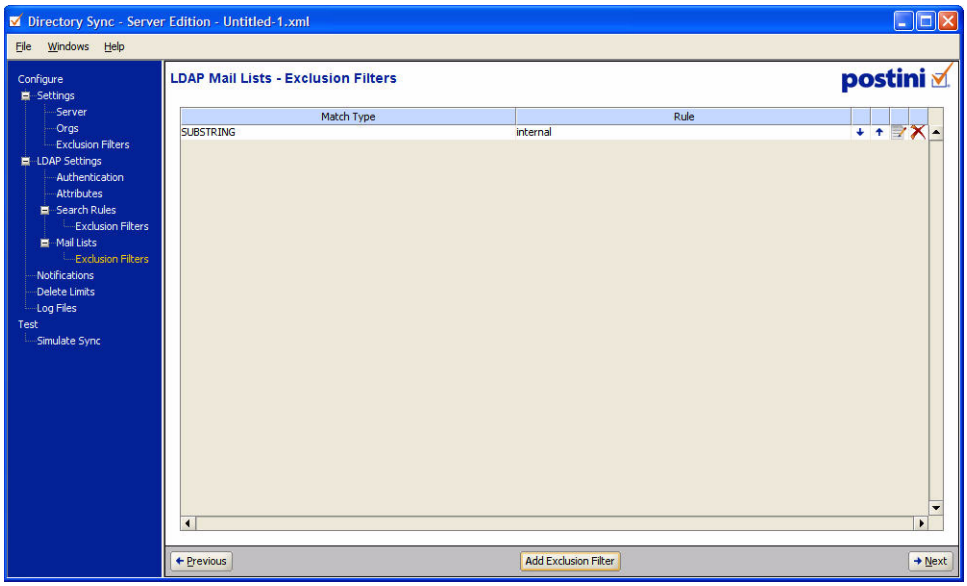
Setting	Description
Scope	Where to apply the Mail List rule. This could be a whole subtree, a single level, or a single object. • **Exact Match:** The address or organization name must match the rule exactly. • **Substring Match:** The address or organization name must contain the text of the rule as a substring. • **Regular Expression:** The address or organization must match the regular expression specified.
Rule	This field is not labelled. This is the search rule used. This rule uses standard LDAP filtering language, and allows sophisticated logic and complex rules for searching. For more information about LDAP search filter language, consult your LDAP documentation. Example: `(objectclass=dominoGroup)`

Exclusion Filters

You can exclude particular addresses from being treated as mailing lists.

Important: Mailing List Exclusion Filters do not function in Release 1.2.22.

If you have any entries in your Active Directory that match a Mail List rule, but should not be treated as a mailing list, list them here.



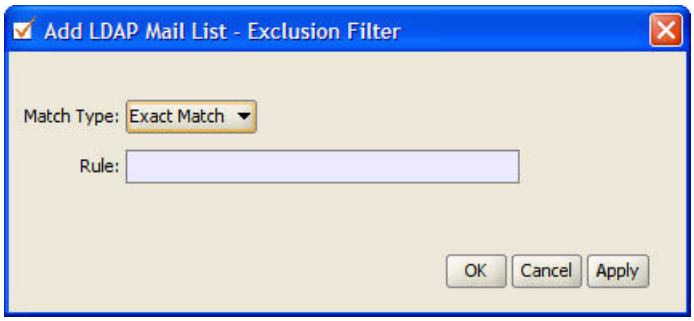
This page shows the list of exclusion filters. In a new configuration, this will be an empty list. To add exclusion filters, click the Add Exclusion Filter button at the bottom of the screen.

On the list of Exclusion Filters, you can change existing filters:

- Reorganize: Click the up arrow or down arrow icon to change the order of exclusion filters.
- Edit: Click the notepad icon to edit the settings of an exclusion filter.
- Delete: Click the X icon to delete the exclusion filter.

Add Exclusion Filter

Click the Add Exclusion Filter at the bottom of the page to prevent an address from being treated as a mailing list.



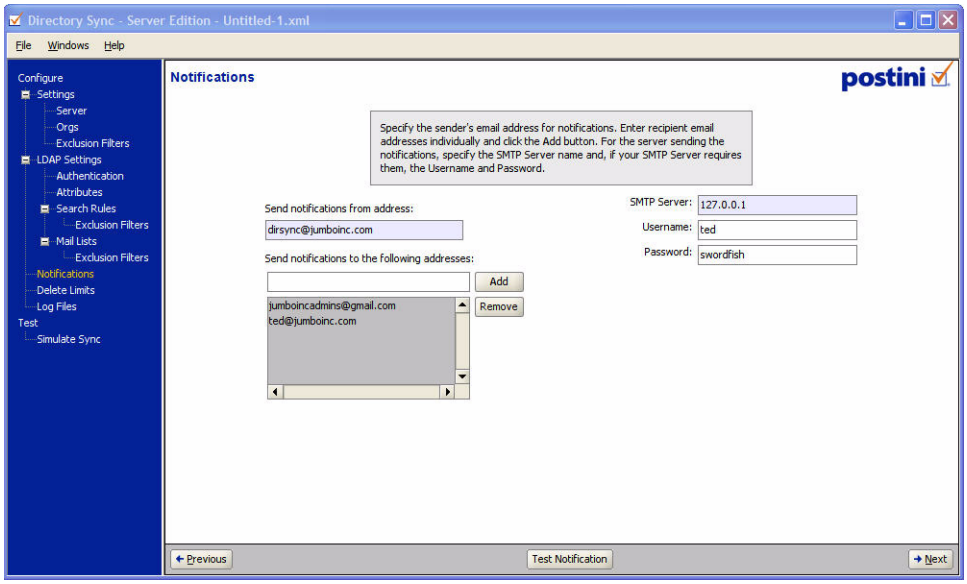
Specify the following:

Setting	Description
Match Type	The type of rule to use for the filter. • **Exact Match:** The address or organization name must match the rule exactly. • **Substring Match:** The address or organization name must contain the text of the rule as a substring. • **Regular Expression:** The address or organization must match the regular expression specified.
Rule	The text of the match or regular expression to compare. Addresses that meet the requirements for an exclusion filter (or users in orgs that meet the requirements) will not be added as mailing lists.

Notifications

You can set Configuration Manager so that every time synchronization occurs, Directory Sync Server Edition will send out a notification to a list of users.

Consider adding a notification to send mail to your own address, and possibly the addresses of any concerned parties in your company.



Specify the following:

Setting	Description
Send notifications from address	Enter the “From:” address for the notification mail. Recipients will see this address as the notification sender. For instance, you might use your own email address. Example: dirsync@jumboinc.com
Send notifications to the following addresses	Notifications will be sent to all addresses on this list. Enter any valid email address on any domain. Enter each recipient email address individually, then click the Add button. Depending on your mail server settings, the directory sync utility may be unable to send mail to external email addresses. Run a Test Notification to confirm that mail is sent properly. Example: `dirsync-admins@jumboinc.com`

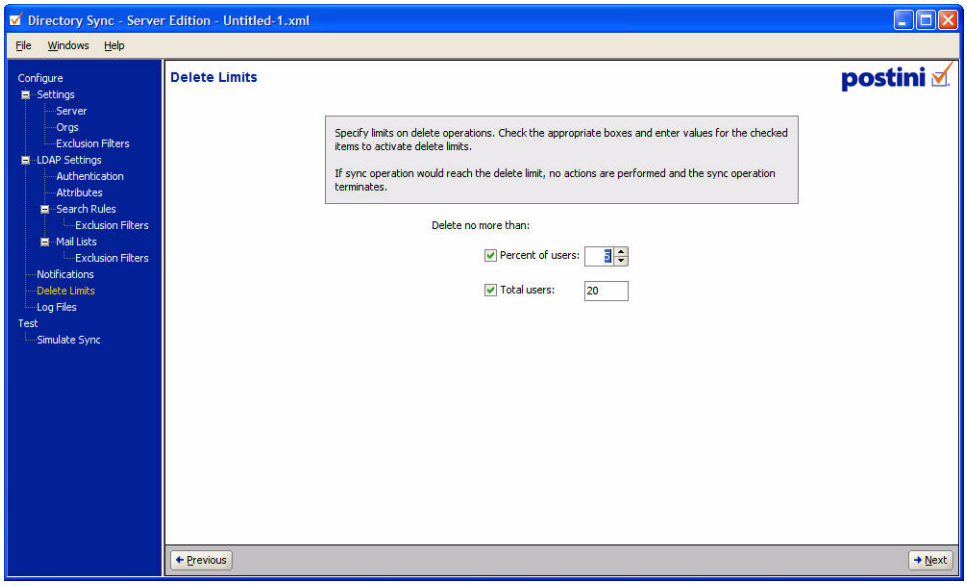
Setting	Description
SMTP Server	The SMTP mail server to use for notifications. Directory Sync Server Edition does not include an outbound mail server, and will connect to the mail server you specify. Example: `127.0.0.1` to run the mail server on the same machine. Example: `mail.jumboinc.com`
Username	If the SMTP server you specify requires SMTP Authentication, enter the user name to use here. Example: `admin5`
Password	If the SMTP server you specify requires SMTP Authentication, enter the Password to use here. Example: `swordfish` **Note:** Like all configuration settings, passwords are stored in an unencrypted XML file.

Test Notification

Click this button to test notifications. Configuration Manager will connect to the SMTP server you specified and send a test notification to the addresses you list.

Delete Limits

As a safeguard, you can limit how many users Directory Sync can delete while synchronization. This is recommended as a way to prevent accidental mass deletion.



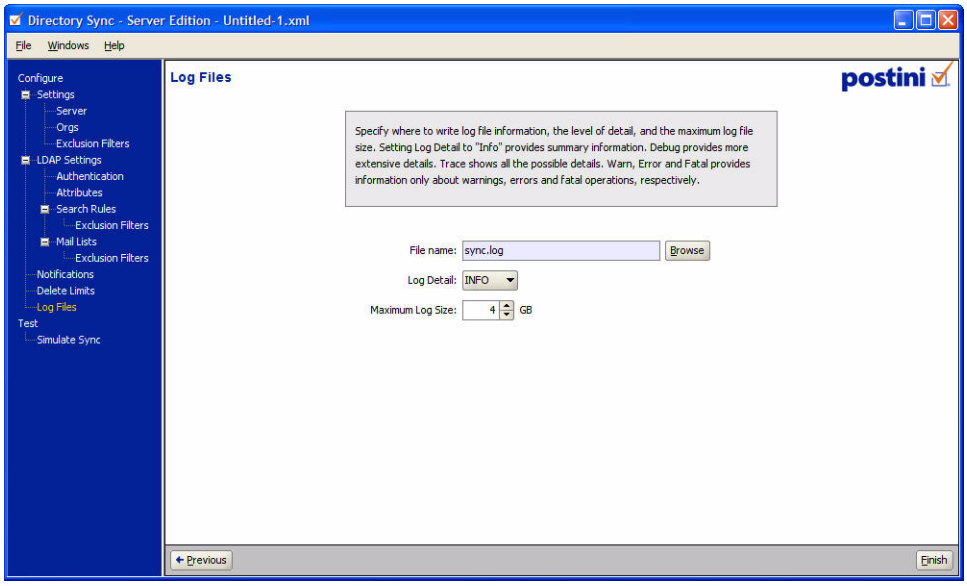
Note: Delete Limits apply during synchronization, but not during simulation. Simulation results will not include Delete Limits.

To set a delete limit, specify one or both of the following:

Setting	Description
Percent of users	Specify a maximum percentage of users that can be deleted. This is a percentage of the users registered on the message security service, not a percentage of users on your LDAP server. Example: 5%
Total users	Specify a maximum number of users that can be deleted. Example: 25

Log Files

You can specify the file name and level of detail of logging for Directory Sync Server Edition.



Specify the following:

Setting	Description
File name	Enter the directory and file name to use for the log file or click Browse to browse your file system. Example: `sync.log`

Setting	Description
Log Detail	The level of detail of the log. Options are FATAL, ERROR, WARN, INFO, DEBUG, TRACE, WARN, ERROR and FATAL. The level of detail is cumulative: each level includes all the details of previous levels. ERROR includes all ERROR and FATAL messages, and so on. • FATAL only logs fatal operations. • ERROR only logs errors and fatal operations. • WARN only logs warnings, errors and fatal operations. • INFO logs summary information. • DEBUG logs more extensive details. • TRACE logs all possible details.
Maximum Log Size	The maximum size of the log file, in gigabytes. When this file reaches half capacity, it is saved as a backup file (which overwrites any existing backup file) and a new file is created. At any time, the total size of these two files (the log file and the backup log file) will not exceed the total maximum size. Example: 4

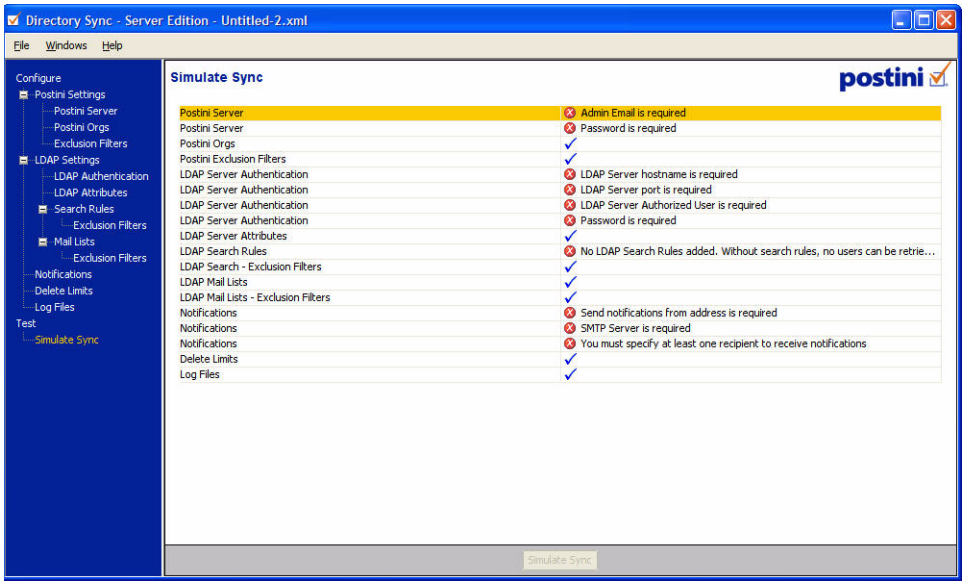
Test

After you enter configuration information, use this section to verify and test your Directory Sync settings.

Note: Configuration Manager does not check for valid LDAP syntax. To find invalid LDAP queries, use Simulate Sync. Invalid LDAP queries will cause errors.

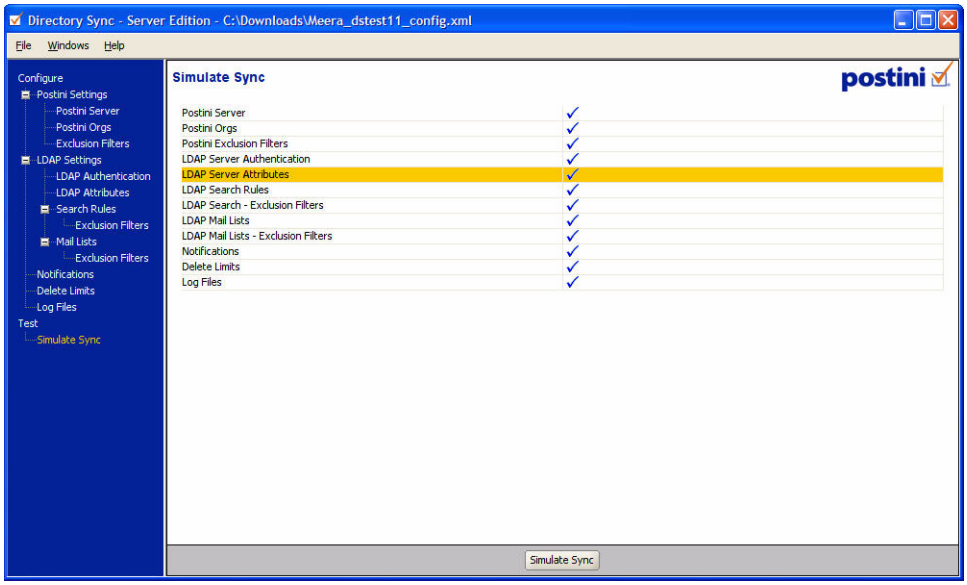
Simulate Sync

When you first go to this page, you will see Validation Results. This page will show a checklist of all the Configuration Manager sections. If you missing required information, you will see error messages showing what needs to be added.



Important: This checklist confirms only the minimum needed for synchronization. You may need to configure additional filters or rules to be sure the results are what you expect.

Once you've completed all required fields, you will be able to use the Simulate Sync button to simulate a synchronization.



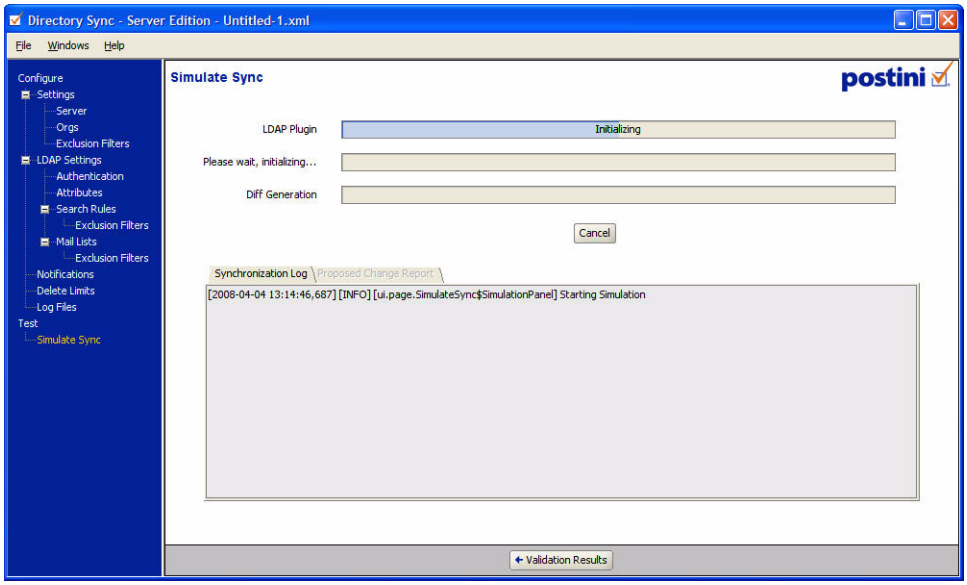
Once you're ready, click Simulate Sync. You will see the Simulate Sync page.

During simulation, Configuration Manager will:

- Connect to the message security service and generate a registered user list.
- Connect to your LDAP server and generate an LDAP user list.
- Generate a list of differences.
- Log all events.
- If connection was successful, show a Proposed Change Report which shows what changes would have been made to your message security service user list.

Note: Simulate sync will never update or change your LDAP server or your users in the message security service. The simulation is strictly for configuration and testing. To run an actual synchronization, use the command line. See "Synchronization" on page 53 for more.

Review the Simulation Results to confirm that the simulation occurred correctly without any unexpected results.



If any errors occur, check the error text. Most error text is human readable, but some error text may contain Java stack trace errors. If you need help troubleshooting these errors, see "Troubleshooting" on page 57.

If the synchronization was successful, check the Proposed Change Report and review it for unexpected results.

Note: The Proposed Change Report doesn't check your Delete Limits.

If you see any errors or unexpected results, you can go back and change your configuration to try again. To change your configuration, click on any of the headings on the left navigation bar.

You can switch between the Validation Results and Simulation Results pages using the buttons at the bottom of the page.

Once you are finished, save your configuration file and run synchronization. See “Synchronization” on page 53.

Chapter 5

Synchronization

About Synchronization

Run the synchronization command to push your LDAP directory server user information to the message security service.

The directory sync utility uses a command line command to run synchronization. The simple command line interface gives you the flexibility to incorporate synchronization into any scripting or scheduling you wish to use.

Before you can synchronize the message security service with your LDAP directory server, you must create rules that detail how to connect to both servers, and what filters and rules to use. These rules are stored in an XML file. To create this XML file, run Configuration Manager. For more information about Configuration Manager, see “Configuration” on page 19.

Most administrators run their first synchronization manually to test the process, import an initial set of users, and confirm the changes. After initial synchronization with the command line, you can set up automatic scheduling for future synchronization.

Command Line Synchronization

The directory sync utility uses a command line to run synchronization. This allows simple synchronization and flexible scheduling.

Before you can run synchronization, create a Configuration XML file using the Configuration Manager user interface. For more information, see For more information about Configuration Manager, see “Configuration” on page 19.

The command line to use for all platforms is

```
sync-cmd
```

Run without any arguments, this command gives an error and directs you to run `sync-cmd -h` for help.

To synchronize, use the following command line to read a configuration file, connect to both servers, generate a list of changes, and apply those changes:

```
sync-cmd -a -c [filename]
```

Replace `[filename]` with the name of the XML file you created in the Configuration Manager.

Synchronization options

The table below describes the possible arguments to the `sync-cmd` command. You can also see this information by running the following:

```
sync-cmd -h
```

in the directory where the directory sync utility is installed.

Option	Values
`-r,--report-out`	Write reports to the specified output file, in addition to writing them to the log.
`-V`	Display detailed application version information.
`-a,--apply`	Apply detected changes.
`-c,--config [filename]`	Specify the configuration to load. Synchronization will not occur without a valid XML file for this argument.
`-h,--help`	View this information and exit.
`-l,--loglevel [level]`	Override the default and/or configured log level with the specified value. Valid values (in increasing order of verbosity) are FATAL, ERROR, WARN, INFO, DEBUG, and TRACE.
`-v`	Display short application version information.

Scheduling Synchronization

Once you have successfully run a manual synchronization, you can set up automatic synchronization. Use existing third-party scheduling software to automate synchronization.

In most cases, scheduling twice a week is recommended. The exact timing will vary based on the number of users you have and how often you need to update them. A large company with many users changing frequently may need to run the directory sync utility daily, while a small company with few changes may not need to run the utility more than once a week.

The exact method to schedule this task depends on the operating system in which the directory sync utility is installed. In Microsoft Windows, use Scheduled Tasks. In Linux or Solaris, use cron. Steps for how to do this are listed below. You can also use any other scheduling software that can launch commands from the command line interface.

Microsoft Windows: Scheduled Tasks

In Microsoft Windows, schedule synchronization using Scheduled Tasks.

Note: These steps apply to most common Microsoft Windows configurations. Scheduled Tasks is a third-party product and is not supported directly. In the event of a Scheduled Tasks issue, contact your Windows administrator.

To schedule a task

1. In Control Panel, open Scheduled Tasks.
2. Double-click Add Scheduled Task.
3. Complete the Scheduled Task wizard using the following information. (Steps may vary depending on your version of Microsoft Windows.)
   - Choose the program `sync-cmd.exe`, located where the directory sync utility is installed.
   - The frequency of the task depends on your synchronization needs. For most environments, twice per week is appropriate.
   - Use Advanced Properties to specify an exact command line. The appropriate command line is:

     ```
     [path]\sync-cmd -a -c [filename]
     ```

     Replace `[path]` with the path where the directory sync utility was installed. Replace `[filename]` with the name of the XML file you created in the Configuration Manager.
4. Test the scheduled task by running manually once. In the Scheduled Tasks window, right-click the task you created and select Run from the right-click menu. Check the log file for errors.

Linux and Solaris: cron

In Linux and Solaris environments, schedule synchronization using `crontab`.

Note: These steps apply to most common Linux and Solaris configurations. Linux and Solaris are third-party products and are not supported directly. In the event of an issue with cron, contact your administrator.

To add a cron job

1. Run `crontab -e` to update the `crontab` file.

2. Add a line in the `crontab` file for the following command:

   ```
   sync-cmd -a -c [filename]
   ```

   The syntax of this line will depend on your operating system and version of cron. For instance, to schedule the task to run at 3:30 AM twice per week, on Monday and Thursday, add the following entry:

   ```
   30 3 * * 1,4 [path]/sync-cmd -a -c [filename]
   ```

   Replace `[path]` with the path where the directory sync utility was installed.Replace `[filename]` with the name of the XML file you created in the Configuration Manager.

3. Save the `crontab` file and exit your text editor.

Chapter 6

Troubleshooting

About Troubleshooting

This chapter covers information about how to troubleshoot any problems that may occur with Directory Sync Server Edition.

Troubleshooting information includes common issues, system tests, and researching issues.

Common Issues

The following describes common issues and questions with directory sync and common resolution.

A mailing list rule or exclusion rule doesn't seem to be doing anything.

Check the scope of the rule. You may need to set the scope to SUBTREE.

A mailing list rule generates errors.

Check the Mailing List Attribute in LDAP Configuration. This is the field that contains the email address of a mailing list. In most cases, this will be mail.

The proxy environment requires a password challenge for external web access.

The directory sync utility can use a proxy server but cannot respond to password challenges. To run synchronization, you will need to change your network setup to allow the directory sync utility to connect without a password challenge, or without a proxy server.

The Base DN information doesn't seem to be correct.

Check to be sure your Base DN doesn't include any spaces.

How do I find out information about my LDAP server fields?

You will need to download an LDAP browser. An LDAP browser allows you to browse through an LDAP directory server and identify all fields and values. Most directory servers do not include a complete LDAP browser.

To install an LDAP browser:

1. Go to www.google.com
2. Search for “download LDAP browser” and choose a browser.
3. Download and install the LDAP browser.

Cannot simulate sync because Notifications server not specified.

To run synchronization, you will need a server capable of sending mail. If you are running directory sync on a mail server machine, you can use the IP address 127.0.0.1 for your mail server. Otherwise, contact your mail administrator for the correct mail information.

System Tests

If you encounter problems, use the tests in Configuration Manager to find the problem:

1. In Configuration Manager, open the XML file you are using for configuration.
2. Under Server, click Test Connection to confirm you can connect to the message security service.
3. Under LDAP Server, click Test Connection to confirm you can connect to your LDAP server.
4. Under Notifications, click Test Notification to confirm you can send a test notification.
5. Under Test, confirm you have filled out all required fields.
6. Under Test, click Simulate Sync to confirm that synchronization is running properly.

If you encounter any problems, not which tests failed and confirm that the configuration information is correct for those sections of Configuration Manager.

Escalating Problems

If you are unable to run directory sync, and cannot resolve the problem using system tests, collect the following information for troubleshooting:

- The most current sync log file, located in the folder where the directory sync utility is installed.
- The version number of the directory sync utility you are running. You can find this in the Configuration Manager UI by going to Help->About, or you can run the command `sync-cmd -V`.
- The current config file you are using. This is an XML file (default name sync.xml) located in the same folder where the directory sync utility is installed.
- The brand and version of the LDAP directory server you're using.
- The operating system on the machine where the directory sync utility is running.

Once you have collected this information, escalate this using your normal support channels. For more information about support for Directory Sync Server Edition, see the Directory Sync Server Edition site:

```
http://www.postini.com/dir_sync
```