# Synchronization Tool Administrator Guide

Symantec.cloud™

# Synchronization Tool Administrator Guide

Documentation version: 1.0

## Legal Notice

Symantec Corporation
350 Ellis Street
Mountain View, CA 94043

http://www.symantec.com

Clients are advised to seek specialist advice to ensure that they use the Symantec.cloud services in accordance with relevant legislation and regulations. Depending on jurisdiction, this may include (but is not limited to) data protection law, privacy law, telecommunications regulations, and employment law. In many jurisdictions, it is a requirement that users of the service are informed of or required to give consent to their email being monitored or intercepted for the purpose of receiving the security services that are offered by Symantec.cloud. Due to local legislation, some features that are described in this documentation are not available in some countries.

Configuration of the Services remains your responsibility and entirely in your control. In certain countries it may be necessary to obtain the consent of individual personnel. Symantec.cloud advises you to always check local legislation prior to deploying a Symantec.cloud service. You should understand your company’s requirements around electronic messaging policy and any regulatory obligations applicable to your industry and jurisdiction. Symantec.cloud can accept no liability for any civil or criminal liability that may be incurred by you as a result of the operation of the Service or the implementation of any advice that is provided hereto.

The documentation is provided "as is" and all express or implied conditions, representations, and warranties, including any implied warranty of merchantability, fitness for a particular purpose or non-infringement, are disclaimed, except to the extent that such disclaimers are held to be legally invalid. Symantec Corporation shall not be liable for incidental or consequential damages in connection with the furnishing, performance, or use of this documentation. The information that is contained in this documentation is subject to change without notice.

Symantec.cloud may at its sole option vary these conditions of use by posting such revised terms to the Web site.

# Technical Support

Welcome to the 7 x 24 x 365 Global Client Support Center

The Global Client Support Center works in partnership with our clients and continually seeks to develop a consistently high level of service. The team consists of technically-trained client-focused individuals. They respond to your issue with the aim of resolving in within the first contact. The team know they are responsible for listening, understanding, and resolving your issues with passion and a smile.

Always feel free to call us as part of the escalation process or at any other time. Full contact and escalation details are available in the following PDF document:

Contact and Escalations document

## Contacting Technical Support

If you have a technical support question or issue and cannot find the information you need, contact the GCSC Team on the following contact details.

To reduce the time it takes to resolve an issue, before you contact the team, please see the short document, Contacting MessageLabs GCSC. The document explains the information that is required for the various types of support issue.

| | |
|---|---|
| Email us at: | support@messagelabs.com |
| Call us on: | EMEA: +44 (0) 870 850 3014 or +44 (0)1452 627766<br>US: +1 (866) 807 6047<br>Asia Pacific: +852 6902 1130<br>Australia: 1 800 088 099<br>New Zealand: 0800 449 233<br>Hong Kong: 800 901 220<br>Singapore: 800 120 4415<br>Malaysia: 1 800 807 872<br>South Korea: 00798 14 800 6906 |
| Open a support ticket in ClientNet | Log into https://clients.messagelabs.com and navigate to **Support > Ticketing** |
| Visit the Web site: | www.messagelabs.com |

| | |
|---|---|
| Visit the Online Help | Online Help |

## Service and maintenance alerts

We recommend that you use ClientNet frequently to check for maintenance information and to keep up to date with what’s new in Symantec.cloud.

We also advise you to add your mobile numbers to ClientNet in the **SMS Alerts** section. We can then advise you of critical service-related issues by text message.

## Feedback

We welcome comments and questions about the services and the features that are described in this documentation. Please let us know how your Symantec.cloud service performs. You can also provide suggestions as to how Symantec.cloud can further support your business needs. Please email us at.

helpfeedback@messagelabs.com

If you raise an issue with GCSC, they send you a short survey each time they resolve and close an incident. Your feedback is taken on board, whether good or bad and about product, service, or support . Where you express dissatisfaction, we will contact you.

# Contents

Chapter 1

# Introduction to the Synchronization Tool

This chapter includes the following topics:

## Introduction to the Synchronization Tool

Symantec.cloud provides the Synchronization Tool to assist you in supplying and maintaining data required by the Email Content Control, Web Security, and Instant Messaging Security Services. The tool is also known as Schemus. The Synchronization Tool gives you complete control of what and when you want to synchronise with us.

The Synchronization Tool extracts user data from a variety of directory sources and synchronizes these with the Email Content Control, Web Security, and IM Content Control services. Using the synchronization tool ensures that information from a variety of sources is synchronized with theSymantec.cloud infrastructure. The Synchronization Tool's capabilities are defined by one or more license keys, provided by Symantec.cloud, and allow a combination of the following synchronization types:

| | |
|---|---|
| Mail synchronization | To synchronize email addresses |

| | |
|---|---|
| Group and User synchronization | To synchronize:<br>■ Users<br>User identities, email addresses, group membership, and IM accounts<br>■ Groups<br>Group identities |

Use Mail synchronization for keeping registered email addresses up to date for the Address Registration feature.

Use Group and User synchronization for keeping user and group data up to date for the Email Content Control and Instant Messaging Security Services rules and for the Web URL Filtering policy rules.

The Synchronization Tool guides you through the configuration process to extract the required data from your directory system. Once correctly configured, the synchronization process can either be run from the Synchronization Tool interface or from the command line. The process can be scheduled to operate automatically. The Synchronization Tool can also send email notifications reporting its outcome at each invocation.

See “Synchronization Tool Overview” on page 8.

See “Synchronization Tool Features” on page 9.

See “Mail Synchronization” on page 10.

See “Group and User Synchronization” on page 10.

# Synchronization Tool Overview

The Synchronization Tool is a Java executable that operates on a range of platforms supported by the Sun Java Runtime Environment (JRE). The tool operates either in an interactive mode through a GUI or as a command-line application suitable for invocation by other scheduling services (such as Windows Scheduler). In the interactive mode, a wizard guides you through the steps to establish connection and data extraction from LDAP-based directory sources, with testing and verification of each step.

The tool is installed on a suitable system within your network, thus simplifying the task of accessing local directories and minimizing security risks. This is done by ensuring that direct access to your directories from outside the firewall is not required.

When run interactively, a full update of all data may be performed. When run from the command line, the tool calculates the incremental changes since the last run and passes only these changes to Symantec.cloud.

See “Introduction to the Synchronization Tool” on page 7.

See “Synchronization Tool Features” on page 9.

See “Mail Synchronization” on page 10.

See “Group and User Synchronization” on page 10.

# Synchronization Tool Features

The Synchronization Tool provides the following features:

| | |
|---|---|
| Wizard-based configuration | Guiding the user through each configuration step |
| Templates for common mail system directories | Including Microsoft Exchange 2000 and 5.5 |
| Configuration testing | Checking of each wizard step, and full configuration verification |
| Filtering | Allowing specific or "wild-carded" addresses to be excluded or converted |
| Safety thresholds | Update limits may be set to detect anomalous situations |
| Reporting | Comprehensive logging and optional alerting by email notifications |
| Custom configuration | Advanced settings to refine the LDAP operations |
| Multi-platform operation | A direct benefit of Java application portability |
| Referral checker | Checks the integrity of continuation references to other LDAP directory servers |
| Full control of automation | Invocation within the application using the from task schedulers or by other client tools |
| Safe test mode | No modification of live data using test output to text files |

See “Introduction to the Synchronization Tool” on page 7.

See “Synchronization Tool Overview” on page 8.

See “Mail Synchronization” on page 10.

See “Group and User Synchronization” on page 10.

# Mail Synchronization

Mail Synchronization is used to automate the process of updating your valid address list for theAddress Registration service. Address Registration enables Email Services clients to protect themselves from dictionary-type spam attacks, by registering their valid email addresses. Symantec.cloud then rejects any email destined for invalid addresses. The Synchronization Tool extracts address data from your directory data sources and exports this data to the Symantec.cloud infrastructure.

**Warning:** You should either use the Synchronization Tool or ClientNet (the latter, in combination with outbound harvesting) to maintain your valid address list and not both together. Using both techniques together may lead to inaccuracies in your address list data.

See “Introduction to the Synchronization Tool” on page 7.

See “Synchronization Tool Overview” on page 8.

See “Synchronization Tool Features” on page 9.

See “Group and User Synchronization” on page 10.

# Group and User Synchronization

Group and User synchronization lets you use your existing directory definitions of users and groups within your Symantec.cloud Email Content Control and IM Content Control and Web URL Filtering rules. The Synchronization Tool extracts User and Group membership data from your directory data sources and exports this data to the Symantec.cloudinfrastructure. The tool operates alongside the ClientNet portal that enables you to upload and manage custom users and groups.

See “Introduction to the Synchronization Tool” on page 7.

See “Synchronization Tool Overview” on page 8.

See “Synchronization Tool Features” on page 9.

See “Mail Synchronization” on page 10.

# Getting set up

This chapter includes the following topics:

## Preparation

You will need to decide on a suitable system within your network on which to install and run the Synchronization Tool. This system should have internal network access to your directory system through LDAP and have external network access to the Symantec.cloud service through HTTPS.

If you intend to run the tool on an automated basis, you should also decide on whether the tool is to be invoked by a scheduling system (e.g. Microsoft Windows Scheduler) or by other applications. For automated use it is important to note that the tool builds a local database for the purposes of tracking changes to your source data. Therefore, it is best if only a single instance of the tool synchronizes a given set of source data.

# Prerequisites

Before downloading the Synchronization Tool from ClientNet, decide whether you need the version of the Synchronization Tool with or without the Java Runtime Environment (JRE). If you already have JRE 1.5 or later, either download image may be used; otherwise, you must download the image with the JRE included. For details of how to discover the JRE you are running and the affect of using the Synchronization Tool with a JRE.

See "About the Java Runtime Environment" on page 51.

Before starting, ensure that you have the following items to hand:

- Symantec.cloud ClientNet portal account details

  **Note:** Symantec.cloud recommends that for security and control purposes, you set up a ClientNet account specifically for use with the Synchronization Tool. This will help to avoid any changes being made to the account that may interfere with the Synchronization process, for example, password changes. The account must be a global administrator account.

- The Synchronization Tool license key:
  See "Obtaining a license key for Mail Synchronization" on page 13.
- The address of your Directory Server and any authentication details you might need to be able to perform searches on it
- Authentication may be possible anonymously.

# Downloading the Synchronization Tool for Mail Synchronization

**To download the Synchronization Tool from ClientNet**

1. Select **Configuration > Email Services > Platform > Tools**
2. Download the Disclosure Agreement by clicking the **attached statement** link.
3. Email the Disclosure Agreement to:

   addressregistration@messagelabs.com

   You will be sent an email containing credentials and a URL to the site from which you can download the Synchronization Tool. Before downloading the Synchronization Tool, you must request a license key.

   See "Obtaining a license key for Mail Synchronization" on page 13.

# Obtaining a license key for Mail Synchronization

To use the Synchronization Tool for synchronizing your email address, user and group data, you will need to acquire a license key.

You can use the tool without a key, to prepare and test for live synchronization, by using the text file export capability to assess the collection of data.

Separate licenses are required for Mail synchronization and for Group and User Synchronization.

You only need one license to synchronize user and group data for the Email Content Control, Web Security, and Instant Messaging Security Services.

A key can be requested in ClientNet. You will receive it in a confirmation email from a Client Services representative after they have verified your details.

**To request a key from ClientNet**

1. Select **Configuration > Email Services > Platform > Tools**.
2. In the **Synchronization Interface Activation** area, click the **Request key** button.
3. Enter your name and check the email address to receive the key.
4. Select the checkbox according to the synchronization type you want to use.
5. Click **OK**.

# Downloading the tool for Group and User Synchronization

**To download the Synchronization Tool from ClientNet**

1 Select either:

1. **Configuration > Web Security Services Configuration > Tools > Tool Download**

or

2. **Configuration > Instant Messaging Security Service Configuration > Setup > Tools**

2 Download the Disclosure Agreement by clicking the **attached statement** link.

3 Email the Disclosure Agreement to:

addressregistration@messagelabs.com

You will be sent an email containing credentials and a URL to the site from which you can download the Synchronization Tool. Before downloading the Synchronization Tool, you must request a license key.

See “Obtaining a license key for Group and User Synchronization” on page 14.

See “About the Java Runtime Environment” on page 51.

# Obtaining a license key for Group and User Synchronization

To use the Synchronization Tool for synchronizing your Group and User data, you will need to acquire a license key.

A key can be requested from the ClientNet portal and will then be displayed within the request page.

**To request a key from the ClientNet portal**

1 Select either:

a. **Configuration > Web Security Services Configuration > Tools > Tool Download**

or

b. **Configuration > Instant Messaging Security Service Configuration > Setup > Tools**

or

c. **Configuration > Email Services > Platform > Tools**

2 In the **Synchronization Interface Activation** area, click the **Request** button.

The key is automatically created and displayed on screen.

When you download the key from the **Email Services > Platform > Tools** page, enter your name, check the email address to receive the key, and check **Address Registration and Users and Groups**.

You can use the tool without a key to prepare and test for live synchronization. To do so, use the text file export capability to assess the collection of data.

Separate licenses are required for Mail synchronization and for Group and User Synchronization.

You only need one license to synchronize user and group data for the Email Content Control, Web Security, and Instant Messaging Security Services.

**Note:** To use Group and User synchronization for the Email Content Control service, the ClientNet administrator must have **Edit Configuration** permission for the **LDAP User Groups** service.

# Installing the Synchronization Tool

Linux

Once you have downloaded the installer, open a terminal, ensure that execute permission is set on the installer file, and then run it. For example:

```
$ chmod +x Schemus_linux_jre.sh
$ ./Schemus_linux_jre.sh
```

Before starting the Synchronization Tool installation, take the usual precaution of ensuring that all other applications running on the computer are closed.

Throughout the installation click **Next** to progress to the next stage. When the **Next** button is disabled, additional information is required on the window before you can continue.

See “Downloading the Synchronization Tool for Mail Synchronization” on page 13.

**To install the Synchronization Tool**

1. Run the installer.
2. Click **Next**.

   In the license agreement window, read the agreement, and if your company is in agreement with the conditions, click **I accept the agreement**, and then click **Next**. The installation location window is displayed.
3. Select the directory in which to install the Synchronization Tool; for example, `C:\Program Files\schemus`. Click **Next**.

   Select where to launch Schemus from; the **Start** menu for Windows, and Symlinks for Linux.

   - Windows
   - Linux
4. Click **Next**. The installation starts.

   Once the copying of files has completed, the installer displays any release notes and change logs. The release notes contain any additional information that has been introduced since this guide was written. Additional features and bug fixes appear in this list as well as the history of changes.
5. Click **Next** to move to the end of the installer
6. Click **Finish** to quit the installer.

# First time settings

The first time that the Synchronization Tool is started, it prompts you to enter the type of synchronization that you will use for the Synchronization Tool. The options are 'Mail' or 'Group + Users' Synchronization. You can set up a configuration for Mail, Group, and User synchronization at the same time, but Symantec.cloud does not recommend this.

The Synchronization Tool only prompts you for this setting the first time it is run. To change this setting, select **Edit > Settings > Synchronization**.

**Note:** Selecting an option for which you do not have a valid license key enables the Synchronization Tool in Safe Test Mode only. This provides test output to text files.

See “Synchronizations” on page 26.

# Symantec.cloud settings

### To enter Symantec.cloud settings

1. Start the Synchronization Tool and select **Edit > Settings**.
2. Enter the client identity and the associated license key.
3. Click on **Symantec.cloud** in the left panel.

   The Access URL is the address used to connect to Symantec.cloud and it is unlikely you will want to change this setting.
4. Enter your Symantec.cloud account **Username** and **Password** and click **Apply**.

   If you see an error message, your local network may be set up to prohibit direct access to the Internet for HTTPS (that is, secure HTTP communication).
5. Click **OK** to close the **Schemus settings** window.

See “License” on page 26.

# Creating a new configuration

Before you can synchronize your data, you must create a configuration profile specifying the data source and destination systems.

### To create a new configuration

1. To create a profile for the first time, do one of the following:

   - Click the **New Configuration** button in the center of the window
   - Click the **New** button to the right of the **Configuration** drop-down list
   - Select **New** from the **File** menu

   The first window of the configuration wizard is displayed. The wizard will lead you through the configuration process. At each stage of the wizard the **Next** button is enabled if sufficient details have been entered to let you proceed.

   The panel on the left hand side of the window displays how far through the creation process you are. To modify a previously completed screen in the wizard, either click the appropriate heading on this panel or successively click the **Back** button. As you progress through the wizard the panel names are enabled behind your current position. If you are modifying an existing configuration, all entries will be available in the left panel.

| | |
|---|---|
| Group and User Synchronization | Group and User synchronizations are two separate types of synchronization and require a separate configuration each. If you are configuring both of these types, you will need to proceed through the configuration wizard twice. |

2 Enter a **Configuration Name**.

The name of the configuration must be unique. It can contain most characters allowed by your operating system. When the Synchronization Tool is used from the command line this name is used to specify the configuration to use. For this reason, we recommend that you restrict the characters to alphanumeric so that the name can be given as a command line parameter easily.

| | |
|---|---|
| Mail Synchronization | If you checked **Mail** in the first time settings, Schemus assumes that you are creating a mail configuration. The Synchronization Type drop-down list is not displayed.<br>See “First time settings” on page 16. |
| Group and User Synchronization | Select either **Groups** or **Users** from the **Synchronization Type** list. Each synchronization type must be configured separately. |

3 Click **Next**.

The name at the top of the left hand side panel displays *example* and has as a suffix the synchronization type in brackets.

4 In the **Data source** window, the **Source Type** drop-down list contains types of LDAP servers and the setting **File**. Select the appropriate LDAP server from the list.

To configure multiple sources of data or if you would like to know how to source your data from a file:

See “The configuration wizard” on page 27.

If you use multiple configurations to synchronize to a single destination, Schemus lets you merge the second configuration with the first configuration by using the multiple sources facility.

Two separate configurations synchronizing to the same destination will overwrite each other's results.

5 Click **Next**.

6 In the **LDAP** window, complete the following:

- Enter the host name of your LDAP server. Unless you know otherwise, leave the port number as the default value (this differs depending on the authentication setting)
- Enter your user name and password to retrieve results from your LDAP server. To retrieve data from Active Directory, it is recommended that the user identity used has read only privileges equivalent to those of a domain administrator.
- It may be that your server lets you retrieve results anonymously, in which case, set the authentication to **anonymous**. However, some servers restrict the results returned to anonymous users.
  Click **Next**.

7 In the **LDAP search**, select the level to search on the hierarchical tree structure on the LDAP server.

Complete the following:

- In the **Search base** field, enter the path and directory to search, or select a directory from the drop-down list.
  Some LDAP servers will not let you search for entries at their root. It may be necessary to manually type in a search base before you can browse further.
- In the **Search scope** field, select whether attributes from the LDAP server are searched below the level set in the search base. Setting this to `Sub-tree` will return the most results.
- For most configurations it is not necessary to edit the **Search filter** field or use the advanced settings. The **Examples** button displays a list of common search filters for your selected directory type.
  For full details of configuring a search filter:
  See “Filters” on page 38.
  If you accidentally change one of these fields, or want to return to the top of your LDAP server's tree, click the **Defaults** button.
  See “Filters” on page 38.

Group and User Synchronization

The LDAP search configuration for Group and User configurations have an additional **Name template** field. The name template defines a rule for constructing a text name that will be used to represent individual users and groups. Using simple template replacement strings the name may be constructed from other LDAP attributes. Text enclosed in percent (%) symbols is treated specially as an attribute; otherwise it is just passed through as text.

See “LDAP search configuration page” on page 31.

8. Click **Next** to perform a search. Your search results are listed in the dialog box.

   If you do not see any results check that:

   - The **Source type** on the **Data Source** window is correct. Changing this setting automatically fills in a number of the advanced configuration settings.
     See “The configuration wizard” on page 27.
   - The **Search scope** on the **LDAP search** window is set to `Sub-tree`. This will return the most results.
   - The **Search base** is set to a suitably high position on your LDAP server's hierarchy, to encompass the mail addresses or groups and users that you are searching for.
   - The **Search base** has not accidentally been altered so that the location entered in this field does not exist. If in doubt, navigate to the top of the LDAP server tree and relocate the directory.
   - You have not accidentally changed the **Search filter**. To reset this setting, click **Defaults**.
   - Your authentication on the **LDAP** window is sufficient to return details from the LDAP server. If you have selected `anonymous` and no results are being returned, try selecting `simple` and enter a user name and password.

   Group and User Synchronization:

   The test results will show the names constructed by the **Name template**. Check that these are returning representative names, for example for users in a Microsoft environment, this should represent the domain\username identity of individual users.

9. Click **Next**.

10 In the **Data repository** window, select where to write your data to. Set the **Repository type** to `Symantec.cloud`.

If you have not yet entered your license details, you will not be able to synchronize your details with Symantec.cloud.

Click **Next**.

11 In the **ClientNet User setup** window, your Symantec.cloud user name and password details will already be set.

See “First time settings” on page 16.

12 Click **Next**.

| | |
|---|---|
| Mail Synchronization | The **Domain setup** window is displayed. There may be a slight delay while the Symantec.cloud service is contacted to retrieve your domain details. Select the domains to use by highlighting each domain, as required, and clicking the **>** button. The selected domain appears in the **Domains to use** list. |
| Group and User Synchronization | This window is not displayed for Group and User configurations. |

13 You have now completed the basic source and destination configuration required for this type of synchronization. Now you can set the following optional settings as required:

**Filters**

To exclude or change details as they are found on your LDAP server and before they are written to the Symantec.cloud server.

See "Filters" on page 38.

**Limits**

Enable you to protect an existing synchronization against accidental modification. Accidental modifications could result from misconfiguration of Schemus or from your LDAP server returning incorrect results. By setting limits on the maximum number of synchronization changes, a radical change in the number of additions, deletions, or modifications can halt the process, thereby safeguarding your data.

See "Limits" on page 39.

**Notification**

The notification settings request Schemus to send an email notification when a synchronization operation is completed, whether or not it was successful. If you are running the Schemus from the GUI, this should not be required. However, if you have scheduled Schemus to run from the command line, this option is strongly recommended.

See "Email notifications" on page 39.

14 Finally, the **Summary** window is displayed.

Verify your configuration settings for this synchronization type, by clicking **Verify** and then **Save**. If you want to perform a regular synchronization, you can click on the **Schedule** button.

See "Scheduling the synchronization" on page 41.

15 Click **Finish**. Or to configure a new synchronization type, select the required type and click **Add**.

Group and User Synchronization:

If you have just created a group configuration, you should select a **Synchronization Type** of **Users** and complete the configuration for that too.

# Synchronizing your data

Once you have created your configuration, you can synchronize your data with Symantec.cloud.

### To synchronize your data with Symantec.cloud

1 Select the required configuration from the drop-down list on the configuration window, or select **View > Configuration**.

The functions on the left panel are also accessible on the **Configuration** menu (except **Delete**, which removes your currently selected configuration and is only available on the menu).

The **Summary** window displays a summary of the synchronization. If you have multiple synchronization types, you can review the settings of each by clicking the **Mail**, **Groups**, and **Users** tabs. The **Schedule** button brings up a window to let you automatically run your Schemus configuration at a predetermined time using your operating system's scheduler. The **Modify** button enables you to edit your settings for the current synchronization type.

2 Choose one of the following methods of synchronizing your data:

**Test Update** Looks at the data on your source (file or LDAP server) and lists the additions, removals, or exclusions. It does not change any details on your repository. Tool tips (activated by leaving the mouse pointer over an entry or clicking on an entry in one of these columns) provide additional information about the entry. For users this will include email address and groups that the user is a member of.

**Update** Compares the details held in your local change tracking database and sends those that have been removed or added. This incremental update is an efficient way to pass changes to Symantec.cloud and preserve unchanged data.

**Replace** Recreates your local change tracking database and resends all data to Symantec.cloud.

**Refresh** Retrieves all data from Symantec.cloud and uses this to recreate your local change tracking database. This allows subsequent update operations to be based upon calculating changes from a current copy of the data held by Symantec.cloud.

To view the results once an update has completed, click **Mail**, **Groups**, and **Users**, as appropriate. To sort the list, click the gray title bar of the column to sort.

To halt the synchronization, click **Stop** (only enabled while synchronization is in progress).

Chapter 3

# Synchronization Tool in Detail

This chapter includes the following topics:

- License
- Synchronizations
- Log settings
- LDAP
- Symantec.cloud
- The configuration wizard
- LDAP server configuration page
- LDAP search configuration page
- Groups
- Filters
- Limits
- Email notifications
- Summary and verification
- Scheduling the synchronization
- The main page
- Logging

- Directory referral checker
- Command line operation

# License

To use the full functionality of Schemus, a license key is required and is available from Symantec.cloud. Each key may be entered from **Edit > Settings**. Select **License** from the left hand panel and click the **Add license** tab.

The **Licensed to** field is the client identity supplied to you for registration purposes.

The **License key** is an alphanumeric field. Spaces are not valid. The license key is provided by Symantec.cloud.

Enter your licensing details and click **Apply**. To see the features that are enabled, your serial number, and license expiry date, click the **Show License** tab.

If you have entered multiple licenses, left and right arrow buttons enable you to view each license. Licenses with duplicate features are automatically removed. If an expiry period is specified in the license, the license with the longer expiry period is retained.

# Synchronizations

Types of synchronization are initially set when the tool is started for the first time. When you create a configuration, the options you defined determine the synchronization types that are presented here. This setting is independent of the features enabled by your license.

The Synchronization page enables you to choose 'Mail' and/or 'Group + Users' synchronization types.

The 'Error recovery' setting determines the action when the communication between your computer and the Symantec.cloud server fails. Choose an option from the drop-down list. **Replace server contents** sends the entire list again (overwriting the contents on the Symantec.cloud service). **Retry update** will resends the differences from the last time the synchronization took place.

# Log settings

On the 'Log Settings' page, use the sliders to determine the level of detail held in the log files. The first slider determines which log messages are written to the application?s log files.

The second slider determines the amount of log messages written to your system logs: on Windows this is the Event log; on Linux this is the syslog.

The **Log Lifetime** specifies the maximum number of days that logs are retained before the Synchronization Tool removes them. If the number of days is set to 0, the log files are held indefinitely.

**Note:** If the logs are held indefinitely in this way, check periodically that you have enough disk space to permit the creation of new logs when the tool is run.

## LDAP

The LDAP page displays the string used to search for entries when you browse the LDAP server on the search configuration screen.

See "About LDAP filters" on page 49.

## Symantec.cloud

On the Message Labs page, unless instructed to do so by Symantec.cloud, do not change the default value in the **Access URL** field. If you change this line by accident, click **Reset Defaults** to put the original value back into this field. The **Username** and **Password** are the account details provided to you by Symantec.cloud.

When you have entered these details, click **Apply** to connect to Symantec.cloud using these details. If you receive an error message when you click Apply, you may need to connect to Symantec.cloud through an HTTP proxy.

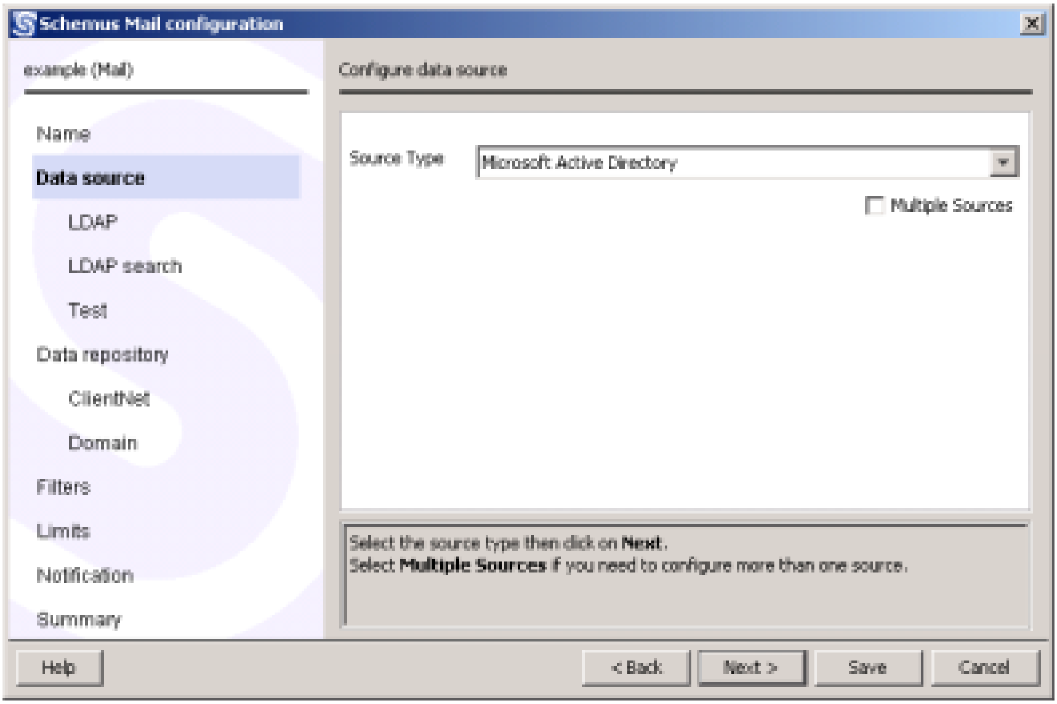
If you need to access the Internet through an HTTP proxy, change the **HTTPS Proxy** setting to **Manual** and enter the connection details in the newly appeared fields. If in doubt, start your Internet browser and look at the connection settings being used for it.

## The configuration wizard

This section describes the pages available by clicking **Modify** on an existing configuration on the Schemus main summary page, or by creating a new configuration.

There may be a single or multiple data sources for each type of synchronization. The single data source is show in the figure below. A selection from a drop-down list of the different types of LDAP servers and the file data source may be made.

For LDAP servers, the type chosen here determines the default attributes used to retrieve data later in the wizard. By choosing the correct type of server from the drop-down list most default values, appearing later in the wizard, will automatically be chosen.

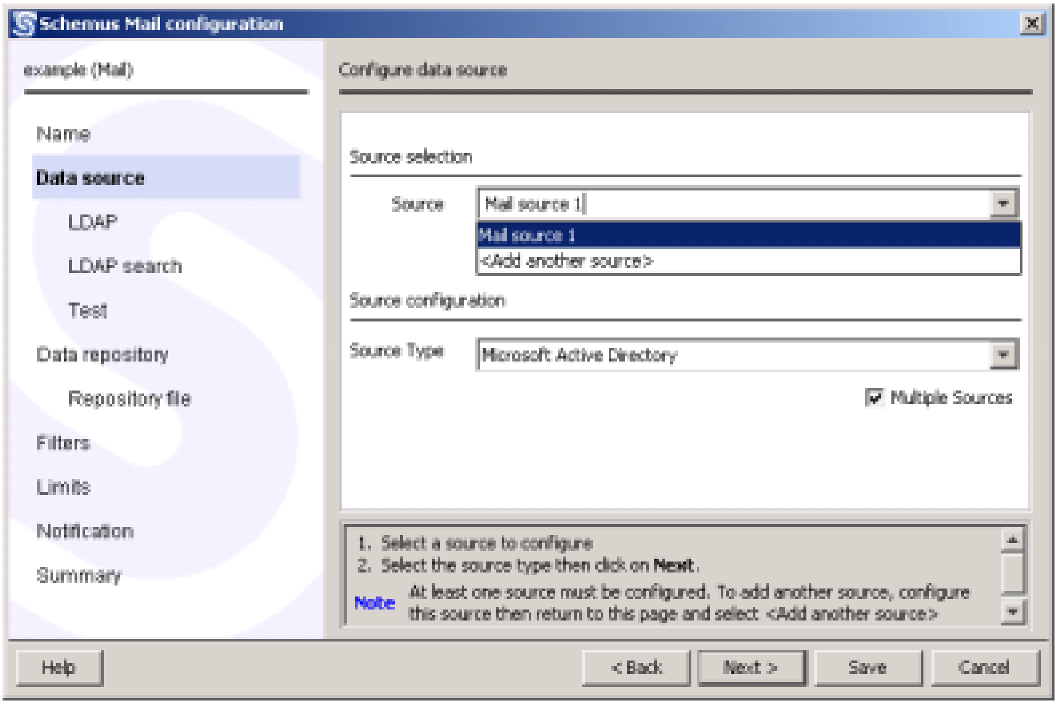


Source Type: Microsoft Active Directory

□ Multiple Sources

Select the source type then click on **Next**.
Select **Multiple Sources** if you need to configure more than one source.

For more complex configurations (e.g. using multiple disparate directories) it may be necessary to have multiple data sources. To enable this feature check the **Multiple Sources** check box. The page will be redrawn as shown below.



Source: Mail source 1

Source Type: Microsoft Active Directory

☑ Multiple Sources

1. Select a source to configure
2. Select the source type then click on **Next**.

Note At least one source must be configured. To add another source, configure this source then return to this page and select <Add another source>

Select **<Add another source>** from the drop-down list and a new source is generated. The drop-down list for **Source** is initially populated with a name beginning with the type of synchronization (mail, groups, or users) and other entries that you have entered and fully filled, although you may change the current name to something more representative.

For each source that you create, there is a **Source Type** and, on subsequent screens, for LDAP settings each source will be associated with its own server name and port, (optionally) any proxy settings, the top of the search point in the directory tree, and attributes to retrieve from the server. Until you have completed these fields, you cannot select your source from the list.

Once multiple sources have been defined the **Multiple Sources** checkbox is disabled. You cannot switch back to the simple data source definition screen until only one source remains. To remove a data source definition, select it from the drop-down list and click Remove button. It is not possible to remove all data sources.

# LDAP server configuration page

On this page, the Host Name is the address of your directory access server (for example, exampleserver.examplecompany.com and 192.168.0.135). Unless you know to the contrary, leave **Port number** set to 389. This is the default port number used for communicating with an LDAP server in plain text mode. Changing the communication protocol may change this default setting.

Although you may be able to retrieve search details from the LDAP server anonymously, connecting in this mode may restrict the number of search results.

If the protocol used to communicate with the server is not plain, you must ensure that either the server uses a certificate that has been signed by a trust point already held in the JRE root certificate store (cacerts), or that if the server uses a self-signed certificate, it has been imported. You can import your certificate into the `*installation directory*/jre/lib/security/cacerts` file using the `*installation directory*/jre/bin/keytool` utility.

Clicking the **Advanced** button will move onto 'Paging' settings and 'Continuation References' settings.

With 'Paging', a page size of 100 results is the default setting and means that a maximum of 100 results are retrieved from the LDAP server at a time. Not all LDAP servers support paging, but the Synchronization Tool automatically switches to nonpaging mode if unavailable and logs this fact.

The configuration of some directory servers may limit the maximum number of results that may be provided in one go. The paging facility is provided to overcome this limitation. For a server that has 220 results, a page size of 100 retrieves entries 1 to 100 the first time, 101 to 200 the second time, and so on. As displayed by the Synchronization Tool, this would just appear as though 220 results had been returned.

An LDAP server may contain referrals to other points on the server, or indeed to points on other LDAP servers. The default action is for the Synchronization Tool to follow these referrals to continue retrieving results. If you notice that a directory server referred to is intermittently available, there are two schemes for handling this: either set the referral action to **Abort update** or set threshold limits to ensure that the update does not continue if there is an abrupt difference in the number of results returned.

The DNS name or IP address that the Synchronization Tool follows is the one that is seen by the computer running the Synchronization Tool application. If you experience problems with the Synchronization Tool following referrals, ensure that you can contact the referred servers by the use of an application like "ping".

# LDAP search configuration page

The **Search base** specifies the base of the hierarchical tree to search for data, and the **Search scope** specifies the detail at which to search for data. These fields are set to the same location whether you configure mail, groups, or users.

The **Search base** field enables you to navigate over the LDAP directory. The drop-down list contains all the entries at that level of the directory. The criteria for which object classes are returned are defined in the setting LDAP.

Select an entry from the drop-down list in the **Search base** field. The drop-down list now contains all entries at your new position in the hierarchical tree. Clicking on the first item in the drop-down list moves you back up the tree. Most LDAP servers do not let you search for entries at their root; you may need to manually type in a search base before you can browse further.

The **Search scope** field lets you select the depth at which entries are looked for at the point in the tree that the search base field specifies. This field contains the following options:

| | |
|---|---|
| One-level | Searches for all objects at the level specified in the **Search base** field |
| Object | Searches for a single object specified by the **Search base** |
| Sub-tree | Searches from the level specified in the **Search base** field downwards until restricted by the LDAP server or the bottom is reached. To return the most results, use this option |

The **Search filter** is the type of object to return data on. When focus is in this text field, the **Examples** button is enabled, letting you select a search filter from a list of predefined entries.

See “About LDAP filters” on page 49.

## Attributes

To use an attribute retrieved from the LDAP server it must be delimited by percent (%) symbols; otherwise, text will be interpreted literally. For example, the mail attribute would appear as %mail% when typed in a text field. In addition, regular expression (regex) matching and replacement can be used to modify those attributes. The syntax is {s/match/replacement/flags} and needs to appear before the closing percent symbol.

```
s = substitute
match = regex to match
replacement = text to replace matches
```

```
/ = separator. "/" is used in this documentation. Any character can be used.
flags = any combination of i, g, e


    i = ignore case
    g = global (match all, if omitted only the first match is used)
    e = replacement is an expression.  The following expression methods are available:


        toIMCEA(string) = encodes the characters of the string into IMCEA format.
        ord(string) = encodes each character of the string as it?s ordinal value
            (in hexadecimal).
        toUpperCase(string) = converts the string to uppercase.
        toLowerCase(string) = converts the string to lowercase.
        isInDomain(address, domain1, domain2, ?) = compares the domain portion of the
            address with each domain in the list.  Returns the address unchanged if
            a match is found. If no match is found, an empty string is returned,
            which will result in the address being discarded. This can be used to
            accept only those addresses belonging to a given set of domains.
        isNotInDomain(address, domain1, domain2, ?) = compares the domain portion of
            the address with each domain in the list. Returns the address unchanged
            if no match is found. If a match is found, an empty string is returned,
            which will result in the address being discarded. This can be used to
            discard addresses belonging to a given set of domains.
        substituteDomains(address, domain1, domain2, ?) = removes the domain portion
            of the address and replaces it with each domain in the list, producing
            multiple addresses.
        substituteMatchDomains(address, domain1, domain2, ?) = removes the domain
            portion of the address and replaces it with each domain in the list,
            producing multiple addresses. The substitution is only done if the
            domain of the original address matches one of the domains in the list
            otherwise the address is unchanged.
        appendDomains(addressLocal, domain1, domain2, ?) = constructs a list of email
            addresses from the local part and each domain. If the local part already
            includes a domain it is unchanged.
```

For more information about using these functions, including examples, access the context sensitive help in Schemus, in the Advanced topics section.

An example retrieving the attribute `proxyAddresses` and performing a substitution on the result would be:

```
%proxyAddresses{s/(smtp: |.*:.*)(.*)/$2/i}%
```

So having retrieved the `proxyAddresses` attribute, all values starting with `smtp:` are used, with the `smtp:` prefix removed. Values not starting with `smtp:` are discarded.

There are three special indexed attributes which extract portions of the distinguished name (dn):

Distinguished name: `%DN[n]%`

Domain component: `%DC[n]%`

Organizational Unit component: `%OU[n]%`

If `n` is nonzero, the name part is extracted.

If `n` is negative, the index is taken from the least-significant end of the dn.

If `n` is positive, the index is taken from the most-significant end.

An example for the distinguished name attribute containing the value "dn=cn=henry, ou=staff, dc=acme, dc=com"

`%DN%` = cn=henry, ou=staff, dc=Metanate, dc=com

`%DC%` = acme.com

`%DC[1]%` = com

`%DC[-1]%` = acme

`%DN[1]%` = com

`%DN[-1]%` = henry

`%OU[1]%` = staff

## Mail attributes

Mail synchronization

- Clicking the **Advanced** button reveals the mail search attributes: 'Primary Mail' and 'Mail Aliases'. The default settings for these attributes are derived from the type of LDAP server you selected in the data source.
  **Primary Mail** is the attribute within the object returned by the search filter that contains the mail address.
  The **Mail Aliases** attribute is a list of optional alternatives to the **Primary Mail** attributes.

## Group attributes for group synchronization

Edit the group attributes as follows:

**Search base**

*dc=com*

**Search scope**

*Sub-tree*

**Search filter**

*(objectCategory=Group)*

**Name**

*%DC[-1]%\\%sAMAccountName%*

This field uses the special attribute rules described in the Attributes section.

Attributes.

To edit the group attributes further, click **Advanced**.

The relevant fields are as follows:

**Group GUID attribute**

*%objectGUID%*

A unique identifier maintained by the LDAP server. Not all servers are guaranteed to support this attribute but it should be used if available (Microsoft Active Directory does). If this attribute is omitted, an identifier will be derived from the distinguished name (DN) of the object class instead.

Using a DN has the undesirable effect that, if the group is renamed rather than the entry just being modified, the group entry is removed and added again. This means that any association with that entry in the ClientNet domain is broken and has to be re-established.

**Group Token attribute**

*%DC%\\%primaryGroupToken%*

The optional attribute that holds the group identifier number. The value may in turn be referred to by the **Primary Group attribute** in the user object class settings. If a user has its primary group set to this group's group token, the user is part of this group. If you synchronize multiple domains, you should also use the domain attribute in this field (%DC%). The reason is that if you have the same value on different domains, this field will be treated uniquely. Ensure that you make the same change to the primary group attribute for users.

**Group Parent attribute**

*%memberOf%*

Used to relate one group to its parent group, if it exists. The optional attribute retrieved from the directory may consist of a single DN that contains the parent of this group.

| | |
|---|---|
| **Group Members attribute** | *%member%*<br>The name of the multi-value attribute that holds the users (in DN form) that are part of this group. |

## User attributes

Users Synchronization:

For details on the **Name template** and the mechanism to generate unique names using templates:

See “Attributes” on page 31.

For users in a Microsoft environment, the "names" constructed by the Name template should represent the "domain\username" identity of individual users..

On the LDAP search page, you can find users in the following ways:

- Group membership
  Obtains the entire list of users by collecting the names allocated to each group.
- Searching the directory
  Searches for all users on the directory server and compares the results from a group membership search and includes users that appear in both lists. This generates the most accurate results because not all directories have information of which users are in groups as well as all users in every group.This doesn't happen if the **Filter Users** option in the Groups configuration is set to **Do not filter**.

To edit the user attributes, click **Advanced**.

The fields are as follows:

- **Primary Mail**
  Used to retrieve the email address for this user.
- **Mail Aliases**
  A list containing alternative sources for mail addresses
- **Primary Group**
  The token number attributed to this user and potentially matching a group's **Group Token attribute** value, which places this user in that group. This attribute should be considered as an extension to the **Other Groups** for placing a user in a particular group; not all LDAP directories support it. When you synchronize across multiple domains, ensure that both this field and the group's **Primary Group** attribute contain the domain attribute (%DN%) so that this field is unique.
- **Other Groups**

The attribute name that describes which group or groups this user belongs to. For Active Directories this is identical to the **Group Parent** for the group object class that points from each group to its users. If this attribute is omitted or your directory does not support this feature, the Synchronization Tool searches for each user in the entire group list.

To correctly associate users with groups, one of the following must be true:

- The **Group Parent Attribute** must exist and the **User GUID attribute** and **Group GUID attribute** must be omitted.
- The group attribute **Group Members attribute** must exist.

- **GUID attribute**
  A unique identifier assigned to each user similar to the **Group GUID attribute** for groups. Omitting this attribute will result in an identifier being derived from the object class's distinguished name. If this attribute is omitted, the **Group GUID attribute** should also be omitted.
- **ML IMServices**
  A multivalued attribute containing the IM account type and name.

## Testing LDAP attributes

If you changed any of the default attributes used for the LDAP search, the advanced version of the test screen lets you confirm that you correctly retrieved the attribute you expected. Ensure that the check box **Show detail** is checked.

To change the order of the columns in the table, click and drag the top of the column.

| | |
|---|---|
| Mail synchronization | There is no detailed option available for mail addresses. |

Groups synchronization

For groups, each line will contain:

- The result from the name template, subsequent to it being changed using any template rule.
- The GUID. If no **Group GUID attribute** has been provided, this will have been derived from the DN.
- The Group Token retrieved using the **Group Token attribute**.
- The DN automatically retrieved for you by the Synchronization Tool.
- The number of parents that this group belongs to (normally none or 1) and the DN of the first of these groups. Retrieved using the **Group Parents attribute**.
- The number of users in this group and the DN of the first of these users. Retrieved using the **Group Members attribute**.

Users synchronization

For users, each line will contain:

- The result from the name template, subsequent to it being changed using any template rule.
- The GUID. If no **User GUID attribute** has been provided, this will have been derived from the DN.
- The email address retrieved using the **Primary Mail attribute**.
- The Primary Group retrieved using the **Primary Group attribute**.
- The Groups retrieved using the **Other Groups** attribute.
- The DN automatically retrieved for you by the Synchronization Tool.
- The Other consists of **Mail Aliases** and **ML IM Services** attribute.

For both groups and users, if the Name, the GUID, or the DN is blank, correct the attribute names before commencing.

# Groups

## Selecting groups to synchronize

Groups synchronization

For each group you may individually select whether it is synchronized to your destination. To include specific groups, select them in the left panel and click the **>** button to move them into the right panel. Group names appearing in the right panel can be included or excluded depending on the setting of the **Groups to** drop-down list.

The **Filter Users** drop-down list determines what happens to users that are found but have had their group excluded. If this is set to **Include only members of included groups**, if a user's group has been excluded, so will the user. If this is set to **Do not filter**, the users are not restricted by the group they are in and are always added. However, they will not appear in a group.

# Filters

The primary purpose of the filters page is to enable you to exclude retrieved entries. You can also used it to modify email addresses (for Mail synchronization) and names (for Groups and Users synchronization) before they are written to the destination data repository. Each line can contain a different pattern to match against with an optional replacement line.

📂

Clicking the 'open' icon at the start of each line changes the pattern entry to specify a file name instead. The file should contain a collection of patterns, with each entry separated by a new line.

To exclude an entry, type the pattern into the left column with no replacement entry in the right column. As entries are discovered from the data source (either a file or LDAP server), they will be checked against patterns in this column and removed. The rules for matching the entries against the pattern are determined by the setting in the drop-down list at the bottom of the screen. This setting can either be set to **Regular expressions** or **Wildcards**. Note that changing this setting affects how all patterns are interpreted.

To modify entries, include a replacement address in the right hand column (the replacement). The replacement rule will be applied against the matching pattern in the left hand column.

When **Wild cards** are selected in the drop-down list, the character *** can be used to match zero or more characters. The character *?* can used to match a single character. If a replacement entry is used, only the result of the first matching *** can be used in the replacement.

For complex pattern matching and replacements, set the drop-down list to **Regular expressions**.

See “About LDAP filters” on page 49.

# Limits

The limits configuration page provides a safeguard against accidental deletion of entries from your data repository.It warns you when thresholds for the number of changes made in a synchronization have been exceeded. This alerts you to potential mistakes in your configurations.

The four thresholds are named:

- Maximum added entries
- Maximum deleted entries
- Maximum changed entries
- Minimum replacement entries

The **Minimum replacement entries** is the number of entries changed for a complete replacement to be allowed (related to the **Replace** button on the main screen).

The numeric value in each limit field can be an absolute number or a percentage of your expected number of entries.

When the threshold limit is exceeded, an error message similar to the following is displayed: "Synchronization Limit Exceeded. There are 23 deletions. This exceeds the limit for this configuration. Do you want to force the update?" Click **Yes** or **No**.

When the Schemus Synchronizer operates in command line mode, if a threshold limit is exceeded, the synchronization is not performed. You will be notified by email if this option has been selected.

See “Email notifications” on page 39.

# Email notifications

This page lets you automatically send an email containing a summary of the synchronization process whenever it happens and whether or not it was successful. Sending a notification summary is recommended if you intend to set up the Synchronization Tool to operate automatically.

The Email notifications drop-down list enables you to select the detail that you want in the email.

The SMTP **Mail Server** is the host name of the server to use to deliver the email (e.g. `smtp.metanate.com` or `mail.metanate.com`).

The **Message Subject** fields are placed in the notification email's subject field. If the **on Success** field is left completely blank then an email notification will only be sent on failure.

The **To** and **cc** fields contain the email addresses to send the summary email to. You can separate multiple recipients with commas.

The **From** field is the address to use for originating the email.

An example email summary notification might look like:

```
Schemus Synchronization report
Update operation with Symantec.cloud completed
Time:         Thu May 11 16:43:36 BST 2006
Host:         exampleserver.exampledomain.com
User:         exampleuser
Configuration:example
Updated domains
    None
Up-to-date domains
    exampledomain.co.uk
    anotherexampledomain.co.uk
Unknown domains
    example.com
    example.blue.com
    example.red.com
Updates
    None
Invalid addresses
    None
Failed updates
    None
Addresses in domains not configured on the repository
    250 additions
    0 deletions
```

# Summary and verification

Clicking the **Verify** button tests your configuration entries simultaneously. As each test is performed an hourglass is displayed beside the component being tested. If the test is successful, a green tick is displayed. If a red cross is displayed against any line, click to the left of the relevant line to correct it. If you have multiple sources, each source is checked in turn.

To set your configuration to automatically run at predetermined times, click **Schedule**. When you are satisfied with your settings, click **Save** to write your configuration settings to disk.

If your data repository is set to Symantec.cloud, the Symantec.cloud server will be contacted during this process.

# Scheduling the synchronization

Clicking the **Schedule** button brings up a dialog box where you can set a time for your synchronization to run.

**To schedule your synchronization**

1. Specify a time in **Run at**.
2. Specify a recurring time in **then run every**.
3. Choose which days from the **on** drop-down list.
4. Check the box **Day of Month** and/or **Day of Week**.
5. Select a Day of Month and/or Day of Week
6. Click **Schedule**.

---

**Note:** If you select both Day of Month and Day of Week, synchronization will run monthly on the chosen date and weekly on the chosen day.

---

# The main page

Once you have created a new configuration, you can select it from the drop-down list on the configuration page. (To get to the configuration window, select **View > Configuration**.) You can modify any of your synchronization types by first selecting the appropriate tab (Mail, Groups, or Users) and then clicking the **Modify** button.

The features available are as follows:

| | |
|---|---|
| **Summary** | Displays your settings and allows your synchronization types to be modified or verified. |

**Test Update** Uses your existing local database to synchronize but does not update the local database or send the results to Symantec.cloud (or write them to file for file repositories).

Data from the test update is displayed showing the entries to add, delete and modify, with a column for entries that have been excluded. Click on an entry in any column to display additional information, such as, whether a user is member of a group.

**Update** Uses your existing local database to calculate the incremental changes to synchronize with Symantec.cloud or a file repository. This is the usual method for synchronizing your data.

**Replace** Clears your local database and resends all your data to Symantec.cloud or recreates your file repository.

**Refresh** Retrieves all your data from Symantec.cloud, or rereads your data from your file repository, and uses this to recreate your local database.

# Logging

Both the GUI and the command line version of the Schemus Synchronizer produce logging. Each generated message contains the following information:

- The time and date that the event occurred
- The logging level
- The configuration (if any) that was in use
- The user that Schemus was being run as
- The component of Schemus that was the source of the logging

To view the logging window, select **View > Logs**.

The features are as follows:

**Log level** Sets the importance of messages that are shown. It is an accumulative setting; if you select INFO, then SEVERE and WARNING levels are also displayed.

**Log file** The name of the directory below the root logging directory that stores the logging lines.

For Windows, this is located in the following folder:

Documents and Settings\All Users\Application Data\Schemus\application\log

For Linux, this is located in the following directory:

schemus/application/log

The name of the log file is made from the year, the month, the day, and an extension. The extension is the number of the invocation of the Synchronization Tool that generated the message.

**Logger** The component of the Synchronization Tool that sourced the message.

The drop-down list lets you restrict the messages shown to a particular component and sub-components. So selecting schemus.sync would show messages from the components `schemus.sync.source`, `schemus.sync.repository`, `schemus.sync.repository.add` and `schemus.sync.repository.remove`. But selecting `schemus.sync.source` would just show messages from the `schemus.sync.source` component.

The components are as follows:

| | |
|---|---|
| Schemus | All components |
| Schemus.settings | Creation of new configuration entries or changes to existing configuration |
| schemus.sync | All synchronization operations |
| Schemus.sync.source | Operations to the source repository (normally an LDAP server) |
| Schemus.sync.repository | All modifications to the destination repository |
| Schemus.sync.repository.add | Entries added to the destination repository |
| Schemus.sync.repository.remove | Entries removed from the destination repository |

Clicking on a line in the message list displays any additional information at the bottom of the window.

Windows Messages with a level of INFO and higher importance are also logged to the application section of the event log.

Linux

Messages with a level of INFO and higher importance are also logged to the user log.

# Directory referral checker

A directory referral, or continuation reference, is a link from one location on an LDAP server to either a different directory server or another location on the same directory server. The action that the Synchronization Tool takes with a referral when performing a synchronization is defined in the configuration profile. A missing or broken referral can result in fewer results being returned than expected.

A diagnostic tool is provided as part of the Synchronization Tool, letting you check the validity of referrals on your LDAP server. It uses the LDAP details and search base from your currently selected configuration to check the links.

Clicking the **Start** button will check the referrals for each synchronization type that you have configured in turn. Click the **Mail**, **Groups**, or **Users** tab to see referrals for that specific synchronization type. Each referral found is displayed in the top half of the split logging window, with specific problems shown in the lower half of the window.

See “LDAP server configuration page” on page 30.

# Command line operation

The Synchronization Tool can be operated from both the graphical user interface (GUI) application or from the command line. Invoking Synchronization Tool from the command line is the first stage to configuring it to operate automatically.

Windows

The command line version of the Schemus Synchronizer on the Linux platform is called schemusc and is located in the install directory. Assuming the installation directory is on your path, first make sure that the GUI version of Schemus Synchronizer is not running. Then open a terminal and type the following command:

```
$schemusc —config "yourconfigurationname"
```

In this command, substitute *yourconfigurationname* for the configuration name of the synchronization you want to perform. If there are spaces within the configuration name, it is necessary to enclose the name in double quotation marks; otherwise the quotation marks are optional.

Linux

The command line version of the Schemus Synchronizer on the Windows platform is called schemusc.exe and is located in the install directory. So assuming it has been installed in the default location, first make sure that the GUI version of Schemus Synchronizer is not running. Then open a command prompt and type the following command:

```
C:\>cd "\Program Files\schemus"
C:\Program Files\schemus>schemusc —config
 "yourconfigurationname"
```

In this command, substitute *yourconfigurationname* for the configuration name of the synchronization you want to perform. If there are spaces within the configuration name, it is necessary to enclose the name in double quotation marks; otherwise the quotation marks are optional.

Appendix A

# Reference and FAQs

This appendix includes the following topics:

- About RegEx strings
- About LDAP filters
- About the Java Runtime Environment
- Frequently Asked Questions

## About RegEx strings

Regular expressions, or RegEx, are a powerful mechanism for matching a sequence of simple characters. The following description is a brief taster for what RegEx can do.

Regular expressions are case sensitive, so a lowercase a is distinct from an uppercase A.

Characters enclosed between `[]` will match against a disjunction of characters. For example:

`[tT]here` Matches against ‘there’

`[]` May also be used on a range of characters separated by a — character. For example,

`[0-9]` Matches any digit.

`[A-Z]` Matches any uppercase alpha character

`[A-Za-z0-9]` Matches any alphanumeric character

`^` The "not" character, so `[^0-9]` matches against any character that is not a digit.

Although ranges may be used to specify a group of characters, there are various shortcuts:

| | |
|---|---|
| `.` | Matches against any character |
| `\d` | Matches against a digit [0-9] |
| `\D` | Matches against a non-digit [^0-9] |
| `\s` | Matches against a whitespace character (such as a tab, space, or line-feed character) |
| `\S` | Matches against a non-whitespace character |
| `\w` | Matches against a word character [a-zA-Z_0-9] |
| `\W` | Matches against a non-word character |

The `\` character is used to denote a special character, so if you want to match against the `\` character you must use two to match against a single `\`. i.e. `\\`

To match against a control character use `\xhh` (for the hexadecimal character `hh)` and `\uhhhh` to match against a Unicode character (for the hexadecimal character `hhhh`).Different ways to the match previous character or expression

| | |
|---|---|
| `*` | Matches against zero or more occurrences of the previous character or expression |
| `+` | Matches against one or more occurrences of the previous character or expression |
| `?` | Matches zero or one occurrences of the previous character or expression |
| `{n}` | Matches *n* occurrences of the previous character or expression |
| `{n,m}` | Matches from *n* to *m* occurrences of the previous character or expression |
| `{n,}` | Matches at least *n* occurrences of the previous character or expression |

If you intend to provide a replacement string, you must group matches by enclosing them in parentheses so that they can be referenced in the replacement. To reference a matched parameter, use `$n`, where n is the parameter starting from 1.

For example, the pattern `([^\s]*?)a([^\s]*)` with the replacement `$1b$2` matches non-whitespace characters up to the first "a" character in to parameter 1 and replaces that "a" with a "b". So the text "badapplepie" would become "bbdapplepie".

The use of `[^\s]*?` with a following `?` is known as a reluctant quantifier. If you wanted to match as much text as possible before matching the "a", leave out the additional `?` and put `([^\s]*)a([^\s]*)`. As a result, the text "badapplepie" becomes "badbpplepie".

**Note:** Additional information on regular expressions and further examples are available in the Schemus context sensitive help.

# About LDAP filters

LDAP Search Filters are used in two places within the Schemus Synchronizer. The first is used to select which objects are returned when browsing for the search base. The second identifies which objects in your directory are to be examined for email address attributes. It is expected that you would more commonly need to modify the second of these two filters.

Syntax

LDAP Search Filters are defined using a notation that is fully described within RFC 2254 "The String Representation of LDAP Search Filters".

http://rfc.net/rfc2254.html

To establish your own filters, you also need an understanding of the schema that your directory uses. The schema defines the objects and their attributes that together comprise your directory content.

The Search Base Filter

This filter is used in the LDAP configuration to select which objects are returned when browsing for the search base. The filter is found within **Edit > Settings**; select **LDAP** on the left panel. The default value for this LDAP filter is as follows:

```
(!(|
    (objectclass=person)
    (objectclass=applicationentity)
    (objectclass=applicationprocess)
    (objectclass=device)
    (objectclass=organizationalrole)
    (objectclass=groupofnames)
```

```
        (objectclass=groupofuniquenames)
    ))
```

In the default LDAP filter shown above, the `!` character means "not" and the `|` character means "or". So the filter returns any objects that do not match any of the object classes shown in the list.

See “LDAP search configuration page” on page 31.

The Search Query Filter:

- The Synchronization Tool lets you define the filter that targets which objects in your directory are to be examined for email address attributes. This filter appears in the LDAP search configuration dialog as the **Search filter**. Here the filter specifies which objects are retrieved, before the mail attribute values are extracted.

Examples:

- If you want to include all objects in your search query, use the following filter:

  ```
  (objectclass=*)
  ```

- The following filter includes all Microsoft Exchange 2000 users who are currently enabled:

  ```
  (&(objectclass=user)(msexchuserAccountcontrol=0))
  ```

- The following filter includes all objects that define users and groups. Note that in Microsoft Exchange 2000 these groups include both Security groups and Mailing lists.

  ```
  (|(objectclass=user)(objectclass=group))
  ```

- If you want to exclude the system mailbox objects found in Microsoft Exchange 2000 from the search described above, you can modify the filter as follows:

  ```
  (&(|(objectclass=user)(objectclass=group))
  (!(cn=SystemMailbox*)))
  ```

# About the Java Runtime Environment

For all platforms except the Macintosh (which already has a JRE), whether or not you install the Java Runtime Environment (JRE) is optional.

The JRE can be installed independently of the Synchronization Tool so that it is available to multiple applications. Alternatively, a separate copy can be installed for each application (with a JRE). The current release of the Synchronization Tool needs JRE version 1.5.

The advantage of installing a JRE with each application is that removing or updating the global JRE does not stop your application from working. The main disadvantage is that the JRE is multiple megabytes in size, so installing a copy for each application consumes disk space. With the decreasing cost and increasing size of storage devices, generally the safest option is to install the Synchronization Tool with its own JRE.

Finding which version of JRE your computer is using:

| | |
|---|---|
| Windows | To discover the version of JRE, start the Control Panel and double-click **Java Plug-in**. The version number is displayed in the **About** tab.<br>Alternately visit the following Web site, which will display your Java version:<br>http://www.java.com/en/download/help/testvm.xml |
| Linux | To discover the version of JRE on your computer visit the following Web site:<br>http://www.java.com/en/download/help/testvm.xml |

# Frequently Asked Questions

This table contains many common questions and answers concerning the Synchronisation Tool

| Question | Answer |
|---|---|
| I am unable to get the addresses for my public folders. How do I correct this? | Change the Search Filter (**Data Source > LDAP search > Search filter**) to:<br>(\|(\|(objectclass=user)(objectclass=group))(objectclass=publicfolder)) |
| When I query Lotus Notes, I can get all my primary email addresses but cannot get all my users' aliases. How do I fix this? | Schemus version 1.14 and later has support for Lotus Notes. Using the attribute templates, it is possible to construct Lotus Notes user aliases from attributes in the directory. |

| Question | Answer |
|---|---|
| To use Mail and the Group/User Synchronization, do I need to two license keys? | Yes. |
| Can the Synchronization Tool do multiple queries if I have different information on two or more ADs? | Versions 1.3 and higher can do this.<br>See "The configuration wizard" on page 27. |
| If you have a lot of filters to set up, is there an easy way to do it? | You can define a text file containing your filter rules. In the **Filter** section, click the folder icon and select the text file. |
| How do I view the Synchronization Tool logs? | Select **View > Logs** |
| How do I change the logging from the default of 30 days? | Go to **Edit > Settings > Log Settings**. |
| How do I set the Synchronization Tool to put its query results into a file instead of synchronizing with Symantec.cloud? | In the **Data Repository** section of the configuration, select **File** as the **Repository Type**. |
| How do I tell the Synchronization Tool to query a file on my server instead of my directory? | In the **Data Source** section of the configuration, select **File** as the **Source Type**. |
| What do the Info and Fine settings mean under the Notification settings? | The email notification settings let you define the level of detail for the logging that you want to see when the Synchronization Tool does it querying and syncing with Symantec.cloud. The fine setting provides the most detail. The larger the company is, the bigger the log file will be. |
| Which URL link should I use to synchronize with Symantec.cloud? | Version 1.3 must use:<br>https://syncapi.messagelabs.com/<br>Version 1.2 must use:<br>https://api.messagelabs.com/<br>For later versions, always click the default button. |

| Question | Answer |
|---|---|
| I set up the summary notification but I still do not receive the email after the Synchronization tool completes the synchronization. Why? | There may be a problem with the way the Summary notification is set up. The Synchronization Tool creates the email locally and so the Symantec.cloud services do not scan or block the email.<br>Check that the computer that The Synchronization Tool is installed on can communicate with the organization's mail server on port 25.<br>If you are have set your email notification to **summary + log (FINE)**, check the mail size limit on the server since the notification supplies all of the logging from the synchronization. The bigger the company, the larger the email. These emails can be around 30 to 50 MBs. |
| After I performed a synchronization, I then added a single address manually in ClientNet. When I synchronized again, the new address did not get added in. Why not? | You should either use the Synchronization Tool or ClientNet to maintain your valid address list and not both together. Using both techniques together may lead to inaccuracies in your address list data. |
| When I set up automatic schedule for synchronizations, I am asked for the name of the configuration file. Where do I find it? | The name of the config file is the name you gave to the configuration type you want to run. The configuration names are listed in the **Configuration** drop-down list in the **Synchronization Tool** main window.<br>Running it from a command line would look something like the following:<br>SchemusC - config example<br>(where "example" is the name of the configuration) |
| Does the Synchronization Tool need my organization to use Active Directory for it to work? | It needs either Active Directory or any other system that uses LDAP. |
| Does the Synchronization Tool need Java to operate? | Yes. Generally it needs the latest version of Java installed.<br>http://www.java.com/en/download/index.jsp |
| Can any other clients see my Active Directory contents after I synchronize them to the Symantec.cloud Infrastructure? | No. Only certain Symantec.cloud personnel can view the contents. |
| Does the Test Update option cause a synchronization with Symantec.cloud? | No. Test Update only does a test query with the directory. |
| How do I avoid a second configuration overwriting the synchronization results of the first configuration sent to Symantec.cloud? | Rather than creating separate configurations you should consider using multiple sources. |