

# Synchronization Tool Administrator Guide

# Synchronization Tool Administration Guide

Documentation version: 1.5

## Legal Notice

Copyright 2016 Symantec Corporation. All rights reserved.

Symantec, the Symantec Logo, and the Checkmark Logo are trademarks or registered trademarks of Symantec Corporation or its affiliates in the U.S. and other countries. Other names may be trademarks of their respective owners.

The product described in this document is distributed under licenses restricting its use, copying, distribution, and decompilation/reverse engineering. No part of this document may be reproduced in any form by any means without prior written authorization of Symantec Corporation and its licensors, if any.

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 CONTAINED IN THIS DOCUMENTATION IS SUBJECT TO CHANGE WITHOUT NOTICE.

The Licensed Software and Documentation are deemed to be commercial computer software as defined in FAR 12.212 and subject to restricted rights as defined in FAR Section 52.227-19 "Commercial Computer Software - Restricted Rights" and DFARS 227.7202, et seq. "Commercial Computer Software and Commercial Computer Software Documentation," as applicable, and any successor regulations, whether delivered by Symantec as on premises or hosted services. Any use, modification, reproduction release, performance, display or disclosure of the Licensed Software and Documentation by the U.S. Government shall be solely in accordance with the terms of this Agreement.

Symantec Corporation  
350 Ellis Street  
Mountain View, CA 94043

<http://www.symantec.com>

# Technical support

If you need help on an aspect of the security services that is not covered by the online Help or administrator guides, contact your IT administrator or Support team. To find your Support team's contact details in the portal, click **Support > Contact us**.

# Contents

Technical support .....	3
Chapter 1	Introduction to the Synchronization Tool ..... 6
	About the Synchronization Tool ..... 6
	About synchronization types that are supported by the Synchronization Tool ..... 7
	Viewing advanced help topics for the Synchronization Tool ..... 7
Chapter 2	Installing the Synchronization Tool ..... 9
	System requirements for the Synchronization Tool ..... 9
	Download and license the Synchronization Tool ..... 11
	Before you install the Synchronization Tool ..... 12
	Install the Synchronization Tool ..... 13
	Start the Synchronization Tool for the first time ..... 14
	About standard settings for the Synchronization Tool ..... 15
	Update the default Synchronization types ..... 19
	Update the Synchronization settings ..... 19
	Updating the Log Settings ..... 21
Chapter 3	Creating configuration profiles ..... 23
	About configuration profiles ..... 24
	Create a configuration profile - process overview ..... 25
	Select a data source for a configuration profile ..... 28
	Select multiple data sources for a configuration profile ..... 30
	Select a file source for mail synchronization ..... 31
	Select a file source for group synchronization ..... 31
	Select a file source for user synchronization ..... 32
	Configure an LDAP data source ..... 34
	Configure an LDAP server - advanced settings ..... 36
	Configure an LDAP search for mail synchronization ..... 37
	Configure an LDAP search for group synchronization ..... 39
	Select groups for an LDAP search ..... 42
	Configure an LDAP search for user synchronization ..... 44
	Test the results of an LDAP search ..... 48

	Configure an Exchange Online data source .....	49
	Configure an Exchange Online search for mail synchronization .....	50
	Configure an Exchange Online search for group synchronization .....	51
	Configure an Exchange Online search for user synchronization .....	52
	Test the results of an Exchange Online search .....	54
	Apply filters to an Exchange Online search configuration .....	55
	Configure an Azure data source .....	56
	Configure an Azure search for mail synchronization .....	57
	Configure an Azure search for group synchronization .....	59
	Select groups for an Azure search .....	60
	Configure an Azure search for user synchronization .....	61
	Test the results of an Azure search .....	63
	Configure an Office 365 data source .....	64
	Configure an Office 365 search for mail synchronization .....	64
	Configure an Office 365 search for group synchronization .....	66
	Configure an Office 365 search for user synchronization .....	67
	Test the results of an Office 365 search .....	68
	Apply filters to an Office 365 search configuration .....	69
	Configure the data repository .....	69
	Add limits to a configuration profile .....	72
	Use filters in a configuration profile .....	73
	Include email notifications in a configuration profile .....	75
	Verify a configuration profile .....	76
	Run the Directory Referral Checker .....	77
Chapter 4	Managing synchronization profiles .....	79
	Modify a configuration profile .....	79
	Delete a configuration profile .....	80
	View the log details for the Synchronization Tool .....	80
Chapter 5	Running the Synchronization Tool .....	84
	Synchronize your data with the cloud security services .....	84
	Run the Synchronization Tool from a command-line interface .....	85
	Schedule the Synchronization Tool .....	86

# Introduction to the Synchronization Tool

This chapter includes the following topics:

- [About the Synchronization Tool](#)
- [About synchronization types that are supported by the Synchronization Tool](#)
- [Viewing advanced help topics for the Synchronization Tool](#)

## About the Synchronization Tool

The Synchronization Tool extracts user information from your LDAP directory service and makes the data available to the Email Security.cloud and Web Security.cloud services, including email and web Data Protection services. The synchronized user information includes email addresses and the user groups that each user belongs to. Once you establish connections to your data sources, you can run the tool manually or on a schedule, to ensure that your cloud security services have the most current data.

The Synchronization Tool is a Java executable that operates on a range of platforms that the Sun Java Runtime Environment (JRE) supports.

To download the Synchronization tool, select **Tools > Downloads** in the portal. If you already have JRE installed on your computer, select the version without JRE that matches your operating system. If you do not have JRE installed on your computer, select the appropriate version that includes JRE

After you download and install the tool, a wizard guides you through the steps to establish connections and data extraction from your data sources. Each step is tested and verified.

For complete instructions on how to use the Synchronization tool, refer to the online Help within the tool, or to the [Synchronization Tool Administrator Guide](#).

See “[System requirements for the Synchronization Tool](#)” on page 9.

## About synchronization types that are supported by the Synchronization Tool

Use the Synchronization Tool to extract the following data from your directory sources and export the data to the cloud security services:

- **Mail**

Use Mail synchronization to keep registered email addresses up-to-date for Email Address Registration. You can upload addresses from only the domains that you specify.

---

**Warning:** Use either the Synchronization Tool or the portal (the latter, in combination with outbound harvesting) to maintain your valid address list. Do not use both techniques together as this approach may lead to inaccuracies in your address list data.

---

- **Group and User**

Use Group and User synchronization to keep user and group membership data up-to-date for Web Security and Data Protection services.

Group and User synchronizations are two separate types of synchronization and each type requires a configuration. To configure both of these types, you must run through the Configuration Wizard twice. If you set up a Groups configuration, you must set up a corresponding Users configuration.

---

**Note:** The Synchronization Tool includes an option to synchronize Containers. Currently, no services use Containers.

---

## Viewing advanced help topics for the Synchronization Tool

Additional online Help is available from the Synchronization Tool application. Topics include options for complex directory configurations, how to program regular expressions, and how to use LDAP attribute templates. The online Help is available only in English.

**To view advanced help topics**

- 1 In the Synchronization Tool, click **Help > Contents**.  
A Help system opens with a table of contents on the left.
- 2 Expand the **Advanced topics** folder and explore the contents.



# Installing the Synchronization Tool

This chapter includes the following topics:

- [System requirements for the Synchronization Tool](#)
- [Download and license the Synchronization Tool](#)
- [Before you install the Synchronization Tool](#)
- [Install the Synchronization Tool](#)
- [Start the Synchronization Tool for the first time](#)
- [About standard settings for the Synchronization Tool](#)
- [Update the default Synchronization types](#)
- [Update the Synchronization settings](#)
- [Updating the Log Settings](#)

## System requirements for the Synchronization Tool

The system requirements for the Synchronization Tool are as follows:

**Table 2-1** System requirements for the Synchronization Tool

Requirement	Recommendation
Operating system	<p>The operating system must support the Java Runtime Environment, version 1.6.0_19 or later. We have tested the tool with the following operating systems:</p> <ul style="list-style-type: none"> <li>■ Windows Server 2003 R2</li> <li>■ Windows Vista SP2</li> <li>■ Windows 2008 R2</li> <li>■ Windows 7 Professional SP1</li> <li>■ Windows Server 2012 R2</li> <li>■ Linux Fedora 20</li> <li>■ CentOS Linux 5.11</li> </ul> <p>We also support the tool on the Solaris platform.</p> <p><b>Note:</b> Not all these operating systems support the extraction of data from the Exchange Online and Office 365 data sources. See below for details.</p>
Memory	<p>Minimum 1Gb</p> <p><b>Note:</b> The memory requirement depends on the amount of data that you synchronize and the log detail that you specify.</p>
Disk space	<p>Minimum 1Gb</p> <p><b>Note:</b> The disk space requirement depends on the amount of data that you synchronize and the log detail that you specify.</p>

For the Office 365 and Exchange Online data sources, you can either install the Microsoft Azure source or install the Windows PowerShell source.

- To use the Microsoft Azure source, you first need to create a Service Principal Account on the Office 365 portal to access the Azure Active Directory.
- Windows PowerShell is an integral part of the Windows 7 and Server 2008 R2 operating systems. You can download versions of Windows PowerShell for Windows XP, Server 2003, Vista, and Server 2008. The PowerShell source requires the installation of Windows PowerShell version 3.0 or greater.

The Office 365 data source also requires the following:

- Windows Azure Active Directory Module for Windows PowerShell
- Windows 7 SP1, Windows 8 R2, or Windows Server 2012
- A Windows version of the Synchronization Tool.

The installation process for the Synchronization Tool checks these requirements. You can only select the Office 365 and Exchange Online source modules during installation if the requirements are met.

See [“About the Synchronization Tool”](#) on page 6.

## Download and license the Synchronization Tool

To use the full functionality of the Synchronization Tool, you must obtain a license key from the portal. A single license key enables you to use the tool to synchronize all synchronization types. You request a license key and download the software from the portal. When you request a license key from the portal, you may need to acknowledge an Export Agreement and enter details of your organization in a form.

---

**Note:** If you do not have a license key, you cannot synchronize your data with the cloud security services. You can still create configuration profiles and test them by sending the output to a text file. To use the full functionality, install the Synchronization Tool, then enter the license key into the application.

---

Before downloading the Synchronization Tool from the portal, decide whether you need a version of the Synchronization Tool that includes the Java Runtime Environment (JRE). The **Downloads** page in the portal details the recommended versions of JRE to use with the Synchronization Tool.

### To obtain a license key for the Synchronization Tool

- 1 In the portal, click **Tools > Downloads**.
- 2 In the **Synchronization Tool** section, click **Request Download Access**.
- 3 If required, read the Export Agreement and agree to the terms and conditions. If you are not required to acknowledge an Export Agreement you can view your license key using the **Request License Key** button.
- 4 If required, complete the **Synchronization Download Form**. Enter the details in English.
  - In the **Authorized contact details** section, enter the name of a director or senior manager at your organization.
  - In the **Download details** section, enter the full address of your organization. Note that we cannot accept a post-office box number.
- 5 Click **Send**.

You receive an email within two business days, to tell you when you can download the Synchronization Tool from the portal.

- 6 When you receive an authorization email, in the portal click **Tools > Downloads**.  
The **Synchronization Tool** section includes **Request License Key** and **Download** buttons.
- 7 Click **Request License Key** to view the license key for the Synchronization Tool.
- 8 Review the versions of the Synchronization Tool that are available.
  - Note that the Office 365 data source requires a Windows version of the tool.
- 9 Select the required version of the Synchronization Tool and click **Download** to download the software.

#### To add a license key to the Synchronization Tool

- 1 When you have installed the Synchronization Tool, start the application.
- 2 Click **Edit > Settings**.
- 3 Click the **Add License** tab and complete the **Licensed to** and **License key** fields.
- 4 Click **Apply** to save the details.

See [“Before you install the Synchronization Tool”](#) on page 12.

See [“Install the Synchronization Tool”](#) on page 13.

See [“Start the Synchronization Tool for the first time”](#) on page 14.

See [“About the Synchronization Tool”](#) on page 6.

## Before you install the Synchronization Tool

You must decide on a suitable system within your network on which to install and run the Synchronization Tool. This system must have internal network access to your directory system through LDAP and have external network access to the portal through HTTPS.

To run the tool on an automated basis, decide whether to invoke the tool by a scheduling system (e.g. Microsoft Windows Scheduler) or by another application.

The tool builds a data file to track changes to your source data. We recommend that you use a single instance of the tool to synchronize a given set of source data. Running multiple instances can result in the source data being out of step with the data in the cloud security services.

Create a portal account specifically for use with the Synchronization Tool. This approach helps to avoid any changes being made to the account that may interfere with the synchronization process, e.g. password changes. The account must be a global administrator account.

Before installing the Synchronization Tool, ensure that you have the following:

- Your portal account details
- The Synchronization Tool license key
- The address of your directory server and the authentication details that you need to perform searches on it  
Authentication may be possible anonymously. Anonymous authentication may restrict the results that the search returns.

See [“Download and license the Synchronization Tool”](#) on page 11.

See [“Install the Synchronization Tool”](#) on page 13.

See [“About the Synchronization Tool”](#) on page 6.

## Install the Synchronization Tool

We recommend that you create a portal account specifically for use with the Synchronization Tool. This approach helps to avoid any changes being made to the account that may interfere with the synchronization process, e.g. password changes. The account must be a global administrator account. For further considerations and system requirements, review the following topics:

See [“System requirements for the Synchronization Tool”](#) on page 9.

See [“Before you install the Synchronization Tool”](#) on page 12.

### To install the Synchronization Tool

- 1 Ensure that all other applications running on the computer are closed, before you start the installation process.
- 2 Start the installer.

For Windows systems, click the executable file that you downloaded from the portal.

For Linux systems, open a terminal, ensure that the execute permission is set on the installer file, and run it. For example.

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

- 3 In the **Welcome** dialog, click **Next**.

- 4 In the **License Agreement** dialog box, read and acknowledge the agreement, and click **Next**.
- 5 In the **Select Destination Directory** dialog box, choose the directory in which to install the tool; for example `C:\Program Files\Schemus`. Click **Next**.  
  
This step is skipped if the installation is an upgrade from a previous version of the tool.
- 6 In the **Select Start Menu Folder** dialog box, choose where you want to launch the Synchronization Tool from; the **Start** menu for Windows, and **Symlinks** for Linux. Click **Next**.
- 7 In the **Select Configuration Directory** dialog box, select a destination for the configuration settings and then click **Next**.  
  
Configuration settings determine the types of synchronization that you can to perform - email, users, and groups. If you upgrade to a later version of the Synchronization Tool, you can keep your existing settings or create new ones.  
  
If you want multiple users to run the tool, select a shared directory.
- 8 In the **Office 365 modules** dialog box, select the Office 365 source modules that you want to use. Note that you can only select these sources if your system satisfies the requirements.
- 9 In the **Information** dialog box, read the release information and then click **Next**.
- 10 Click **Finish** to exit the setup wizard.

See [“Start the Synchronization Tool for the first time”](#) on page 14.

See [“About the Synchronization Tool”](#) on page 6.

See [“Download and license the Synchronization Tool”](#) on page 11.

See [“System requirements for the Synchronization Tool”](#) on page 9.

## Start the Synchronization Tool for the first time

When you start the Synchronization Tool for the first time, you choose the data that you want to extract from your directory sources and synchronize with the cloud security services. Select from the following synchronization types:

- Mail
- Group + Users
- Containers

The Containers synchronization type will be implemented in future functionality. Currently no cloud security services use containers.

When you create a new profile using the Configuration Wizard, you can only choose from the types that you have specified. To change the default synchronization types, click **Edit > Settings > Synchronization** and select the check boxes for the types that you want to use.

---

**Note:** If you update the Synchronization Tool to a later version, the synchronization types that you selected when you first installed the tool are retained, and you are not presented with the option to change them.

---

See [“About configuration profiles”](#) on page 24.

See [“About the Synchronization Tool”](#) on page 6.

## About standard settings for the Synchronization Tool

In the **Settings** dialog, you view and amend various standard settings such as the license key, the default synchronization types, and the access details for the portal.

### To access the standard settings

- ◆ In the Synchronization Tool, click **Edit > Settings**.

The **Settings** dialog is displayed.

The settings that you can change in this dialog are described in the following table.

**Table 2-2** Standard settings for the Synchronization Tool

Setting	Description
License	You need a license key to run the tool and synchronize your data with the portal. You can run the tool in test mode without a license.  See <a href="#">“Download and license the Synchronization Tool”</a> on page 11.

**Table 2-2** Standard settings for the Synchronization Tool (*continued*)

Setting	Description
<b>Synchronizations</b>	<p>The first time that you start the Synchronization Tool, you are prompted to enter the types of data that you want to extract from your directory sources. In the <b>Synchronizations</b> dialog, you can change the synchronization types that are displayed when you create a new configuration profile.</p> <p>See <a href="#">“Update the default Synchronization types”</a> on page 19.</p> <p>See <a href="#">“Update the Synchronization settings”</a> on page 19.</p>
<b>Log Settings</b>	<p>The <b>Log Settings</b> enable you to define the level of detail that is written to the log files and the number days that you want to keep the logs for.</p> <p>See <a href="#">“Updating the Log Settings”</a> on page 21.</p> <p>See <a href="#">“View the log details for the Synchronization Tool”</a> on page 80.</p>
<b>Exchange Online</b>	<p>Enter the authentication details for connecting to the Microsoft cloud to receive the information that is used by the Office 365 and Exchange Online data sources.</p> <p>The <b>Access URL</b> field is the address used to connect to the Microsoft cloud. Do not change the default value in this field. If you change this line by accident, click <b>Reset Defaults</b> to recover the original value.</p> <p>Enter your account <b>Username</b> and <b>Password</b> details for the Office 365 cloud services and click <b>Apply</b>.</p>



**Table 2-2** Standard settings for the Synchronization Tool (*continued*)

Setting	Description
<b>Azure</b>	<p>The <b>Host Name</b> field is the name of the server that processes requests for the Microsoft Azure service. This setting is the default and you should not need to change it.</p> <p>The <b>Tenant Context ID</b> is an identifier that Microsoft provides to access the Office 365 portal.</p> <p>The <b>Principal ID</b> is a hexadecimal GUID value of your Service Principal account. Note that Microsoft sometimes refers to Principal ID as Client ID.</p> <p>The <b>Symmetric Key</b> is your Service Principal account password or key that was specified when the account was created.</p> <p>The <b>HTTPS Proxy</b> lets you configure a proxy to connect to the Microsoft Azure service.</p> <p>Click <b>Apply</b> to test and authenticate the settings you entered. You can also select <b>Reset Defaults</b> to recover the original values.</p> <p>See <a href="#">“Configure an Azure search for mail synchronization”</a> on page 57.</p> <p>See <a href="#">“Configure an Azure search for group synchronization”</a> on page 59.</p> <p>See <a href="#">“Configure an Azure search for user synchronization”</a> on page 61.</p>

**Table 2-2** Standard settings for the Synchronization Tool (*continued*)

Setting	Description
LDAP	<p>The LDAP search string is used to determine the entries to display in the <b>LDAP</b> drop-down list when you set up the LDAP search options.</p> <p>The default setting is suitable for most types of LDAP server and you should not need to edit this string.</p> <p>See <a href="#">“Configure an LDAP search for mail synchronization”</a> on page 37.</p> <p>See <a href="#">“Configure an LDAP search for group synchronization”</a> on page 39.</p> <p>See <a href="#">“Configure an LDAP search for user synchronization”</a> on page 44.</p>
Symantec.cloud	<p>The <b>Access URL</b> field is the address used to connect to the portal. Do not change the default value in this field. If you change this line by accident, click <b>Reset Defaults</b> to recover the original value.</p> <p>Enter your portal account <b>Username</b> and <b>Password</b> and click <b>Apply</b>.</p> <p>If you receive an error message you may need to connect to the portal through an HTTP proxy. To access the Internet through an HTTP proxy, change select <b>Manual</b> from the <b>HTTPS Proxy</b> drop-down and enter the connection details in the newly appeared fields. If in doubt, start your Internet browser and view the connection settings.</p>

## Update the default Synchronization types

When you start the Synchronization Tool for the first time after installation, you are prompted to choose the synchronization types that you want to use in your configuration profiles. You can modify the list of default synchronization types in the **Settings** dialog.

To modify the default Synchronization types

- 1 Start the Synchronization Tool.
- 2 Select **Edit > Settings**.
- 3 Select **Synchronizations** from the left-hand menu.
- 4 In the **Available Synchronization Types** section, select the types that you want to choose from when you create a configuration profile.
- 5 Click **Apply** to save your changes.

## Update the Synchronization settings

The Synchronization settings control how extracted data is stored on the cloud server.

To update the Synchronization settings

- 1 Start the Synchronization Tool
- 2 Select **Edit > Settings**.
- 3 Select **Synchronizations** from the left-hand menu.
- 4 In the **Synchronization Settings** section, review the following settings.

## Error recovery

The **Error recovery** setting determines the action to take if communication between your computer and the cloud server fails. Choose from the following options:

- **Replace server contents**

On the next synchronization, the tool sends all data that it retrieves from the directory to the cloud security services.

The synchronization overwrites the content that is already held on the server.

You lose any data that you have not added to the cloud security services using the Synchronization Tool.

- **Retry update**

After a communications error with the cloud security services, the tool makes a note of all the changes that were to be made. On the next synchronization, these are merged with any new changes made to the data sources, and the cloud security services are updated with the combined results. Data that you have not added to the cloud security services by the Synchronization Tool is preserved.

### Difference calculation

The **Difference calculation** setting manages the local storage of data on the computer running the application for the purposes of detecting changes between previous synchronizations. Choose from the following options:

- **Store extracted data**

This setting stores the data that the tool has retrieved from the directory and sent to the cloud security services. The data is stored in readable text.

- **Store a digest**

This setting stores a cryptographic checksum of the data that the tool has retrieved from the directory. Changes to data are detected but details of those changes are unavailable.

**Note:** This setting does not affect Mail synchronization. The full email address is required to enable the addresses that have been deleted in the directory to be removed from the cloud security services.

- 5 Click **Apply** to save your changes.

## Updating the Log Settings

The **Log Settings** enable you to define the level of detail that is written to the log files and the number days that you want to keep the log files.

### To update the Log Settings

- 1 Start the Synchronization Tool.
- 2 Select **Edit > Settings**.
- 3 Select **Log Settings** from the left-hand menu.

- 4 In the **Log Detail** section, review the following settings:

**Log Details**

Use the sliders to determine the level of detail that is held in the log files.

The **All Logging** slider determines the log messages that are written to the application's log files.

The **System Log** slider determines the number of log messages that are written to your system logs. On Windows systems this is the Event log. On Linux this is the syslog. At the lowest setting, only the most important messages are logged.

**Log Lifetime**

Enter the number days that you want to retain the logs. To keep the log files indefinitely, set this number to 0. If you choose to keep the log files indefinitely, ensure that you have adequate disk space to allow new logs to be created. The default setting is 30 days.

- 5 Click **Apply** to save your changes.

# Creating configuration profiles

This chapter includes the following topics:

- [About configuration profiles](#)
- [Create a configuration profile - process overview](#)
- [Select a data source for a configuration profile](#)
- [Select multiple data sources for a configuration profile](#)
- [Select a file source for mail synchronization](#)
- [Select a file source for group synchronization](#)
- [Select a file source for user synchronization](#)
- [Configure an LDAP data source](#)
- [Configure an LDAP server - advanced settings](#)
- [Configure an LDAP search for mail synchronization](#)
- [Configure an LDAP search for group synchronization](#)
- [Configure an LDAP search for user synchronization](#)
- [Test the results of an LDAP search](#)
- [Configure an Exchange Online data source](#)
- [Configure an Exchange Online search for mail synchronization](#)
- [Configure an Exchange Online search for group synchronization](#)

- [Configure an Exchange Online search for user synchronization](#)
- [Test the results of an Exchange Online search](#)
- [Apply filters to an Exchange Online search configuration](#)
- [Configure an Azure data source](#)
- [Configure an Azure search for mail synchronization](#)
- [Configure an Azure search for group synchronization](#)
- [Configure an Azure search for user synchronization](#)
- [Test the results of an Azure search](#)
- [Configure an Office 365 data source](#)
- [Configure an Office 365 search for mail synchronization](#)
- [Configure an Office 365 search for group synchronization](#)
- [Configure an Office 365 search for user synchronization](#)
- [Test the results of an Office 365 search](#)
- [Apply filters to an Office 365 search configuration](#)
- [Configure the data repository](#)
- [Add limits to a configuration profile](#)
- [Use filters in a configuration profile](#)
- [Include email notifications in a configuration profile](#)
- [Verify a configuration profile](#)
- [Run the Directory Referral Checker](#)

## About configuration profiles

To extract email, user and group data from a source, you create a configuration profile that includes the following:

- The details of the data source
- The data repository that you want to extract the data to.

You can add filters to ensure that you only extract the data that you require. A Configuration Wizard guides you through the process of creating a profile.



A configuration profile can contain more than one synchronization type. To add a further synchronization type, proceed through the wizard for the first type and save your settings. Then return to the first step to select another synchronization type to configure.

Configuration settings and synchronization data are stored in a directory with the same name as the configuration profile. The location varies according to the operating system, as follows:

**Table 3-1** Synchronization data locations for operating systems

Operating system	Location
Windows XP/2003	C:\Documents And Settings\All Users\Application Data\Schemus\configurations
Windows Vista/7/2008/2012	C:\ProgramData\Schemus\configurations
Linux (home directories)	~/schemus/configurations
Linux (shared)	/var/opt/schemus/configurations

## Create a configuration profile - process overview

A configuration profile is a combination of settings that you create and save using the Configuration Wizard. You run a profile when you want to synchronize your data with the cloud security services.

The following table provides an overview of the procedure for creating a configuration profile:

**Table 3-2** Process overview for creating configuration profiles

Step	Action	Details
Step 1	Start the Configuration Wizard	To start the wizard, select <b>File &gt; New</b> .

**Table 3-2** Process overview for creating configuration profiles (*continued*)

Step	Action	Details
Step 2 - Name	Enter a name and a synchronization type for the configuration	<p>Enter a name for the configuration profile.</p> <p>Select the type of synchronization that you want to configure in the profile:</p> <ul style="list-style-type: none"> <li>■ Mail</li> <li>■ Groups</li> <li>■ Users</li> </ul> <p>If you selected only the Mail synchronization type when you started the tool for the first time, the <b>Synchronization Type</b> drop-down does not appear.</p> <p>See <a href="#">“About synchronization types that are supported by the Synchronization Tool”</a> on page 7.</p>
Step 3 - Data source	Choose a data source	<p>Choose from the following data source types:</p> <ul style="list-style-type: none"> <li>■ Exchange Online</li> <li>■ Office 365</li> <li>■ Microsoft Active Directory</li> <li>■ Lotus Domino</li> <li>■ Generic LDAP</li> <li>■ File</li> <li>■ Azure</li> </ul> <p>To configure more than one source, select the <b>Multiple Sources</b> check box.</p> <p>See <a href="#">“Select a data source for a configuration profile”</a> on page 28.</p> <p>See <a href="#">“Select multiple data sources for a configuration profile”</a> on page 30.</p>
Step 4 - Server details	Enter the connection details for the data source	<p>Enter the address and the connection details for the data source from which you want to extract mail or group and user details.</p> <p>See <a href="#">“Configure an LDAP data source”</a> on page 34.</p> <p>See <a href="#">“Configure an Exchange Online data source”</a> on page 49.</p> <p>See <a href="#">“Configure an Azure data source”</a> on page 56.</p> <p>See <a href="#">“Configure an Office 365 data source”</a> on page 64.</p>

**Table 3-2** Process overview for creating configuration profiles (*continued*)

Step	Action	Details
Step 5 - Search details	Enter the details of the attribute search	<p>Enter the search query information to find the email address, group, and user data to synchronize.</p> <p>See <a href="#">“Configure an LDAP search for mail synchronization”</a> on page 37.</p> <p>See <a href="#">“Configure an LDAP search for group synchronization”</a> on page 39.</p> <p>See <a href="#">“Configure an LDAP search for user synchronization”</a> on page 44.</p> <p>See <a href="#">“Configure an Exchange Online search for mail synchronization”</a> on page 50.</p> <p>See <a href="#">“Configure an Exchange Online search for group synchronization”</a> on page 51.</p> <p>See <a href="#">“Configure an Exchange Online search for user synchronization”</a> on page 52.</p> <p>See <a href="#">“Configure an Azure search for mail synchronization”</a> on page 57.</p> <p>See <a href="#">“Configure an Azure search for group synchronization”</a> on page 59.</p> <p>See <a href="#">“Configure an Azure search for user synchronization”</a> on page 61.</p> <p>See <a href="#">“Configure an Office 365 search for mail synchronization”</a> on page 64.</p> <p>See <a href="#">“Configure an Office 365 search for group synchronization”</a> on page 66.</p> <p>See <a href="#">“Configure an Office 365 search for user synchronization”</a> on page 67.</p>
Step 6 - Testing	Test the results of the attribute search	<p>Use the test page to confirm that you have retrieved the expected attributes.</p> <p>See <a href="#">“Test the results of an LDAP search”</a> on page 48.</p> <p>See <a href="#">“Test the results of an Exchange Online search”</a> on page 54.</p> <p>See <a href="#">“Test the results of an Office 365 search”</a> on page 68.</p> <p>See <a href="#">“Test the results of an Azure search”</a> on page 63.</p>
Step 7 - Data repository	Choose a data repository	<p>Choose to write your data to the cloud security services or to File. You use the File option to test a configuration profile, before synchronizing your data with the cloud security services.</p> <p>See <a href="#">“Configure the data repository”</a> on page 69.</p>

**Table 3-2** Process overview for creating configuration profiles (*continued*)

Step	Action	Details
Step 8 - Filters	Choose to filter your data	<p>You use filters to exclude or make modifications to the email addresses and user and group data that the tool extracts from your data source. The changes or exclusions are made before the tool writes the data to the data repository.</p> <p>See <a href="#">“Use filters in a configuration profile”</a> on page 73.</p>
Step 9 - Limits	Add restrictions on the number of changes that a synchronization run can make	<p>You can set restrictions on the number of changes that are made when you synchronize data with the cloud server. When you set limits, you avoid making undesired large-scale changes.</p> <p>See <a href="#">“Add limits to a configuration profile”</a> on page 72.</p>
Step 10 - Notification	Enter email addresses for notifications	<p>You can choose to receive an email when a synchronization run has completed.</p> <p>See <a href="#">“Include email notifications in a configuration profile”</a> on page 75.</p>
Step 11 - Summary	Review a summary of your profile	<p>Review the settings that you have entered for your configuration profile.</p> <p>Click <b>Verify</b> to test the settings in the configuration.</p> <p>Click <b>Schedule</b> to schedule the tool to run at a specific time or at regular intervals.</p> <p>See <a href="#">“Verify a configuration profile”</a> on page 76.</p> <p>See <a href="#">“Schedule the Synchronization Tool”</a> on page 86.</p>

## Select a data source for a configuration profile

In the Data source step of the Configuration Wizard, you establish the **Source Type** for the configuration profile. When you create a profile for Mail, Group and User synchronization, you can select from the following options:

- Microsoft Active Directory
- Exchange Online
- Office 365
- Lotus Domino
- Generic LDAP
- File
- Azure

For LDAP server, Exchange Online, and Office 365 synchronization, the **Source Type** determines the default attributes that are used to retrieve data later in the wizard.

When you select **File** as the data source, you select a text file containing a list of records for synchronizing with your destination data repository.

Typically, large organizations have a complex directory configuration with multiple directory sources, domain configurations, or directory Naming Contexts, which cannot be searched from a single search base.

Where multiple LDAP searches are required, the options available are to:

- Create a single configuration with multiple sources to be merged when synchronizing.
- Create a separate configuration for each search.

When a single LDAP search cannot be configured to retrieve all the data, we recommend that multiple sources are specified within a single configuration. The Synchronization Tool merges the data from all of the sources before it sends them to the cloud security services. Multiple Sources are configured by clicking on **Data Source** from the left pane in the wizard and selecting the Multiple Sources check box.

---

**Note:** Since a number, rather than a GUID or DN, identifies the Primary Group Token in Active Directory, groups from different domains may have the same identifier. If you search multiple domains for Users and Groups, we recommend that the group ID attribute includes a value such as the Domain Component (DC). By doing so, groups from different domains can be distinguished from each other. The default attributes used by the Synchronization Tool include the DC for this reason.

---

Multiple configurations are not recommended since each configuration operates independently of the others. So multiple configurations can lead to corruption or inconsistent results when you synchronize your data with the cloud security services.

One situation where multiple configurations may safely be used is for mail synchronizations where multiple email domains are configured on the portal. Each configuration must use different email domains. To ensure that each configuration uses a different email domain, select a different set of domains on the **Domains** page in each configuration.

We do not recommend that you configure multiple configurations for Group and User synchronization as the group memberships may not be updated correctly. If you do create multiple configurations for Mail, or Group and User synchronization with overlapping email domains, select **Retry update** from the **Synchronization**

**Type** settings screen. Retrying the update reduces the likelihood that data from one synchronization deletes the data from another.

## Select multiple data sources for a configuration profile

You use multiple data sources in the following situations:

- To search multiple areas of a single LDAP server
- To search multiple LDAP servers
- To combine LDAP searches with Office 365 and Exchange Online searches.

If you have multiple data sources, the tool consolidates all of your source data before it synchronizes the data with your destination target.

### To add an additional data source to a configuration profile

- 1 In the Configuration Wizard, select **Data Source** from the left-hand menu.
- 2 Select the **Multiple Sources** check box.
- 3 In the **Source** drop-down, select **Add another source**. The source name defaults to the source type.
- 4 In the **Source Type** drop-down, select a data source.
- 5 Provide the following details for a data source before you add an additional one.
  - Its own server name and port
  - The top of the search point in the directory tree
  - The attributes to retrieve from the server

When you define multiple sources, the **Multiple Sources** check box is disabled. You cannot switch back to the single data source definition window unless you delete the additional data source definitions.

To delete a data source definition, select it from the **Source** drop-down list and click **Remove**.

See [“Configure an LDAP data source”](#) on page 34.

See [“Configure an Exchange Online data source”](#) on page 49.

See [“Configure an Office 365 data source”](#) on page 64.

See [“Configure an Azure data source”](#) on page 56.

## Select a file source for mail synchronization

In the **Data source** step of the Configuration Wizard, you can specify that you want to extract your email addresses from a file.

Enter a folder path and file name, or browse to a file.

A Mail synchronization source file should consist of one or more SMTP email addresses on individual lines. The line separators in the file can be either carriage returns and line feeds (known as DOS format), or line feeds only (known as UNIX format).

See [“Create a configuration profile - process overview”](#) on page 25.

## Select a file source for group synchronization

In the Data source step of the Configuration Wizard, you can specify that you want to extract your group data from a file.

Either enter a folder path and file name, or browse to a file. A Group synchronization source file is in the same format as the CSV or the LDIF output file.

**Table 3-3** Source files for Group synchronization

Source file type	Description
CSV	<p>The CSV file should not contain a header line. Data lines should consist of:</p> <ul style="list-style-type: none"> <li>■ The distinguished name of the group (optional)</li> <li>■ The Parent LDAP Container ID (only if the DN is present)</li> <li>■ A unique identifier (GUID)</li> <li>■ The group name</li> <li>■ Identifiers (GUIDs) for the groups that this group belongs to, if any—separated by commas</li> </ul> <p>Each field must be separated by a comma, and each group must start on a new line. Any commas or backslashes that occur in the fields must be escaped (comma = \0x002c, backslash = \0x005c).</p> <p>The line separators in the file can be one of the following type:</p> <ul style="list-style-type: none"> <li>■ Carriage returns and line feeds (known as DOS format). For example: <pre>dn=CN=staff\0x002cOU=Groups\0x002cDC=mycorp\0x002cDC=com, parent-naming-component-id=BBBBBBBBB-BBBB-BBBB-BBBBBBBBBBBBBBBBBB, FFFFFFFF-FFFF-FFFF-FFFFFFFFFFFFFFFF,staff, AAAAAAAA-AAAA-AAAA-AAAAAAAAAAAAAAAA</pre> </li> <li>■ Line feeds (known as UNIX format). For example: <pre>FFFFFFFF-FFFF-FFFF-FFFFFFFFFFFFFFFF,staff, AAAAAAAA-AAAA-AAAA-AAAAAAAAAAAAAAAA</pre> </li> </ul> <p>The distinguished name and parent-naming-component-id fields can be omitted if not required.</p>
LDIF	<p>LDIF format should also include the <code>ObjectClass</code> (in this case, <code>Group</code>) and the most significant Naming Component of the Distinguished Name. A blank line must separate each LDIF record. For example:</p> <pre>dn: CN=staff,OU=Groups,DC=mycorp,DC=com objectClass: Group cn: staff name: staff objectGUID: FFFFFFFFFF-FFFF-FFFF-FFFFFFFFFFFFFFFF parent-ldapcontainer-id: BBBBBBBBBB-BBBB-BBBB-BBBBBBBBBBBBBBBBBB</pre>

## Select a file source for user synchronization

In the **Data source** step of the Configuration Wizard, you can specify that you want to extract your user data from a file.



Either enter a folder path and file name, or browse to a file. A User synchronization source file is the same format as the CSV or LDIF output file.

**Table 3-4** Source files for user synchronization

Source file type	Description
CSV	<p>The CSV file should not contain a header line. Data lines should consist of:</p> <ul style="list-style-type: none"> <li>■ The distinguished name of the user (optional)</li> <li>■ The creation date, alias email address, ML-IMService, Display Name and Parent LDAP Container ID attributes (only if the DN is present)</li> <li>■ A unique identifier (GUID)</li> <li>■ The user name</li> <li>■ The user's primary email address</li> <li>■ The identifiers (GUIDs) of groups that this user belongs to, if any, separated by commas</li> </ul> <p>Each field must be separated by a comma, and each user record must start on a new line. Any commas or backslashes occurring in the fields must be escaped (comma = \0x002c, backslash = \0x005c). The line separators in the file can be one of the following type:</p> <ul style="list-style-type: none"> <li>■ Line feeds (known as UNIX format). For example:</li> </ul> <pre>FFFFFFFF-FFFF-FFFF-FFFFFFFFFFFFFFFFFFFF,jsmith,jsmith@mycorp.com, AAAAAAAA-AAAA-AAAA-AAAAAAAAAAAAAAAAAAAA</pre> <ul style="list-style-type: none"> <li>■ Carriage returns and line feeds (known as DOS format). For example:</li> </ul> <pre>dn=CN=john smith\0x002cOU=Users\0x002cDC=mycorp\ 0x002cDC=com,createdtimestamp=20080718114948.0Z\ 0x002displayname=John Smith\0x002mailalias= jsmith@mycorp.org0x005c0x002cj.smith@mycorp.com\ 0x002cml-imservices=IM:YHO:jsmith\ 0x002cparent-naming-component-id= BBBBBBBBB-BBBB-BBBB-BBBBBBBBBBBBBBBBBB, FFFFFFFF-FFFF-FFFF-FFFFFFFFFFFFFFFFFFFF,jsmith,jsmith@mycorp.com, AAAAAAAA-AAAA-AAAA-AAAAAAAAAAAAAAAAAAAA</pre> <p>The distinguished name and the createdtimestamp,mailalias,ml-imservices,displayname, and parent-naming-component-id fields can be omitted if not required.</p>

Table 3-4 Source files for user synchronization (continued)

Source file type	Description
LDIF format	<p>The LDIF format should additionally include the <code>ObjectClass</code> (in this case, <code>User</code>) and the most significant naming component of the Distinguished Name. LDIF records are separated by a blank line. For example:</p> <pre>dn: CN=john smith,OU=Users,DC=mycorp,DC=com objectClass: User cn: john smith name: jsmith mail: jsmith@mycorp.com memberOf: AAAAAAAA-AAAA-AAAA-AAAAAAAAAAAAAAAA mailalias: jsmith@mycorp.org mailalias: j.smith@mycorp.com ml-imservices: IM:YHO:jsmith objectGUID: FFFFFFFF-FFFF-FFFF-FFFFFFFFFFFFFFFF parent-ldapcontainer-id: BBBBBBBB-BBBB-BBBB-BBBBBBBBBBBBBBBB displayname: John Smith createdtimestamp: 20080718114948.0Z</pre>

## Configure an LDAP data source

When you select Microsoft Active Directory, Lotus Domino or Generic LDAP as the data source for a configuration profile, you provide the connection details for your directory server.

To configure an LDAP data source

- 1 In the **LDAP** step of the Configuration Wizard, complete the following fields:

Host name	Enter the IP network address of the LDAP server. You can enter the name in DNS form (for example, <code>dsa.acme.com</code> ) or in dotted quad (for example, <code>192.168.0.10</code> ).
Port number	Confirm the <b>Port number</b> . The default for unencrypted LDAP communication is port 389. Do not change this setting unless you communicate with your LDAP server on a non-standard port.

## Authentication

Select one of the following options:

- **Anonymous**

No authentication details are required to access the LDAP server. Anonymous authentication may restrict the results that the search returns.

- **Simple**

If you select this option, enter the user name for your server, and optionally the password. The credentials are sent unencrypted so should only be used on a secure connection.

- **Strong**

If you select this option, enter the user name and password for your server. The credentials are encrypted and if supported by the server, the LDAP session is also protected.

Select an encryption type from the drop-down list:

- **Plain**

Sends unencrypted text over the connection.

- **SSL - Secure Socket Layer**

The SSL provides a cryptographically-secure communication that uses a certificate that the LDAP server provides.

**Note:** The certificate must be signed by a trust point that is held in the Java certificate store. Self-signed certificates must be signed by a trust point that is imported into the Java certificate store. For further information, click **Help > Contents** in the Synchronization Tool and review the **Advanced topics** section.

- **TLS - Transport Layer Security**

TLS is similar to SSL, and also requires a certificate that the LDAP server provides. An anonymous plain connection is initially established, then upgraded to an authenticated secure connection.

- 2 Click **Advanced** to establish paging size and continuation references.

See [“Configure an LDAP server - advanced settings”](#) on page 36.

- 3 Click **Next**. The application attempts to communicate with your LDAP server using your settings. If there is a problem communicating with the server, an error message is displayed. Click **Back** to change your settings.

# Configure an LDAP server - advanced settings

In the **LDAP** step of the Configuration Wizard, you enter the address and the connection details for the LDAP server to extract mail, or group and user details from. Click **Advanced** to specify paging and continuation references.

Table 3-5 LDAP - Advanced settings

Setting	Description
Paging	<p>Some directory servers can be configured to limit the maximum number of results that can be returned at one time. The paging facility overcomes 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 201 to 220 the third time.</p> <p>To enable paging, in the <b>Paging type</b> drop-down list, select <b>page</b>. In the <b>Page Size</b> text box, enter the number of results to retrieve. The default page size is 50 results. This means that a maximum of 50 results are retrieved from the LDAP server at one time.</p> <p>Not all LDAP servers support paging. If paging is unavailable, the Synchronization Tool attempts the search without paging.</p>

**Table 3-5** LDAP - Advanced settings (*continued*)

Setting	Description
<b>Continuation References</b>	<p>An LDAP server can contain referrals to other points on the server, or to points on other LDAP servers. You can specify what the application does when it encounters a referral on an LDAP server, or if a referred server is not available. To define how to handle referrals, in the <b>Action</b> drop-down list, select one of the following:</p> <ul style="list-style-type: none"> <li>■ <b>Follow</b> By default, the application follows any referrals to continue retrieving results. If a referral cannot be followed, the synchronization is aborted.</li> <li>■ <b>Ignore</b> The application ignores the referral and continues the synchronization process. Abort update - the application does not attempt to follow any referrals. If a referral is encountered, it ends the synchronization process and logs this fact.</li> <li>■ <b>Abort update</b> The application does not attempt to follow any referrals. If a referral is encountered, it ends the synchronization process and logs this fact.</li> </ul> <p>For further information, click <b>Help &gt; Contents</b> in the Synchronization Tool and review the topic <i>Continuation references and referrals</i> in the Advanced topics section.</p> <p>If you notice that a referred server is only available intermittently, you can set threshold limits. Threshold limits ensure that the update does not continue where there is a noticeable difference in the number of results that are returned. So if a referred server is unavailable, the threshold limit stops the update, and prevents the potential loss of data from an entire server.</p>

## Configure an LDAP search for mail synchronization

In the **LDAP search configuration** step of the Configuration Wizard, select the level of the hierarchical tree structure at which to search for email addresses.

We recommend that you accept the default LDAP search settings for your Mail synchronization.

**To configure the LDAP search configuration settings for mail synchronization**

- 1 In the **LDAP search configuration** step of the Configuration Wizard, complete the following fields:

**Search base** The **Search base** field and the drop-down list let you navigate through the LDAP directory. The list is initially populated with the directory's naming contexts.

Select an entry from the drop-down list or edit the search base field to select a search base. When an item is selected from the list, the drop-down displays the entries at that directory level that are specified in the **Search base** field. To move up the tree, click on the first item in the drop-down list.

Some LDAP servers do not let you search for entries at their root. In this case, you must enter a search base or select one of the items from the list before you can continue.

**Search scope** The **Search scope** setting lets you select the depth of the search:

- **Object**—searches for a single object that is in the location that is specified as the search base
- **One level**—searches for all objects at the level that is specified in the **Search base** field;
- **Sub-tree**—searches from the level that is specified in the **Search base** downwards, until the LDAP server restricts the results or the search or reaches the bottom of the tree. Use this option to return the most results.

**Search filter** The **Search filter** setting determines the objects that are returned from the directory.

To select from a list of common filters, click in the **Search filter** field and click **Examples**. You can type a search filter directly into the **Search filter** field or you can enter a filter using the LDAP filter editor. To use the LDAP filter editor, click the button to the right of the **Search filter** field.

- 2 Click **Save** to save your changes, or **Next** to move to the next step in the Wizard.

### To configure the advanced mail search attributes

- 1 In the **LDAP search configuration** step of the Configuration Wizard,, click **Advanced**.
- 2 Specify the data to retrieve from the LDAP server for the mail synchronization.

The default settings for these attributes are taken from the LDAP server type you selected as your data source on the **Data source** page. Attributes are entered as templates and let you extract and transform data from any number of LDAP attributes.

#### **Primary Mail**

This attribute contains the mail address attributes within the object that are returned by the search filter.

#### **Mail Aliases**

This attribute is a list of optional alternatives to the **Primary Mail** attributes. To view and select from a list of mail attribute examples, click in the **Mail Aliases** field and click **Examples**.

- 3 Click **Save** to save your changes, or **Next** to move to the next step in the Wizard.

## Configure an LDAP search for group synchronization

In the **LDAP search** step of the Configuration Wizard, you select the level of the hierarchical tree structure at which to search for group entries.

We recommend that you accept the default LDAP search settings for your Groups synchronization.

### To configure the LDAP search configuration settings for group synchronization

- 1 In the **LDAP search** step of the Configuration Wizard, complete the following fields:

<b>Search base</b>	<p>The <b>Search base</b> field and the drop-down list let you navigate through the LDAP directory.</p> <p>Enter your search starting point in the LDAP server tree structure, then select an entry in the drop-down list.</p> <p>That entry appears in the <b>Search base</b> field. The drop-down list now contains all the entries at the directory level that are specified in the <b>Search base</b> field. To move up the tree, click on the first item in the drop-down list.</p> <p>Some LDAP servers do not let you search for entries at their root. In this case, you may need to enter a search base manually before you can browse further.</p>
<b>Search scope</b>	<p>The <b>Search scope</b> setting lets you select the depth of the search:</p> <ul style="list-style-type: none"> <li>■ <b>Object</b>—searches for a single object that is in the location that is specified as the search base</li> <li>■ <b>One level</b>—searches for all objects at the level that is specified in the <b>Search base</b> field;</li> <li>■ <b>Sub-tree</b>—searches from the level that is specified in the <b>Search base</b> downwards, until the LDAP server restricts the results or the search or reaches the bottom of the tree. Use this option to return the most results.</li> </ul>
<b>Search filter</b>	<p>The <b>Search filter</b> setting defines the type of object to return data on.</p> <p>To select from a list of common filters, click in the <b>Search filter</b> field and click <b>Examples</b>. You can type a search filter directly into the <b>Search filter</b> field or you can enter a filter using the LDAP filter editor. To use the LDAP filter editor, click the button to the right of the <b>Search filter</b> field.</p>
<b>Name</b>	<p>The <b>Name</b> field defines a rule for constructing a text name that is used to represent individual groups. An attribute template is used to construct the group's name.</p>

- 2 Click **Save** to save your changes, or **Next** to move to the next step in the Wizard.

#### To configure the advanced group search attributes

- 1 In the **LDAP search** step of the Configuration Wizard, click **Advanced**.
- 2 Specify the data to retrieve from the LDAP server to resolve group names and relationships.

The default settings for these attributes are taken from the LDAP server type that you selected as your data source on the **Data source** page.



Attributes are entered as templates that let you extract and transform data from any number of LDAP attributes.

#### **GUID**

**GUID** is a unique identifier maintained by the LDAP server. Use this attribute if it is available on your server. Microsoft Active Directory supports GUID. Not all servers support it. If you omit this attribute, the Synchronization Tool derives an identifier from the distinguished name (DN) of the object class. The disadvantage of using a value that is derived from the DN is that if the user is renamed, the user entry is removed. It is then re-added instead of being modified in the portal. This means that any group associations that are configured are broken and must be re-established.

#### **Group Token**

**Group Token** is an optional attribute that holds a numeric identifier for a group. When the Synchronization Tool determines group membership, it matches the values of the Primary Group attribute of the user objects against the Group Token values of the Group objects. A match indicates that the user belongs to the group.

**Note:** The Group Token is specific to Active Directory so may be unavailable in other directories, for which it should be left blank.

#### **Group Parents**

**Group Parents** is an attribute that is used to relate a group to its parent group, if it exists. The optional attribute that is retrieved from the directory may consist of the DN of the parent group.

## Group Members

**Group Members** is a multiple-value attribute that holds the users (in DN form) who are part of this group.

**Note:** Group membership can be represented in the directory by use of either:

- **Group Members**  
A list of Users/Groups belonging to a Group
- **Group Membership**  
A list of Groups to which a Group/User belongs  
The Synchronization Tool allows either convention. For users to be correctly associated with groups one of these must be specified. The Group Membership attribute is labeled **Group Parents** for **Group** objects and both **Primary Group** and **Other Groups** for User Objects.

**Note:** Active Directory maintains membership lists on both Group and User objects. So the Group Members attribute of the group object class lists all the users for the group. The Other Groups and Primary Group attributes list all the groups to which the user belongs. In theory, these should be equivalent. In practice, when the directory is modified, some tools may update one list but not the other. Specifying both attributes causes the lists to be merged.

- 3 Click **Save** to save your changes, or **Next** to move to the next step in the Wizard.

For further information, click **Help > Contents** in the Synchronization Tool and see the LDAP Searches section.

## Select groups for an LDAP search

In the LDAP search step of the Configuration Wizard, you can specify the groups in your data source that you want to synchronize.

By default, all groups are synchronized.

**Table 3-6** Group selection settings

Setting	Description
<b>Available Groups</b>	<p>To exclude a group from synchronization, select the group in the <b>Available Groups</b> list, and click &gt; or &gt;&gt; to move it to the <b>Groups to exclude</b> list.</p> <p>The &gt; button moves the selected groups to the <b>Groups to exclude</b> list.</p> <p>The &gt;&gt; button moves the selected groups and all nested groups to the <b>Groups to exclude</b> list.</p> <p>To synchronize only the selected groups, select <b>include</b> from the top drop-down.</p> <p>To filter a group list, enter text in the field below the list. Only items with a prefix matching the text typed are shown in the list.</p>
<b>Excluded Group parents</b>	<p>The <b>Excluded Group parents</b> setting determines the action to take when a subset of available groups is selected. The setting enables some groups to be included, but one or more of the groups to which they belong can be excluded from the upload.</p> <p>The available options are:</p> <ul style="list-style-type: none"> <li>■ <b>Remove</b>—each group is uploaded with the excluded group removed from its <b>Member Of</b> list.</li> <li>■ <b>Replace with ancestors</b>—each group is uploaded with the excluded group removed from its <b>Member Of</b> list and replaced with the entries in the <b>Member Of</b> list of the excluded group. If any of these members are also excluded the process is repeated until only included groups remain in the uploaded group's <b>Member Of</b> list.</li> </ul>
<b>Filter Users</b>	<p>The <b>Filter Users</b> drop-down list enables you to exclude user records based on the group membership of the user.</p> <p>Select <b>Include only members of included groups</b> to exclude the user records that do not belong to any of the synchronized groups. This setting affects the Users synchronization. This option is useful if, on the User search page, users are found by searching the directory. In this mode the <b>Group Members</b> attribute of the Group record and both the <b>Primary Group</b> and <b>Other Groups</b> attributes of the User record are used to determine group membership. If the User synchronization configuration uses group membership to find users, only group members are found and this setting has no effect.</p>

# Configure an LDAP search for user synchronization

Configure the LDAP search to find users in your directory sources.. The Users search is independent of the Groups search; but the results of the Groups search are used to resolve group membership relationships. Searching for users can include users even if they are not listed as members in the Group records.

We recommend that you accept the default LDAP search settings for your user synchronization.

**To configure the LDAP search configuration settings for user synchronization**

- 1 In the **LDAP search** step of the Configuration Wizard, complete the following fields:

## Searching the directory

To exclude users who do not belong to any of the synchronized groups, as specified by the groups' **Group Members** attributes or by the users' **Primary Group** or **Other Groups** attributes, select **Include only members of included groups** on the **Group Selection** page in the Groups synchronization.

Enter the following information:

- **Search base**—Enter your search starting point in the LDAP server tree structure. Some LDAP servers do not allow the directory to be searched from the root. In this case, this field should not be left blank.  
**LDAP browser**—The drop-down list below the **Search base** field lets you navigate through the LDAP directory. Select an entry from the list to set the search base. The list is re-populated with the entries at the selected level. The first item in the list moves up one level.  
**Note:** When you browse up to a higher level in the directory, it is possible to select a node that cannot be searched. In this case, delete the content of the **Search base** field to browse the available naming contexts.
- **Search scope**—provides three options for selecting the depth of the search:
  - **Object**—searches for a single object that is in the location that is specified as the search base
  - **One level**—searches for all objects at the level that is specified in the **Search base** field;
  - **Sub-tree**—searches from the level that is specified in the **Search base** downwards, until the LDAP server restricts the results or the search or reaches the bottom of the tree. Use this option to return the most results.
- **Search filter**—Defines the type of object to return data on. You can select from a list of common filters by clicking in the Search filter field and then clicking **Examples**. A search filter can be typed directly into the Search filter field or can be entered using the LDAP filter editor. To use the LDAP filter editor, click the button to the right of the **Search filter** field.
- **Name**—Defines a rule for constructing a textual name that is used to represent individual users. An attribute template is used to construct the user's name.

For further information, click **Help > Contents** in the Synchronization Tool and review the Advanced topics section on LDAP Attribute Templates.

### **Group membership**

For Group membership, a list of users is obtained from the Group members attributes from the group records. For each user found, the directory must be accessed to obtain the user's details. The Group membership search can be less efficient than performing a single search.

Users who are not listed in the groups' Group members attributes are not included as members. This is the case even if they have been associated with the group by the user's **Primary Group** or **Other Groups** attribute.

If the **Include members of nested groups** check box is selected, the Synchronization Tool uses all groups that are selected on the Groups synchronization configuration and all nested groups within them when it searches for users. By including members of nested groups, you can select a small number of top-level groups from the Group selection page of the Groups synchronization.

If the **Include members of nested groups** check box is unselected, the members of nested groups are ignored.

Enter the following information:

- **Search depth**—gives the maximum nesting depth to use when you search within nested groups.
- **Search base**—not required to find Users by group membership
- **Search scope**—not required to find Users by group membership
- **Search filter**—if the Search filter is not specified, all items that are found in the Group members attribute are used. Otherwise, the filter is applied as for the directory search. The search filter may be useful to return only enabled users. Or if the group contains a mixture of users and nested groups, use the search filter to exclude group records.

- 2 Click **Save** to save your changes, or **Next** to move to the next step in the Wizard.

### **To configure the advanced user search attributes**

- 1 In the **LDAP search** step of the Configuration Wizard, click **Advanced**.
- 2 Specify the data to retrieve from the LDAP server to resolve user names and group ownership.

The default settings for these attributes are taken from the LDAP server type you selected as your data source on the **Data source** page. Attributes are entered as templates and let you extract and transform data from any number of LDAP attributes.

The attributes that are relevant for user synchronization are as follow:

<b>Primary Mail</b>	This attribute retrieves a user's email address.
<b>Mail Aliases</b>	Contains any aliases that are set up for a user. To view and select from a list of mail attribute examples, click in the <b>Mail Aliases</b> field and then click <b>Examples</b> .
<b>Primary Group</b>	The <b>Primary Group</b> is the token number attributed to a user. If the <b>Primary Group</b> matches a group's Group Token value, it places this user in that group. This attribute should be considered as an extension to the Other Groups attribute for placing a user in a particular group. Not all LDAP directories offer support for it.
<b>Other Groups</b>	<p>Contains the attribute name that describes the group or groups this user belongs to. For Active Directories this attribute is symmetrical to the <b>Group Parent</b> attribute for the group object class that points from each group to its users. If you omit this attribute, or your directory does not support this feature, the application searches for each user in the entire list of groups.</p> <p><b>Note:</b> For users to be correctly associated with groups, one of the following must be true:</p> <ul style="list-style-type: none"> <li>■ The Group Parent attribute exists, and the user GUID and group GUID attributes do not.</li> <li>■ The Group Members attribute exists. GUID is a unique identifier assigned to each user in a similar manner to the GUID attribute for groups.</li> </ul>
<b>GUID</b>	The GUID a unique identifier that is assigned to each user in a similar manner to the GUID attribute for groups. If the GUID is omitted, the Synchronization Tool creates a suitable value from the object's Distinguished Name.
<b>ML-IMServices</b>	<b>ML-IMServices</b> contains the attribute name from which to retrieve IM account details. This attribute is only required if you use Instant Messaging Security Services.

- 3 For further information, click **Help > Contents** in the Synchronization Tool and review the Advanced topics section.

See [“Create a configuration profile - process overview”](#) on page 25.

# Test the results of an LDAP search

After configuring the LDAP search options, click **Next** to move to the **Test** stage. The Synchronization Tool retrieves a small number of search results that enable you to decide whether your search has returned the data that you expect.

Mail synchronization	No detailed option is available for mail addresses.
Groups synchronization	<p>For groups, each line contains:</p> <ul style="list-style-type: none"> <li>■ The result from the name template, after it is changed using any template rule.</li> <li>■ The GUID. If you have not provided a <b>Group GUID attribute</b>, the GUID is derived from the DN.</li> <li>■ The Group Token that is retrieved using the <b>Group Token attribute</b>.</li> <li>■ The DN automatically retrieved by the Synchronization Tool.</li> <li>■ The number of parents that this group belongs to (normally 0 or 1) and the DN of the first of these groups. These results are retrieved using the <b>Group Parents attribute</b>.</li> <li>■ The number of users in this group and the DN of the first of these users. These results are retrieved using the <b>Group Members attribute</b>.</li> </ul>
Users synchronization	<p>For users, each line contains:</p> <ul style="list-style-type: none"> <li>■ The result from the name template, after it is changed using any template rule.</li> <li>■ The GUID. If you have not provided a <b>User GUID attribute</b> the GUID is derived from the DN.</li> <li>■ The email address that is retrieved using the <b>Primary Mail attribute</b>.</li> <li>■ The Primary Group that is retrieved using the <b>Primary Group attribute</b>.</li> <li>■ The Groups that are retrieved using the <b>Other Groups attribute</b>.</li> <li>■ The DN automatically retrieved by the Synchronization Tool.</li> <li>■ The <b>Other</b> consists of <b>Mail Aliases</b> and <b>ML IM Services</b> attribute.</li> </ul> <p><b>Note:</b> For both groups and users, if the Name, the GUID, or the DN is blank, correct the attribute names before commencing.</p>

If you see no results, check that:

- The **Source Type** that you selected in the **Data Source** step of the Configuration Wizard is correct.
- The **Search scope** in the **LDAP search** step is set to **Sub-tree**.



- The **Search base** in the **LDAP search** step is set to a suitable level in your LDAP server's hierarchy to find the required mail addresses or groups and users.
- The location that is specified in the **Search base** field in the LDAP search step exists in the LDAP server directory. If in doubt, return to the top of the LDAP server tree and navigate to the location you want.
- You have not changed the **Search filter** field. Click **Defaults** to reset this field setting.
- Your authentication settings are sufficient to return details from the LDAP server. If you select **anonymous** from the **Authentication** drop-down list and no results are returned, select **simple** and enter a user name and password.
- For users and groups, the search results display the names that are constructed from the **Name** field. Check that these are representative names. For example, for users in a Microsoft environment, the names should represent the "domain\username" identity of individual users.

## Configure an Exchange Online data source

When you select the Exchange Online data source for a configuration profile, you provide the account details that enable the Synchronization Tool to retrieve mail, group and user data from the source.

### To configure an Exchange Online data source

- 1 In the **Exchange Online** step of the Configuration Wizard, review the following fields:

<b>Custom account details for the synchronization</b>	Select the <b>Custom account details for the synchronization</b> check box to enter alternative connection details to the standard settings that you have provided in the <b>Exchange Online</b> panel ( <b>Edit &gt; Settings</b> ).
<b>User name</b>	The <b>User name</b> defaults from the details you provide in the <b>Exchange Online</b> panel ( <b>Edit &gt; Settings</b> ). To add custom settings, select the <b>Custom account details for the synchronization</b> check box.
<b>Password</b>	The <b>Password</b> defaults from the details you provide in the <b>Exchange Online</b> panel ( <b>Edit &gt; Settings</b> ). To add custom settings, select the <b>Custom account details for the synchronization</b> check box.

- 2 Click **Next** to move to the next step in the Wizard or **Save** to save your changes.

# Configure an Exchange Online search for mail synchronization

When you select the **Exchange Online** data source for mail synchronization, the next step in the Configuration Wizard is to configure the search to return the attributes that you require.

## To configure the Exchange Online search configuration settings for mail synchronization

- 1 In the **Exchange Online search configuration** step of the Configuration Wizard, select from the following data types:

<b>Users</b>	Calls the cmdlet "get-user" to retrieve attributes.
<b>Contacts</b>	Calls the cmdlet "get-contact" to retrieve attributes.
<b>Groups</b>	Calls the cmdlet "get-group" to retrieve attributes.
<b>Recipients</b>	Calls the cmdlet "get-recipient" to retrieve attributes.
- 2 For details of the attributes that the "get-user", "get-contact" and "get-group" and "get-recipient" cmdlets retrieve, see the Microsoft documentation for the Windows Azure Active Directory Module for Windows PowerShell
- 3 Click **Save** to save your changes, or **Next** to move to the next step in the Wizard.

### To configure the advanced mail search attributes

- 1 In the **Exchange Online search configuration** step of the Configuration Wizard, click **Advanced**.
- 2 Review the following settings:

<b>Primary Mail</b>	<p>The <b>Primary Mail</b> is the attribute returned by Exchange Online that contains the email address. Although users may only have a single primary email address this can be returned in either the PrimarySMTPAddress (which is mapped internally to the "mail" attribute) or EmailAddresses attribute. If this results in multiple email addresses then all unique values are returned.</p> <p>The percent (%) symbols indicate that the text should be interpreted as an attribute name whose value is returned. The curly brackets contain a regular expression to modify the value returned in the attribute.</p>
<b>Mail Aliases</b>	<p>This attribute is a list of optional alternatives to the <b>Primary Mail</b> attributes. To view and select from a list of mail attribute examples, click in the <b>Mail Aliases</b> field and click <b>Examples</b>.</p>

- 3 Click **Save** to save your changes, or **Next** to move to the next step in the Wizard.

## Configure an Exchange Online search for group synchronization

When you select the **Exchange Online** data source for group synchronization, the next step in the Configuration Wizard is to configure the search to return the attributes that you require.

### To configure the Exchange Online search configuration settings for group synchronization

- 1 In the **Exchange Online search configuration** step of the Configuration Wizard, review the following settings:

<b>Groups</b>	Calls the cmdlet "get-group" to retrieve the attributes.
<b>Name</b>	The <b>Name</b> field is a template that is used to construct the group names for synchronization.

- 2 Click **Save** to save your changes, or **Next** to move to the next step in the Wizard.

### To configure the advanced group search attributes

- 1 In the **Exchange Online search configuration** step of the Configuration Wizard, click **Advanced**.
- 2 Review the following setting:

#### **GUID**

The **GUID** (global unique identifier) is an attribute that exclusively identifies the group name from the Search screen.

The GUID is used to track changes as the attributes that are connected to the GUID are sent as modifications. If a GUID is changed, the change is seen as a deletion of all the attributes that are associated with the previous GUID followed by an addition of the new attributes.

If your configuration consists of both an Active Directory source and an Office 365 source and the same group names appear on both sources then the GUID should be set to an attribute for correlating these changes, such as %Identity%. Choose an attribute that is unique for each source but identifies an entry as a duplicate between the two sources.

- 3 Click **Save** to save your changes, or **Next** to move to the next step in the Wizard.

## Configure an Exchange Online search for user synchronization

When you select the **Exchange Online** data source for user synchronization, the next step in the Configuration Wizard is to configure the search to return the attributes that you require.

### To configure the Exchange Online search configuration settings for user synchronization

- 1 In the **Exchange Online search configuration** step of the Configuration Wizard, review the following settings:

- |                             |  |
|-----------------------------|--|
| <b>User Selection</b>       | <p>Choose from the following options:</p> <ul style="list-style-type: none"><li>■ <b>Keep all users</b><br/>All users that are found from using the cmdlets selected in the <b>Search Configuration</b> are retained.</li><li>■ <b>Keep immediate members</b><br/>Only users that are in one or more groups are retained. Any orphaned users are excluded. Note that it is possible to orphan a user by excluding all groups that it appears in as part of the Groups configuration. When the user appears inside a hierarchical structure of groups it is considered to be orphaned if its immediate parent does not exist.</li><li>■ <b>Keep nested members</b><br/>Only users that are in one or more groups are retained. Any orphaned users are excluded. Note that it is possible to orphan a user by excluding all groups that it appears in as part of the Groups configuration. When the user appears inside a hierarchical structure of groups it is considered to be orphaned only if all of the groups in the structure have been excluded</li></ul> |
| <b>Search Configuration</b> | <p>Select the required data type and click <b>Filter</b> to restrict the attributes that you want to return.</p> <p>See <a href="#">“Apply filters to an Exchange Online search configuration”</a> on page 55.</p>   |
| <b>Name</b>                 | The attribute containing the user's login name for use on the portal.  |
| <b>Display Name</b>         | The display name that is presented to the user after they have logged in to the portal.  |
- 2 Click **Save** to save your changes, or **Next** to move to the next step in the Wizard.

### To configure the advanced user search attributes

- 1 In the **Exchange Online search configuration** step of the Configuration Wizard, click **Advanced**.

<b>Primary Mail</b>	An attribute containing the preferred email address.
<b>Mail Aliases</b>	A list of alternative emails returned in EmailAddresses
<b>Group Member ID</b>	The value that links the user to its parent group.
<b>GUID</b>	The Synchronization Tool uses this attribute to track changes. A change of GUID results in the associated user details being deleted and re-added. If your configuration consists of both an Active Directory source and an Exchange Online source and the same user names appear on both sources then set the GUID to an attribute for correlating these changes, such as %Identity% or %mail%

- 2 Click **Save** to save your changes, or **Next** to move to the next step in the Wizard.

## Test the results of an Exchange Online search

After configuring the Exchange Online search options,. The Synchronization Tool retrieves a small number of search results that enable you to decide whether your search has returned the data that you expect. Review the results for mail, group and user synchronization, as follows:

Mail	The search results display the email addresses that match your search.
------	--

## Groups

If the **Show detail** check box is selected, the search results display the group names, the unique identifiers and the members that appear within the group.

If the **Name**, **DN**, or **Members** columns are blank, correct the attribute names in the **Office 365 Search** dialog before you continue.

Click **Next** to move to the **Group Selection** dialog.

Each group that Exchange Online discovers appears in the **Available Groups** list. The drop-down to "Include" or "Exclude" groups acts on those groups that have been added to the right-hand list.

The ">" button moves all the selected group names into the right-hand list. The "<" button moves groups in the right-hand list back to the **Available Groups** list. The ">>" button moves groups and any child groups to the right-hand list. The "<<" button moves groups and any child groups back to **Available Groups**.

To synchronize all groups, ensure that the right-hand list is empty and set the drop-down list to "Exclude" groups.

The **Excluded Group parents** drop-down determines the behavior when only part of a hierarchy of groups have been included. Set to **Remove** to treat a group whose parent is not included as an isolated group. Set to **Replace with ancestors** to place the group in any ancestor that has been included.

## Users

If the **Show detail** check box is selected, the search results display the user names, the unique identifiers and the members for the users.

# Apply filters to an Exchange Online search configuration

You can apply filters to an Exchange Online mail, group, and user search configuration. The filters let you restrict the data that is returned by the Exchange Online search.

### To apply filters to an Exchange Online search configuration

- 1 In the **Exchange Online search configuration** dialog click **Filters**.
- 2 The screen displays the parameters that are relevant to the search configuration that you have specified. Review the following settings:

#### **Filter**

By default all entries are returned.

Select the **Filter** check box to pass the contents of the text field to the "get-recipient" PowerShell command parameter "-Filter".

Specify an OPATH filter to restrict the information that the search of the directory server returns. In Exchange Server 2010 and Exchange Server 2007, the OPATH filtering syntax replaces the LDAP filtering syntax. For further details, see the documentation from Microsoft.

You can add further filters to the data that you make available to the cloud security services in the **Filters** step of the Configuration Wizard.

#### **RecipientType**

By default all recipient types are returned. This filter lets you restrict the recipient types to results based on that setting.

#### **RecipientTypeDetails**

By default users with all recipient types are returned.

- 3 Click **OK** to return to the **Exchange Online search configuration** dialog.

## Configure an Azure data source

When you select the Azure data source for a configuration profile, you provide the account details that enable the Synchronization Tool to retrieve mail, group, and user data from the source.



### To configure an Azure data source

- 1 In the **Azure** step of the Configuration Wizard, review the following fields:

#### Custom account details for the synchronization

Select the **Custom account details for the synchronization** check box to enter alternative connection details to those that you have already provided in the **Azure** panel. (**Edit > Settings**).

#### Tenant Context ID

The **Tenant Context ID** defaults from the details you provided in the **Azure** panel (**Edit > Settings**). To add custom settings, select the **Custom account details for the synchronization** check box.

#### Principal ID

The **Principal ID** defaults from the details you provide in the **Azure** panel (**Edit > Settings**). To add custom settings, select the **Custom account details for the synchronization** check box.

#### Symmetric Key

The **Symmetric Key** defaults from the details you provide in the **Azure** panel (**Edit > Settings**). To add custom settings, select the **Custom account details for the synchronization** check box.

- 2 Click **Advanced** to display the Query Configuration settings, which are used to control how data is returned by Azure. The **Full with paging** setting requests the data in blocks. The size of each block is entered in the **Page Size** field. The **Full without paging** setting requests the entire data set in one block. The **Differential** setting requests the changes in the data set since the last download. Differential data is always returned in one block.
- 3 Click **Next** to move to the next step in the Wizard or **Save** to save your changes.

See [“Configure an Azure search for mail synchronization”](#) on page 57.

## Configure an Azure search for mail synchronization

When you select the **Azure** data source for mail synchronization, the next step in the Configuration Wizard is to configure the search to return the attributes that you require.

**To configure the Azure search configuration settings for mail synchronization**

- 1 In the **Azure search configuration** step of the Configuration Wizard, select from the following data types:

**Users**

The filter for **Users** is sent to the Azure server to retrieve a subset of attributes from the overall data set.

**Groups**

The filter for **Groups** is sent to the Azure server to retrieve a subset of attributes from the overall data set.

**Contacts**

The filter for **Contacts** is sent to the Azure server to retrieve a subset of attributes from the overall data set.

The Users, Groups, and Contacts data types correspond to the different resources available on the Azure server. The **Filters** must be specified in Microsoft's ODATA syntax. The Azure server processes the filters to improve the efficiency of the operation and reduce the amount of data returned. Note that the **Resources** and **Filters** cannot be used with the **Differential Query Configuration**, which can be set when configuring the Azure data source. If differential queries are used, the Resources check boxes are disabled.

- 2 Click **Save** to save your changes, or **Next** to move to the next step in the Wizard.

### To configure the advanced mail search attributes

- 1 In the **Azure search configuration** step of the Configuration Wizard, click **Advanced**.
- 2 Review the following settings:

#### Primary Mail

**Primary Mail** is an attribute that contains the primary email address.

#### Mail Aliases

This attribute is a list of optional alternatives to the **Primary Mail** attributes. To view and select from a list of mail attribute examples, click in the **Mail Aliases** field and click **Examples**.

#### GUID

This attribute is a unique identifier that the Synchronization Tool uses to track whether or not an email address is a duplicate.

- 3 Click **Save** to save your changes, or **Next** to move to the next step in the Wizard.

See [“Configure an Azure data source”](#) on page 56.

## Configure an Azure search for group synchronization

When you select the **Azure** data source for group synchronization, the next step in the Configuration Wizard is to configure the search to return the attributes that you require.

### To configure the Azure search configuration settings for group synchronization

- 1 In the **Azure search configuration** step of the Configuration Wizard, review the following settings:

#### Groups

The filter for **Groups** is sent to the Azure server to retrieve a subset of attributes from the overall data set.

The Groups data type corresponds to the resource available on the Azure server. The **Filters** must be specified in Microsoft's ODATA syntax. The Azure server processes the filters to improve the efficiency of the operation and reduce the amount of data returned. Note that the **Resources** and **Filters** cannot be used with the **Differential Query Configuration**, which can be set when configuring the Azure data source. If differential queries are used, the Resources check boxes are disabled.

- 2 Click **Save** to save your changes, or **Next** to move to the next step in the Wizard.

### To configure the advanced group search attributes

- 1 In the **Azure search configuration** step of the Configuration Wizard, click **Advanced**.
- 2 Review the following setting:

#### Name

The **Name** field is a template that is used to construct the group names for synchronization.

#### GUID

The **GUID** (global unique identifier) is an attribute that exclusively identifies the group name from the Search screen.

- 3 Click **Save** to save your changes, or **Next** to move to the next step in the Wizard.

See [“Select groups for an Azure search”](#) on page 60.

## Select groups for an Azure search

In the Azure search step of the Configuration Wizard, you can specify the groups in your data source that you want to synchronize.

By default, all groups are synchronized.

Table 3-7 Group selection settings

Setting	Description
Available Groups	<p>To exclude a group from synchronization, select the group in the <b>Available Groups</b> list, and click &gt; or &gt;&gt; to move it to the <b>Groups to exclude</b> list.</p> <p>The &gt; button moves the selected groups to the <b>Groups to exclude</b> list.</p> <p>The &gt;&gt; button moves the selected groups and all nested groups to the <b>Groups to exclude</b> list.</p> <p>To synchronize only the selected groups, select <b>include</b> from the top drop-down.</p> <p>To filter a group list, enter text in the field below the list. Only items with a prefix matching the text typed are shown in the list.</p>
Excluded Group parents	<p>The <b>Excluded Group parents</b> setting determines the action to take when a subset of available groups is selected. The setting enables some groups to be included, but one or more of the groups to which they belong can be excluded from the upload.</p> <p>The available options are:</p> <ul style="list-style-type: none"><li>■ <b>Remove</b>—each group is uploaded with the excluded group removed from its <b>Member Of</b> list.</li><li>■ <b>Replace with ancestors</b>—each group is uploaded with the excluded group removed from its <b>Member Of</b> list and replaced with the entries in the <b>Member Of</b> list of the excluded group. If any of these members are also excluded the process is repeated until only included groups remain in the uploaded group's <b>Member Of</b> list.</li></ul>

# Configure an Azure search for user synchronization

When you select the **Azure** data source for user synchronization, the next step in the Configuration Wizard is to configure the search to return the attributes that you require.

To configure the Azure search configuration settings for user synchronization

- 1 In the **Azure search configuration** step of the Configuration Wizard, review the following settings:

## User Selection

Choose from the following options:

- **Keep all users**  
 All users that are found from the use of **Search Configuration** are retained.
- **Keep immediate members**  
 Only users that are in one or more groups are retained. Any orphaned users are excluded. Note that it is possible to orphan a user by excluding all groups that it appears in as part of the Groups configuration. When the user appears inside a hierarchical structure of groups it is considered to be orphaned if its immediate parent does not exist.
- **Keep nested members**  
 Only users that are in one or more groups are retained. Any orphaned users are excluded. Note that it is possible to orphan a user by excluding all groups that it appears in as part of the Groups configuration. When the user appears inside a hierarchical structure of groups it is considered to be orphaned only if all of the groups in the structure have been excluded.

## Search Configuration

The Users and Contacts data types correspond to the different resources available on the Azure server. The **Filters** must be specified in Microsoft's ODATA syntax. The Azure server processes the filters to improve the efficiency of the operation and reduce the amount of data returned. Note that the **Resources** and **Filters** cannot be used with the **Differential Query Configuration**, which can be set when configuring the Azure data source. If differential queries are used, the Resources check boxes are disabled.

- 2 Click **Save** to save your changes, or **Next** to move to the next step in the Wizard.

### To configure the advanced user search attributes

- 1 In the **Azure search configuration** step of the Configuration Wizard, click **Advanced**.

<b>Name</b>	The attribute containing the user's login name for use on the portal.
<b>Display Name</b>	The human-readable display name that is presented to the user after they have logged in to the portal.
<b>Primary Mail</b>	<b>Primary Mail</b> is an attribute that contains the primary email address.
<b>Mail Aliases</b>	<b>Mail Aliases</b> are any alternative email addresses or aliases.
<b>GUID</b>	The <b>GUID</b> (global unique identifier) is an attribute that exclusively identifies the user name.

- 2 Click **Save** to save your changes, or **Next** to move to the next step in the Wizard.

## Test the results of an Azure search

After configuring the Azure search options, click **Next** to move to the **Test** stage. The Synchronization Tool retrieves a small number of search results that enable you to decide whether your search has returned the data that you expect.

<b>Mail</b>	The search results display the email addresses that match your search.
<b>Groups</b>	If the <b>Show detail</b> check box is selected, the search results display the group names, unique identifiers, and the members that appear within the group and any parent groups.
<b>Users</b>	If the <b>Show detail</b> check box is selected, the search results display the user names, unique identifiers, and the members that appear within the users data source.

## Configure an Office 365 data source

When you select the Office 365 data source for a configuration profile, you provide the account details that enable the Synchronization Tool to retrieve mail, group and user data from the source.

### To configure an Office 365 data source

- 1 In the **Office 365** step of the Configuration Wizard, review the following fields:

<b>Custom account details for the synchronization</b>	Select the <b>Custom account details for the synchronization</b> check box to enter alternative connection details to those that you have provided in the <b>Exchange Online</b> panel ( <b>Edit &gt; Settings</b> ).
<b>User name</b>	The <b>User name</b> defaults from the details you provide in the <b>Exchange Online</b> panel ( <b>Edit &gt; Settings</b> ). To add custom settings, select the <b>Custom account details for the synchronization</b> check box.
<b>Password</b>	The <b>Password</b> defaults from the details you provide in the <b>Exchange Online</b> panel ( <b>Edit &gt; Settings</b> ). To add custom settings, select the <b>Custom account details for the synchronization</b> check box.

- 2 Click **Next** to move to the next step in the Wizard or **Save** to save your changes.

## Configure an Office 365 search for mail synchronization

When you select the **Office 365** data source for mail synchronization, the next step in the Configuration Wizard is to configure the search to return the attributes that you require.



## To configure the Office 365 search configuration settings for mail synchronization

- 1 In the **Office 365 search configuration** step of the Configuration Wizard, select from the following data types:

<b>Users</b>	Calls the cmdlet "get-msoluser" to retrieve attributes.
<b>Contacts</b>	Calls the cmdlet "get-msolcontact" to retrieve attributes.
<b>Groups</b>	Calls the cmdlet "get-msolgroup" to retrieve attributes.

For details of the attributes that the "get-msoluser", "get-msolcontact" and "get-mseolgroup" cmdlets retrieve, see the Microsoft documentation for the Windows Azure Active Directory Module for Windows PowerShell.

- 2 Click **Save** to save your changes, or **Next** to move to the next step in the Wizard.

## To configure the advanced mail search attributes

- 1 In the **Office 365 search configuration** step of the Configuration Wizard, click **Advanced**.
- 2 Review the following settings:

<b>Primary Mail</b>	<p><b>Primary Mail</b> is a list of attributes containing the email addresses. Although users may only have a single primary email address, the address can be returned in either the EmailAddress or ProxyAddresses attributes. Where there are multiple email addresses, all unique values are returned.</p> <p>The percent (%) symbols indicate that the text should be interpreted as an attribute name whose value is returned. The curly brackets contain a regular expression to modify the value that is returned in the attribute.</p>
<b>Mail Aliases</b>	<p>This attribute is a list of optional alternatives to the <b>Primary Mail</b> attributes. To view and select from a list of mail attribute examples, click in the <b>Mail Aliases</b> field and click <b>Examples</b>.</p>

- 3 Click **Save** to save your changes, or **Next** to move to the next step in the Wizard.

# Configure an Office 365 search for group synchronization

When you select the **Office 365** data source for group synchronization, the next step in the Configuration Wizard is to configure the search to return the attributes that you require

## To configure the Office 365 search configuration settings for group synchronization

- 1 In the **Office 365 search configuration** step of the Configuration Wizard, review the following settings:

<b>Groups</b>	Calls the cmdlet "get-msolgroup" to retrieve the attributes.
<b>Name</b>	The <b>Name</b> field is a template that is used to construct the group names for synchronization.

- 2 Click **Save** to save your changes, or **Next** to move to the next step in the Wizard.

## To configure the advanced group search attributes

- 1 In the **Office 365 search configuration** step of the Configuration Wizard, click **Advanced**.
- 2 Review the following setting:

<b>GUID</b>	<p>The <b>GUID</b> (global unique identifier) is an attribute that exclusively identifies the group name from the Search screen.</p> <p>The GUID is used to track changes as the attributes that are connected to the GUID are sent as modifications. If a GUID is changed, the change is seen as a deletion of all the attributes that are associated with the previous GUID followed by an addition of the new attributes.</p> <p>If your configuration consists of both an Active Directory source and an Office 365 source and the same group names appear on both sources then the GUID should be set to an attribute for correlating these changes, such as %Identity%. Choose an attribute that is unique for each source but identifies an entry as a duplicate between the two sources.</p>
-------------	--

- 3 Click **Save** to save your changes, or **Next** to move to the next step in the Wizard.

# Configure an Office 365 search for user synchronization

When you select the **Office 365** data source for user synchronization, the next step in the Configuration Wizard is to configure the search to return the attributes that you require.

To configure the Office 365 search configuration settings for user synchronization

- 1 In the **Office 365 search configuration** step of the Configuration Wizard, review the following settings:

<b>User Selection</b>	Choose from the following options: <ul style="list-style-type: none"><li>■ <b>Keep all users</b> All users that are found from using the cmdlets selected in the <b>Search Configuration</b> are retained.</li><li>■ <b>Keep immediate members</b> Only users that are in one or more groups are retained. Any orphaned users are excluded. Note that it is possible to orphan a user by excluding all groups that it appears in as part of the Groups configuration. When the user appears inside a hierarchical structure of groups it is considered to be orphaned if its immediate parent does not exist.</li><li>■ <b>Keep nested members</b> Only users that are in one or more groups are retained. Any orphaned users are excluded. Note that it is possible to orphan a user by excluding all groups that it appears in as part of the Groups configuration. When the user appears inside a hierarchical structure of groups it is considered to be orphaned only if all of the groups in the structure have been excluded.</li></ul>
<b>Search Configuration</b>	Select the required data type and click <b>Filter</b> to restrict the attributes that you want to return.  See <a href="#">“Apply filters to an Office 365 search configuration”</a> on page 69.
<b>Name</b>	The attribute containing the user's login name for use on the portal.
<b>Display Name</b>	The display name that is presented to the user after they have logged in to the portal.

- 2 Click **Save** to save your changes, or **Next** to move to the next step in the Wizard.

## To configure the advanced user search attributes

- 1 In the **Office 365 search configuration** step of the Configuration Wizard, click **Advanced**.

<b>Primary Mail</b>	<b>Primary Mail</b> is a list of attributes containing the e-mail addresses. Although users may only have a single primary email address, this can be returned in either the EmailAddress or ProxyAddresses attribute. If this results in multiple email addresses, then all unique values are returned. The percent (%) symbols indicate that the text should be interpreted as an attribute name whose value is returned. The curly brackets contain a regular expression to modify the value returned in the attribute. Refer to Appendix A for full details of regular expression syntax
<b>GUID</b>	<b>GUID</b> is the attribute used by the Synchronization Tool to track changes. A change of GUID will result in the associated user details being deleted and re-added. If your configuration consists of both an Active Directory source and an Office 365 source and the same user names appear on both sources then the GUID should be set to an attribute for correlating these changes, such as %EmailAddress%.

- 2 Click **Save** to save your changes, or **Next** to move to the next step in the Wizard.

## Test the results of an Office 365 search

After you configure the Office 365 search options, click **Next** to move to the **Test** stage. The Synchronization Tool retrieves a small number of search results that enable you to decide whether your search has returned the data that you expect.

Mail	The search results display the email addresses that match your search.
Groups	<p>If the <b>Show detail</b> check box is selected, the search results display the group names, the unique identifiers and the members that appear within the group.</p> <p>If the <b>Name</b>, <b>DN</b>, or <b>Members</b> columns are blank , correct the attribute names in the <b>Office 365 Search</b> dialog before you continue.</p>
Users	If the <b>Show detail</b> check box is selected, the search results display the user names, the unique identifiers and the members that appear within the users.

# Apply filters to an Office 365 search configuration

You can apply filters to an Office 365 mail, group, and user search configuration. The filters let you restrict the data that is returned by the Office 365 search.

## To apply filters to an Office 365 search configuration

- 1 In the **Office 365 search configuration** dialog click **Filters**.
- 2 The screen displays the parameters that are relevant to the search configuration that you have specified. Review the following settings:

### SearchString

By default all entries are returned.

Select the **SearchString** check box to pass the contents of the text field to the "get-msolgroup" PowerShell command parameter "-SearchString".

Specify a **Search String** filter to restrict the results to entries that start with the string. No wildcards are permitted.

### EnabledFilter

By default, entries are returned whether they are enabled or not. This filter lets you restrict them to results based on that setting.

### GroupType

**GroupType** is the command line option "-GroupMemberType" and by default, all group member types are returned. This filter restricts the types that are returned to those check boxes selected as "Security", "Mail Enabled Security" or "Distribution List". The Microsoft Office 365 portal only shows "Mail Enabled Security" groups in the administrative view.

- 3 Click **OK** to return to the **Office 365 search configuration** dialog.

See ["Create a configuration profile - process overview"](#) on page 25.

# Configure the data repository

The data repository is the destination for your email, group, and user data, after the Synchronization Tool has extracted it from your directory sources.

## To configure the data repository

- 1 In the **Data repository** step of the Configuration Wizard, select from the following options for **Repository Type**:

**Symantec.cloud** Click **Next** to enter your portal user name and password details and synchronizes your email addresses with the addresses on the portal account. Your email addresses are transmitted to the cloud security services whenever you perform a synchronization.

The tool uses the user name and password settings that are defined in **Edit > Settings**. To override these default user name and password settings, check the **Custom account details for this synchronization** box, and enter the new details. If you cannot access the portal server directly due to a firewall, you may need to configure a proxy. If a proxy is configured, it is used for all communications with the cloud security services.

## File

Click **Next** to select the location of the data repository file. The synchronization process requires the following three files:

- A file to hold the list of current email addresses
- A file to hold additions since the last synchronization
- A file to hold deletions since the last synchronization

The file repository can be used for testing. The file holding the current list represents the state of the repository after the synchronization. The additions and the deletions files show what would be sent to the cloud security services to adjust the repository based on the source data.

**Note:** When you browse to a file, the **Additions** and **Deletions** fields are automatically completed with file names that are based on your file selection. For example, for a mail synchronization, if your file is called *test-mail.txt*, the additions file is called *test-mail-additions.txt*, and the deletions file is called *test-mail-deletions.txt*.

From the **File Format** drop-down list, select one of the following:

- **Escaped CSV**  
 Creates a file in Comma-Separated Variable (CSV) format.  
 The file is in text format, with one email address per line.
- **LDIF**  
 Creates a file in the LDAP Data Interchange Format (LDIF).  
 Each directory entry is represented as a record, including the `dn` and `objectClass` attributes.

Both formats are suitable to use as a File source. The escaped CSV format guarantees that each record is on a separate line. The LDIF format may be more convenient if complicated records are to be edited by hand. The CSV is the most convenient format for mail records.

**Note:** The contents of the files represent the data that is sent to the repository, after LDAP templates and filters have been applied. For example, selecting **LDIF** does not generate an LDIF dump of the directory.

- 2 Click **Save** to save the changes to the profile, or click **Next** to move to the next step in the Wizard.

See [“About configuration profiles”](#) on page 24.

# Add limits to a configuration profile

Threshold limits warn you when the number of added or deleted entries exceeds a specified amount. Threshold limits help to protect you from mistakes in your configuration profile, especially if you use filters to exclude or modify data from the data repository.

When you run the Synchronization Tool interactively, and the limit that you have established is exceeded, a 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**, as required.*

When you schedule a synchronization run, and the limit you have established is exceeded, the synchronization is not performed. If you have included an email notification in the profile, you are notified that synchronization has not occurred.

## To add limits to a configuration profile

- 1 In the **Limits** step of the Configuration Wizard, select the check box next to one of the following options:

<b>Maximum added entries</b>	This setting determines the largest number of entries from your data source that can be added. If this number is exceeded, the synchronization does not proceed.
<b>Maximum deleted entries</b>	This setting determines the largest number of entries from your data source that can be deleted. If this number is exceeded the synchronization does not proceed. A percentage greater than 100% is treated as 100%
<b>Maximum changed entries</b>	<p>This setting determines the largest number of entires from your data source that can be modified. If this number is exceeded the synchronization does not proceed.</p> <p><b>Note:</b> This setting is not relevant to the synchronization of email addresses.</p>
<b>Minimum replacement entries</b>	This setting is for an action that causes the entire contents of the repository to be overwritten. It determines the number of entries that have changed for a complete replacement to be allowed. If fewer entries are found in the data source, the synchronization does not proceed.

- 2 Enter a threshold limit, as a number or a percentage. For a percentage, add the percent symbol (%) to the number.
- 3 Click **Save** to save the changes to the profile, or click **Next** to move to the next step in the Wizard.



# Use filters in a configuration profile

Use filters to make changes to the data that the Synchronization Tool extracts from your directory sources. The changes are made before the tool extracts the email, group, and user data to the cloud security services.

The **Filters** section is one of the steps in the Configuration Wizard. You can establish filters when you create a configuration. You can also add filters to an existing configuration. For the Office 365 and Exchange Online data sources, you can filter the results of a search at the **Search** step of the Configuration Wizard.

---

**Note:** The Synchronization Tool requires all filters to be of the same type for a configuration (wildcards, regular expressions, or literal text). If you have previously used wildcard filters and you need to convert them to regular expressions replace '\*' with '(.\*)' and ? with . in the pattern, and '\*' with '\$1' in the replacement string.

---

## To exclude items in your data source

- 1 In the **Filters** step of the Configuration Wizard, do one of the following:
  - Type a text string into the **Pattern** field. Do not include any text in the **Replacement** field. You can include multiple pattern entries, each on separate line.
  - Click the folder icon in front of the **Pattern** field and locate a file that includes the patterns that you want to exclude. Ensure that each pattern is on a separate line in the file.
- 2 Choose one of the following options from the drop-down list:
  - **Regular expressions**—use regular expressions for complex pattern matching and replacement.  
For further information, click **Help > Contents** in the Synchronization Tool and review the Advanced topics section.
  - **Wildcards**—

Asterisk (*)	Use an asterisk (*) to match one or more characters. For example, <i>*y@acme.com</i> matches the email address <i>andy@acme.com</i> but not the address <i>john@acme.com</i> .
--------------	--

Question mark (?)	Use a question mark (?) to match a single character. For example, <i>?andy@acme.com</i> matches the email address <i>mandy@acme.com</i> and <i>sandy@acme.com</i> but not <i>andy@acme.com</i>
-------------------	--

- **Literal text**—use this option to match the precise text in the filters list.

The tool checks each entry in the data source file or LDAP server against the patterns that you have included. The entries that match a pattern are not included in the target data repository.

- 3 Click **Save** to save the changes to the profile, or click **Next** to move to the next step in the Wizard.

#### To modify items in your data source

- 1 In the Filters step of the Configuration Wizard, do one of the following:
  - Type a text string into the **Pattern** field and include the text that you want to replace it with in the **Replacement** field. You can include multiple pattern entries, each on separate line.
  - Click the folder icon in front of the **Pattern** field and locate a file that includes the patterns that you want to modify. Ensure that each pattern is on a separate line in the file. In the **Replacement** field, add the replacement text for each entry in the file. For each text file, which may include multiple patterns, enter a single replacement string.
- 2 Choose one of the following options from the drop-down list:
  - **Regular expressions**—use regular expressions for complex pattern matching and replacement. For further information, click **Help > Contents** in the Synchronization Tool and review the Advanced topics section.
  - **Wildcards**—

Asterisk (*)	Use an asterisk (*) to match one or more characters. For example, <i>*y@acme.com</i> matches the email address <i>andy@acme.com</i> but not the address <i>john@acme.com</i> .
--------------	--

Question mark (?)	Use a question mark (?) to match a single character. For example, <i>?andy@acme.com</i> matches the email address <i>mandy@acme.com</i> and <i>sandy@acme.com</i> but not <i>andy@acme.com</i>
-------------------	--

- **Literal text**—use this option to match the precise text in the filters list.

The tool checks each entry in the data source file or LDAP server against the patterns and applies the replacements that you have specified.

- 3 Click **Save** to save the changes to the profile, or click **Next** to move to the next step in the Wizard.

# Include email notifications in a configuration profile

A notification is an email that is automatically sent when you use a configuration profile to synchronize your data with the cloud security services.

You specify the recipients of the email notification and the information that the email contains. If you schedule the Tool to run at a specific time, we recommend that you include an email notification in the configuration profile.

## To include an email notification in a configuration profile

- 1 In the Configuration Wizard, select **Notification** from the left-hand menu.
- 2 In the **Email notifications** drop-down, select the information that you want to see in the email. The options are:
  - **None**
  - **Summary**
  - **Summary + Log (WARNING)**
  - **Summary + Log (INFO)**
  - **Summary + Log (FINE)**
- 3 Complete the **SMTP Settings** section. The options are:
  - **Mail Server**—enter the host name of the server to use to deliver the email, for example `smtp.acme.com`
  - **on Success**—enter the text that appears in the Subject field of the email for successful synchronizations.
  - **on Failure**—enter the text that appears in the Subject field of the email for unsuccessful synchronizations.
  - **From**—enter the originating address for the email notification
  - **To, cc**—enter the addresses to receive the email notification. Separate multiple recipients with commas

If you omit the **on Failure** message, the **on Success** message is used for both successful synchronizations and unsuccessful synchronizations. If you omit the **on Success** message, notifications are only sent when a synchronization fails.

- 4 Click **Next**.

The tool verifies that the entries in the **Notification email** section are valid.

The following is an example of a summary notification:

```
Schemus Synchronization report
Update operation with example.cloud completed
Time:          Thu May 11 16:43:36 BST 2011
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
```

## Verify a configuration profile

A configuration profile is a combination of settings that you create and save using the Configuration Wizard. You verify a new profile in the last step in the Configuration Wizard. You can also verify an existing profile at any time.

### To verify an existing profile

- 1 Start the Synchronization Tool and select the required configuration profile from the **Configuration** drop-down.

The Summary of settings view is displayed.

- 2 Click **Verify** to test the settings.

The tool runs through a series of tests. If a test is successful, a green tick appears next to the test. If a red cross is displayed, click to the left of the line to correct it. If you have configured multiple sources, each source is checked in turn.

If your data repository is set to the cloud, the tool contacts the cloud security services server during this process.

## Run the Directory Referral Checker

The Directory Referral Checker checks whether referrals on the LDAP server can be followed. A tab is shown for each synchronization type and under each there is another tab for each LDAP source.

Starting at the configured search base for each source, it searches for and follows referrals. The process repeats for each referral until the search is complete or an error occurs.

### To run the Directory Referral Checker:

- 1 Start the Synchronization Tool
- 2 Select a configuration profile from the **Configuration** drop-down.
- 3 Click **View > Directory Referral Checker**.
- 4 Click **Start**.

The LDAP source for each synchronization type is checked in turn.

- 5 Examine the output under each tab to check for problems. When a referral is found, the information that is provided by the directory is displayed in the table, with an icon showing the current status:

- **Waiting**—the Synchronization Tool is attempting to contact the remote server but has not yet received a response
- **Cannot connect to host**—the Synchronization Tool has been unable to connect to the remote host. One of the following issues may be the cause:
  - The referenced host is unavailable
  - The directory service is not running on the referenced host

- The host was not found on the network
- The referral information is incorrect

Further information is provided in the information window.

- **Required BaseDN does not exist**—the location that is referenced by the referral does not exist in the remote directory

For further information, click **Help > Contents** in the Synchronization Tool and review the topic Continuation references and referrals in the Advanced topics section.

# Managing synchronization profiles

This chapter includes the following topics:

- [Modify a configuration profile](#)
- [Delete a configuration profile](#)
- [View the log details for the Synchronization Tool](#)

## Modify a configuration profile

A configuration profile is a combination of settings that you create and save using the Configuration Wizard. You use the profile to extract email, group and user data from your directory sources, and make it available to the cloud security services.

### To modify a configuration profile

- 1 Start the Synchronization Tool.
- 2 Select a configuration profile from the **Configuration** drop-down.
- 3 Click **Modify** to enter the Configuration Wizard.
- 4 To access the step in the Wizard that you want to change, choose from the options on the left-hand panel. For example, click **Data Repository** to set the repository to either **File** or **Symantec.cloud**.
- 5 Click **Save** to save your changes.

## Delete a configuration profile

A configuration profile is a combination of settings that you create and save using the Configuration Wizard. You use the profile to extract email, group and user data from your directory sources, and make it available to the cloud security services.

### To delete a configuration profile

- 1 Start the Synchronization Tool.
- 2 Select a configuration profile from the **Configuration** drop-down.
- 3 Click **Configuration > Delete**.
- 4 In the **Delete Configuration** dialog, click **Yes** to confirm that you want to delete the configuration profile.

## View the log details for the Synchronization Tool

When you run the Synchronization Tool, either interactively or from a command line, logs are generated that help you to understand the actions that the tool has performed.

### To view the logging details for the Synchronization Tool

- 1 Start the Synchronization Tool.
- 2 Click **View > Logs**.

The following details are displayed:

#### Time

The time that the message was logged.

Use the **Log file** drop-down to show the messages that have been logged for a specific date.



## Level

The importance of messages that are shown. It is a cumulative setting; if you select INFO, then *severe* and *warning* levels are also displayed.

Use the **Log level** drop-down to filter the messages. For example, you can choose to display only messages with a level of WARNING.

- 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.

## Logger

The component of the Synchronization Tool that sourced the message. 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 that are added to the destination repository.
- Schemus.sync.repository.remove  
Entries that are removed from the destination repository.

Use the **Logger** drop-down to filter the messages. For example, you can choose to display only messages where the component is Schemus.sync.source.

**Log file**

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

For Windows, this name is located in the following folder:

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

For Linux, this name 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.

**User**

The user that the Synchronization Tool was run as when the message was logged.

**Configuration**

The configuration profile that was running when the message was added to the logs.

**Message**

A description of the message.

- 3 Click on a message to display any additional information at the bottom of the window.

See [“About synchronization types that are supported by the Synchronization Tool”](#) on page 7.

See [“About standard settings for the Synchronization Tool”](#) on page 15.

See [“About the Synchronization Tool”](#) on page 6.

See [“About configuration profiles”](#) on page 24.

# Running the Synchronization Tool

This chapter includes the following topics:

- [Synchronize your data with the cloud security services](#)
- [Run the Synchronization Tool from a command-line interface](#)
- [Schedule the Synchronization Tool](#)

## Synchronize your data with the cloud security services

Once you have created and tested your configuration profile, you can synchronize your data with the cloud security services.

**To synchronize your data with the cloud security services**

- 1 Start the Synchronization Tool.
- 2 Select a configuration profile from the drop-down list in the configuration window, or select **View > Configuration**.

The **Summary** window displays a summary of the configuration profile settings. If the profile includes more than one synchronization type, review the settings of each type by clicking the **Mail**, **Groups**, and **Users** tabs.

- 3 Choose one of the following methods of synchronizing your data:

**Test Update**

Looks at the data in your source (file or LDAP server) and lists the additions, removals, or exclusions. For users, this setting includes the email address and the groups that the user is a member of.

**Note:** When you use the **Test Update** method, no data is synchronized with the cloud security services.

<b>Update</b>	Compares the details that are held in your local change tracking database and sends those that have been removed or added. An incremental update is an efficient way of passing changes to the cloud security services and preserving unchanged data.
<b>Replace</b>	<p>Recreates your local change tracking database and resends all data to the cloud security services, replacing the data that is currently present for that synchronization.</p> <p><b>Warning:</b> Take care when using this method. The data that is currently present in the cloud security services for the synchronization is removed, before the update takes place.</p>
<b>Refresh</b>	<p>Retrieves all data from the cloud security services and recreates your local change tracking database. You might want to use the <b>Refresh</b> method in the following situations:</p> <ul style="list-style-type: none"> <li>■ If you have reinstalled the Synchronization Tool software on a different computer and want to recreate the change tracking database</li> <li>■ If you have added or deleted entries through the portal.</li> </ul> <p>A subsequent update operation is based upon calculating changes from a current copy of the data that is held in the cloud security services.</p>

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).

See [“About configuration profiles”](#) on page 24.

## Run the Synchronization Tool from a command-line interface

You can run the Synchronization Tool from the graphical user interface (GUI) application or from a command-line interface (CLI).. Invoking the Synchronization Tool from a CLI is the first stage to configuring it to operate automatically.

## Linux

The CLI version of the synchronizer on the Linux platform is called *schemusc* and is located in the install directory. Assuming that the installation directory is on your path, first make sure that the GUI version of the 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.

## Windows

The CLI version of the synchronizer on the Windows platform is called *schemusc.exe* and is located in the install directory. So assuming that it has been installed in the default location, first make sure that the GUI version of the 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 profile you want to run. If there are spaces within the configuration profile name, enclose the name in double quotation marks. If there are no spaces within the configuration profile name, you do not need to include the quotation marks.

## Schedule the Synchronization Tool

You can schedule the Synchronization Tool to run at a specific time in the future or at regular intervals.

On Microsoft Windows systems, enter a user name and password the first time a synchronization is scheduled.

Enter the details of the account under which the application is to run when it is scheduled. The Windows Task Scheduler requires these details and the Synchronization Tool does not retain them. If you do not enter account details, the scheduled task is invoked under the local system administrator account. This account may not have the required privileges to perform the synchronization.

You can also edit the schedule and the account details from the Windows Task Scheduler.

On UNIX systems, the schedule is created using the `crontab` of the account. Ensure that this account is the account under which the scheduled operation is to run and that the account has permission to use the `crontab` command.

#### To schedule a synchronization

- 1 Click **Schedule** to set a time for the synchronization profile to run.
- 2 Specify a time in **Run at**.
- 3 Specify a recurring time in **then run every**.
- 4 Choose the days to run from the **on** drop-down list.
- 5 Click **Day of Month** or **Day of Week** and make your selections. If you select both Day of Month and Day of Week, the Synchronization Tool runs as follows:
  - Every month on the chosen date, and
  - Every week on the chosen day.
- 6 Click **Schedule** to save the changes.

#### To remove a synchronization schedule

- ◆ Click **Clear**.

The calendar icon is grayed to show that the synchronization is no longer scheduled.