

# nuix INVESTIGATE TOOLKIT

## Installation and Configuration Guide

Version 8.2.0

January 2020

## DISCLAIMER

© 2017 Nuix. All rights reserved.

This publication is intended for informational purposes only. The information contained herein is provided “as-is” and is subject to change without notice. Although reasonable care has been taken to ensure that the facts stated in this publication are accurate and that the opinions expressed are fair and reasonable, no representation or warranty, express or implied, is made as to the fairness, accuracy or completeness of the information or opinions contained herein, and no reliance should be placed on such information or opinions. Neither Nuix nor any of its respective members, directors, officers, or employees nor any other person accepts any liability whatsoever for any loss arising from any use of such information or opinions or otherwise arising in connection with this publication. Furthermore, this publication contains the confidential and/or proprietary information of Nuix which may not be reproduced, redistributed, or published in any form or by any means, in whole or in part, without the express prior written consent of Nuix. The use, reproduction, and/or distribution of any Nuix software described in this publication requires an applicable software license.

## Revision History:

The following changes have been made to this document

Version Number	Revision Date	Description
1.0	February 2018	Initial release
7.6	September 2018	Updated to reflect changes in the 7.6 release
7.8	May 2019	Updated to reflect changes in the 7.8 release
8.0.4	October 2019	Renamed to Investigate Toolkit to reflect product name change  Added support for new Search Filter standard
8.2.0	January 2020	Updated groups to reflect changes to Investigate  Fixed bug in reporting  Added group ID to reports

# Content

<b>INTRODUCTION .....</b>	<b>6</b>
About Investigate Toolkit.....	6
About this Guide .....	6
Document Conventions.....	6
<b>INSTALLATION .....</b>	<b>7</b>
Prerequisites.....	7
Toolkit Files.....	7
<b>TOOLKIT CONFIGURATION .....</b>	<b>8</b>
Global Settings .....	8
Investigate Settings .....	8
LDAP Settings .....	9
Logging.....	10
Save .....	11
Users Import .....	12
Configuring a User Type.....	12
Deleting a User Type.....	13
Groups Import.....	13
Configuring a Group .....	13
Deleting a Group .....	14
Directories Import .....	14
Configuring a Directory.....	15
Deleting a Directory Mapping .....	16
Group Templates .....	16
Creating a Template .....	16
Modify a Template .....	17
Delete a Template .....	17
<b>SYNCHRONIZATION .....</b>	<b>18</b>
LDAP Synchronization .....	18
Directories Synchronization .....	18
Running the Synchronization .....	18
Manual Synchronization .....	18
Silent Synchronization .....	19
<b>REPORTING.....</b>	<b>20</b>

Data Reported .....	20
Users .....	20
Groups.....	20
Cases .....	20
Audit Events .....	20
Running Reports.....	21
Manual Reporting .....	21
Silent Reporting.....	22
<b>CREATE AND EDIT JSON .....</b>	<b>23</b>
Search Filters.....	23
<b>CREATE A SECURITY GROUP.....</b>	<b>25</b>
<b>APPENDIX: LDAP .....</b>	<b>26</b>
Connection Strings .....	26
Filters .....	26
<b>APPENDIX: SEARCH FILTER STANDARDS.....</b>	<b>27</b>
Root Node.....	27
Searches Array .....	27
Level .....	27
Query .....	27
<b>APPENDIX: LDAPS CONNECTIONS.....</b>	<b>28</b>

# Figures

Figure 1: Investigate Toolkit Main Page.....	8
Figure 2: Global Settings.....	8
Figure 3: Investigate Settings.....	9
Figure 4: LDAP Settings.....	10
Figure 5: Logging Settings .....	11
Figure 6: Options Enabled Settings .....	12
Figure 7: Users Import Settings .....	12
Figure 8: Users Selected.....	13
Figure 9: Import Groups Settings .....	13
Figure 10: Groups Selected .....	14
Figure 11: Configure Directories Settings .....	15
Figure 12: Matching Cases .....	16
Figure 13: Group Templates .....	17
Figure 14: Manual Synchronization.....	19
Figure 15: Run Reports .....	21
Figure 16: Generate Reports .....	22
Figure 17: Create and Edit Search Filters.....	23
Figure 18: Loaded Search Filter.....	24

# Introduction

Welcome to the Nuix Investigate Toolkit Installation and Configuration Guide.

## About Investigate Toolkit

The Investigate Toolkit provides additional functionality to Nuix Investigate, including the ability to:

- Import users from Active Directory into Investigate
- Add users to Investigate groups based on Active Directory groups
- Add cases to Investigate groups based on the directory location
- Run CSV and Excel audit reports
- Create and edit search filters

Once configured, the toolkit can be scheduled to perform these actions silently and provide an audit log of the actions taken.

## About this Guide

This guide provides step by step instructions to help you configure and use the Investigate Toolkit.

## Document Conventions

The following conventions are used in this guide:

//This is a line of code

This is a Menu > Option.

### Note

This box indicates a helpful note, or additional information.

### Tip

This box indicates a tip that could include useful details that may assist you in understanding how to apply the information included in the guide, or to provide an example.

### Warning

This box indicates information that is critical and should be reviewed.

# Installation

## Prerequisites

The Investigate toolkit requires Microsoft .NET Framework 4.5 to be installed.

## Toolkit Files

Installation is not required in order to use the Investigate Toolkit. The toolkit is comprised of the following files, which should be copied into a single directory:

- *Investigate\_Toolkit.exe*
- *Investigate\_Toolkit.exe.config*

**Tip**

The toolkit can be run from any machine that has access to both Investigate and Active Directory via LDAP.

# Toolkit Configuration

The following sections outline the process for configuring and testing the Investigate Toolkit.

**Note** Some options are disabled until Global Settings have been configured.

To begin using the toolkit, double-click on the file *Investigate.exe*.

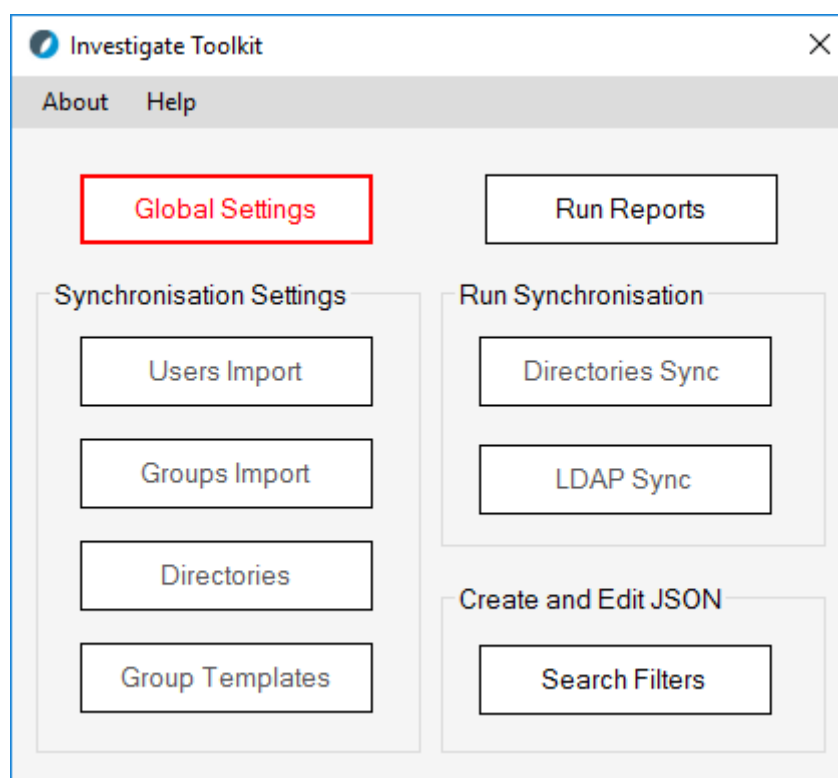


Figure 1: Investigate Toolkit Main Page

## Global Settings

Clicking the global settings button allows you to configure connection details and logging settings. These settings must be defined before Users, Groups, or Directories can be configured.

Figure 2: Global Settings

## Investigate Settings

The following Investigate details must be provided on the Investigate Settings tab.

### 1. Nuix Servers

- Investigate URL: The URL where Investigate can be accessed.
- User Management URL: The URL of the UMS server being used with Investigate.

**Warning** Do not place a trailing slash on the URL as this will cause the validation to fail.

### 2. Misc

Select an action to take when a user has had their access removed in Active Directory. Options include:



- Locking the user
- Deleting the account from Investigate

### 3. Investigate Login

Enter the Username and Password of a valid Investigate administrator account.

#### Tip

Create an Administrator account to use exclusively with the toolkit. Having a dedicated account will ensure that you can easily identify the Audit Events performed by the toolkit from those performed by other users.

- When all fields have been completed, select Validate Investigate. The system will attempt to make a connection to Investigate using the provided details.

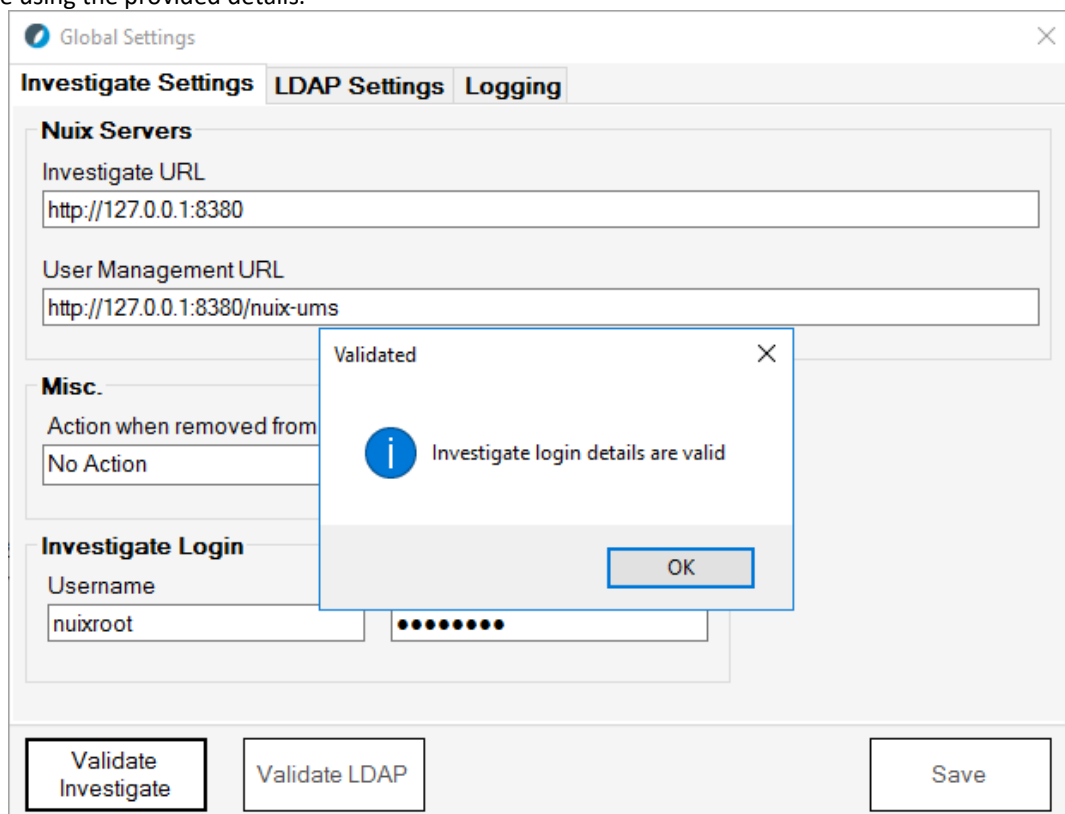


Figure 3: Investigate Settings

## LDAP Settings

The following LDAP details must be provided on the LDAP Settings tab.

- LDAP Server**  
Enter the connection string for Active Directory in LDAP format
- Use SSL**  
Select the Use SLL checkbox if making an LDAPS connection. Please see the appendix for further details on using LDAPS
- LDAP Login**  
Enter the Username and Password of an account that has read access to the domain. The username must be entered using the User Principal Format, for example user@domain.com.

#### Tip

To avoid having to update the password, create a service account with a password that is set to never expire.

- LDAP Attributes**

- Enter the Active Directory attribute to use as the Investigate Username. This field will default to *sAMAccountName*.
  - Enter the Active Directory attribute to use as the LDAP Distinguished Name when validating the user. This field will default to *userPrincipalName*.
5. When all fields have been completed, click Validate LDAP to validate the provided information.

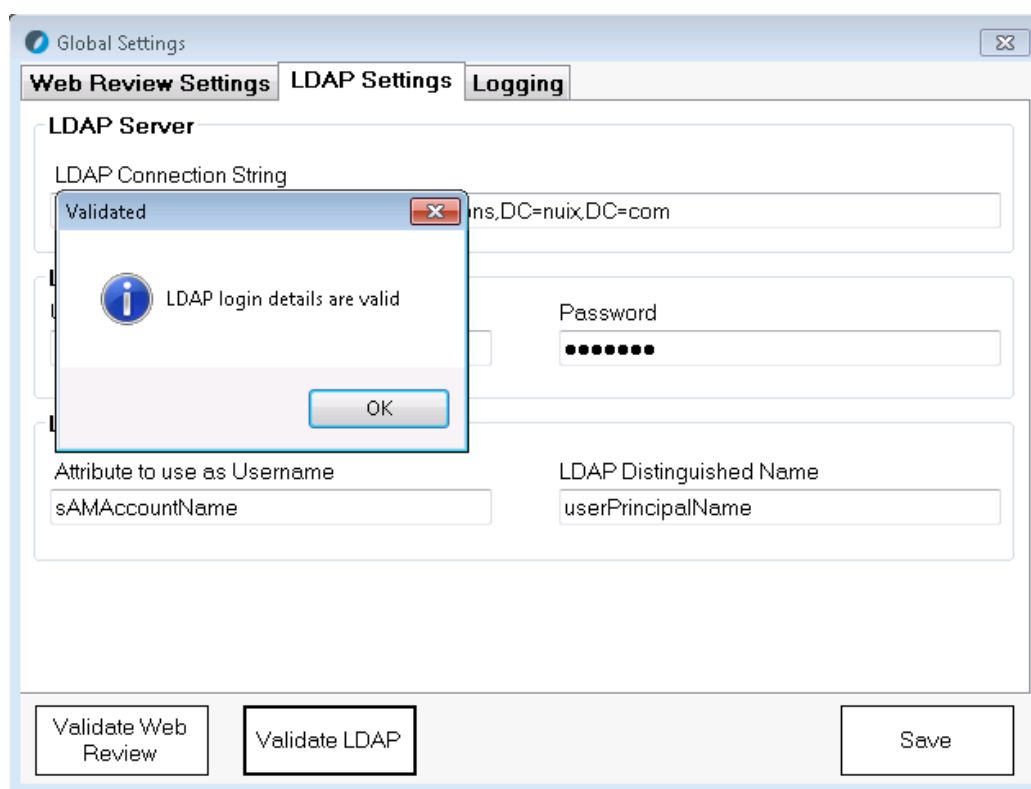


Figure 4: LDAP Settings

## Logging

The following logging details should be provided on the logging tab.

### 1. Logging

- Log level: - Define the level of detail captured in the application logs. "Info" is the recommended level.
- Max Log Size: - Define the maximum size (in MB) of the log file before it is rolled over. A value of zero (0) will set the log size to unlimited.
- Log File: - Define a location and file name for the log file. This field defaults to the current location of the toolkit executable.

### 2. Auditing

- Enabled: - Select to enable Auditing. Auditing logs the changes that the toolkit makes to Investigate users and groups.
- Max Log Size: - Define the maximum size (in MB) of the audit file before it is rolled over. A value of zero (0) will set the log size to unlimited.
- Log File: - Define a location and file name for the audit file. This field defaults to the current location of the toolkit executable.

### 3. Reporting

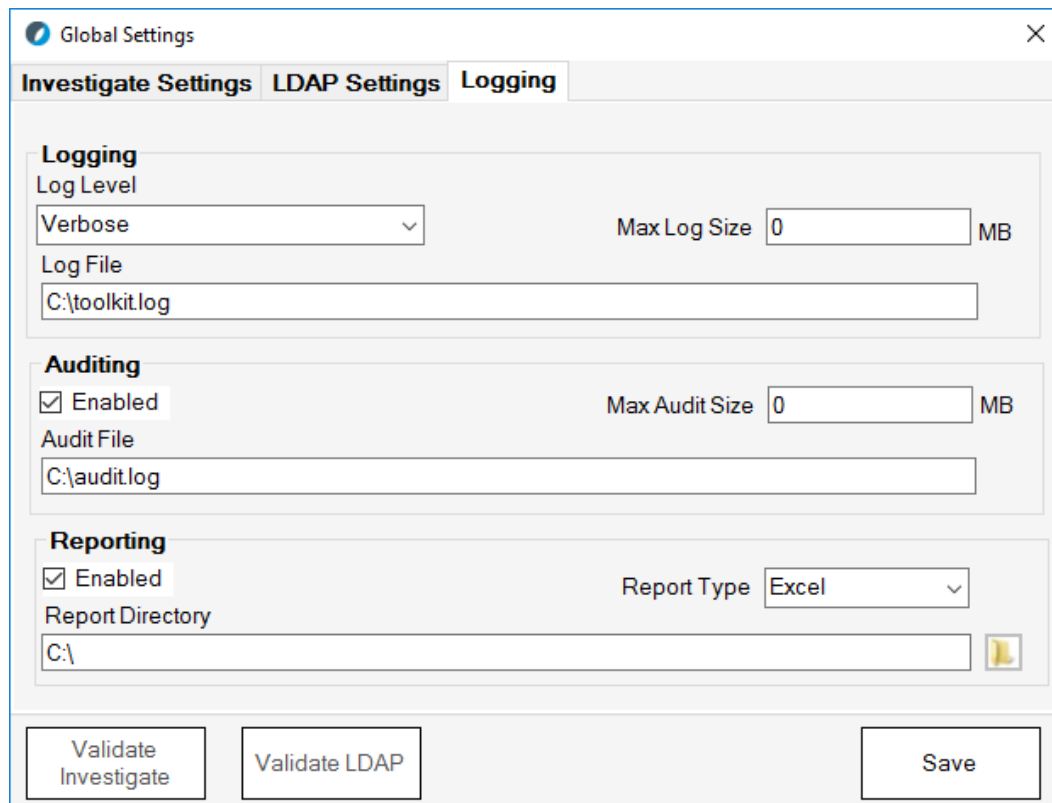
- Enabled: - Select to enable Reporting. Reporting allows you to configure the reporting settings so that reports can

be scheduled.

- Report Type: - Choose the format to use when generating reports. Options include CSV or Excel.

**Note** Installation of Microsoft Excel is *not required* in order to generate Excel reports.

- Report Directory: - Define a location where reports will be generated. To select a local file path, click the button to the right of the textbox.



The image shows the 'Global Settings' dialog box with the 'Logging' tab selected. The dialog has three tabs: 'Investigate Settings', 'LDAP Settings', and 'Logging'. The 'Logging' tab contains three sections: 'Logging', 'Auditing', and 'Reporting'. In the 'Logging' section, 'Log Level' is set to 'Verbose', 'Max Log Size' is 0 MB, and 'Log File' is 'C:\toolkit.log'. In the 'Auditing' section, 'Enabled' is checked, 'Max Audit Size' is 0 MB, and 'Audit File' is 'C:\audit.log'. In the 'Reporting' section, 'Enabled' is checked, 'Report Type' is 'Excel', and 'Report Directory' is 'C:\'. At the bottom, there are three buttons: 'Validate Investigate', 'Validate LDAP', and 'Save'.

Figure 5: Logging Settings

## Save

When finished, click Save to add your changes to the configuration file.

**Note** All passwords are encrypted using AES256 before being saved to the configuration file.

After saving you are returned to the Main page of the toolkit and the Synchronization Setting buttons for Users Import, Groups Import, and Directories will have been enabled and the "Global Settings" button will no longer have red text.

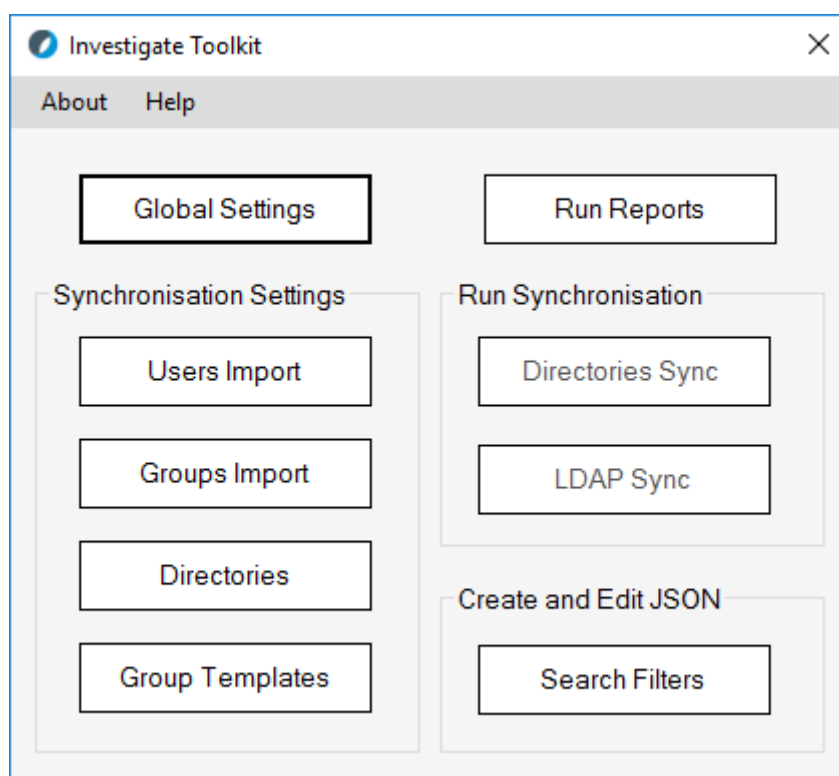


Figure 6: Options Enabled Settings

## Users Import

The Users import settings page allows you to configure the import settings for different Investigate user types. These settings link Active Directory groups to specific Investigate user types. When synchronization is run, the users will be imported into Investigate at the appropriate user level.

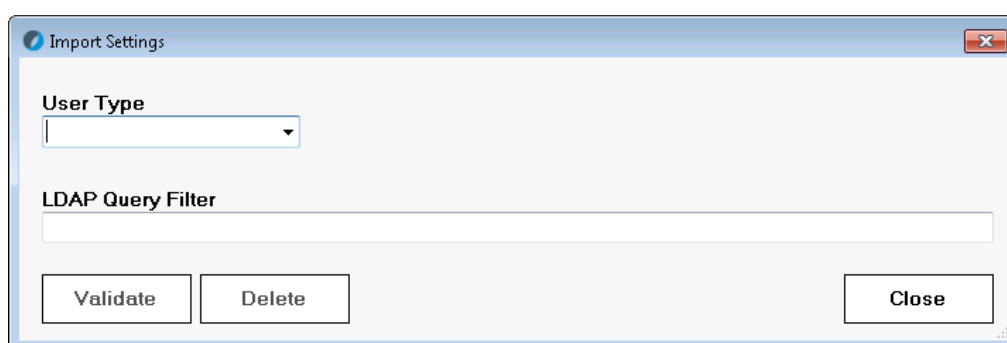


Figure 7: Users Import Settings

## Configuring a User Type

1. Selecting a User Type from the drop down. User types include:

- User
- Administrator

### Note

Each user type corresponds directly with the user types available within Investigate. If a User Type does not have a previously saved configuration, it will be displayed in red font.

2. Provide an LDAP Query Filter to select which Active Directory users should be imported.
3. Click Validate.
4. A new window will open that displays a preview of all users that would be imported with the current LDAP Query Filter.

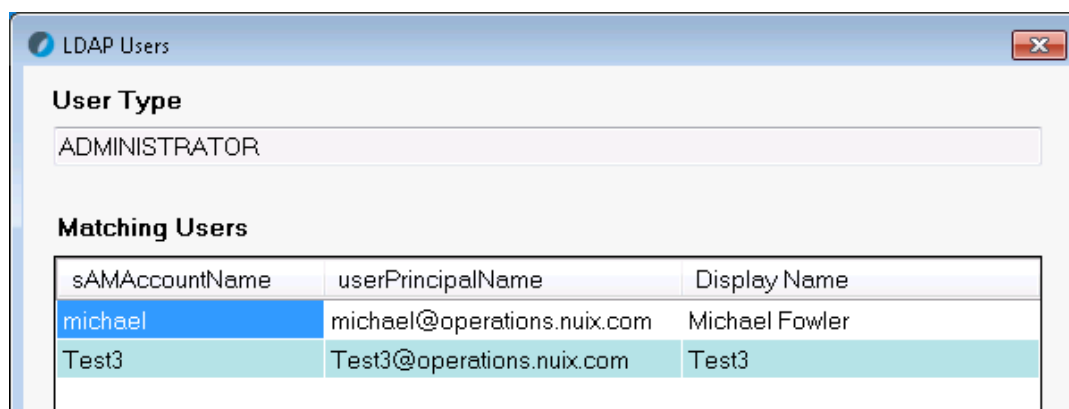


Figure 8: Users Selected

5. Click Save or Cancel as appropriate.
6. Repeat steps 1 - 4 as needed to configure the import of each User Type.

## Deleting a User Type

If you need to change or remove the settings for a user type, use the following steps to delete the configuration for a particular User Type.

1. Select a configured User Type from the drop-down menu.
2. Click Delete.
3. A warning will display to ensure you want to perform this action
4. Click OK to confirm the deletion of the selected User Type configuration settings.

## Groups Import

The Groups import allows you to configure the import settings for the Investigate groups. This links Active Directory group(s) to a Investigate group and when the synchronization is run the users will be imported into the configured Investigate group.

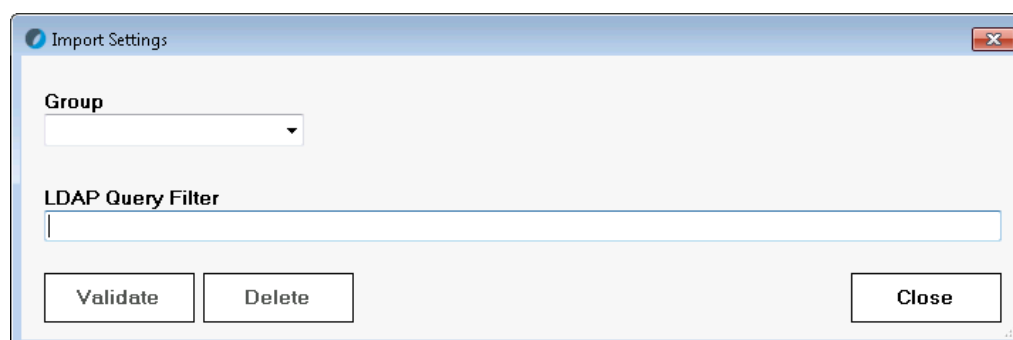


Figure 9: Import Groups Settings

## Configuring a Group

1. Begin by selecting a Group.

### Note

The list of groups is compiled directly from active groups that currently exist within Investigate. If a specific group does not have a previously saved configuration, it will be displayed in red font.

2. Provide an LDAP Query Filter to select which Active Directory users should be imported. Provide an LDAP Query Filter to select which Active Directory users should be imported.
3. Click Validate.
4. A new window will open that displays a preview of all users that would be imported with the current LDAP Query Filter.

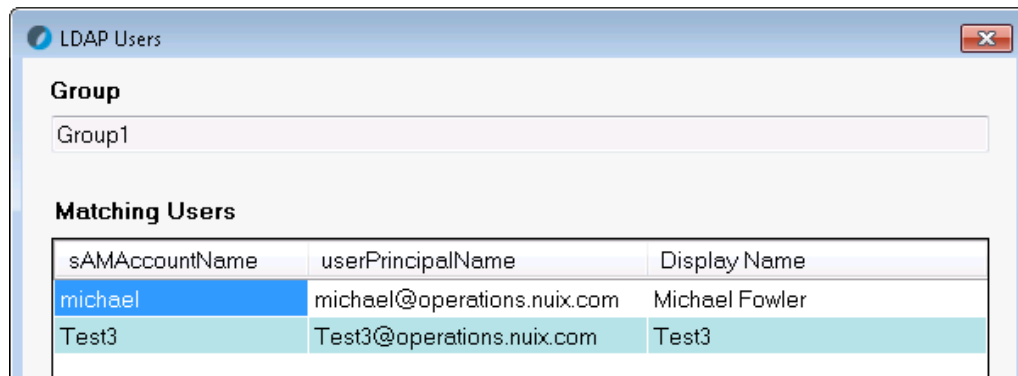


Figure 10: Groups Selected

5. If the preview of matching users is acceptable, click Save.
6. Repeat steps 1 - 4 as needed to configure the import of each Group.

## Deleting a Group

If you need to change or remove the settings for a group, use the following steps to delete the configuration for a particular Group.

1. Select a configured Group.
  2. Select the delete button
  3. A warning will display to ensure you want to take this action
- Select OK and the configuration for this group will be deleted

## Directories Import

The Directories Import settings page allows you to link a directory from the Inventory Management Server to one or more Investigate groups.

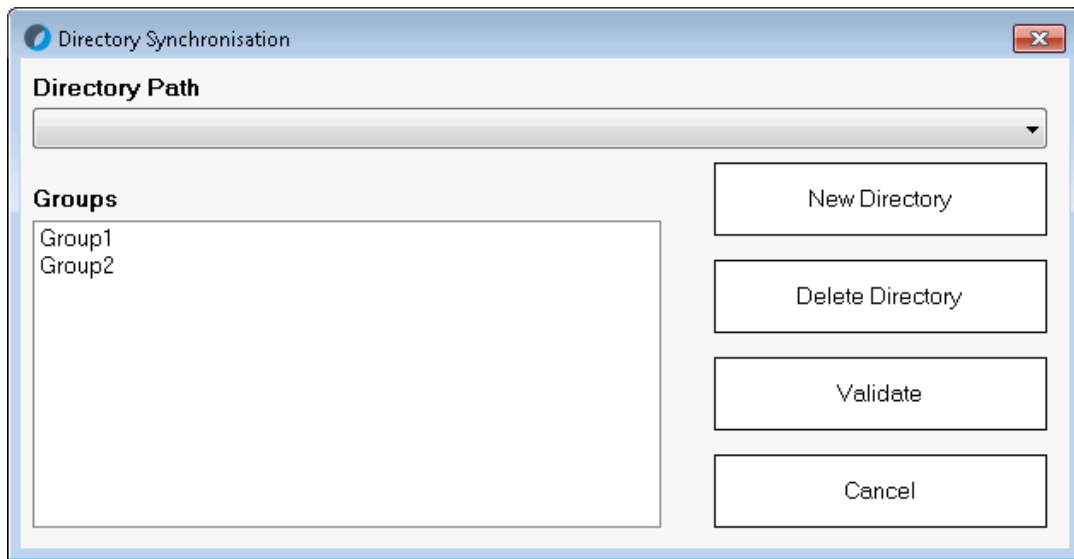


Figure 11: Configure Directories Settings

## Configuring a Directory

1. Begin by selecting New Directory.
2. Enter the path to an IMS case directory.
3. Select one or more groups to map to the selected IMS case directory.
4. Click Validate.
4. When validation is performed a new window will open that displays the selected groups and the cases that are currently located within the IMS directory.

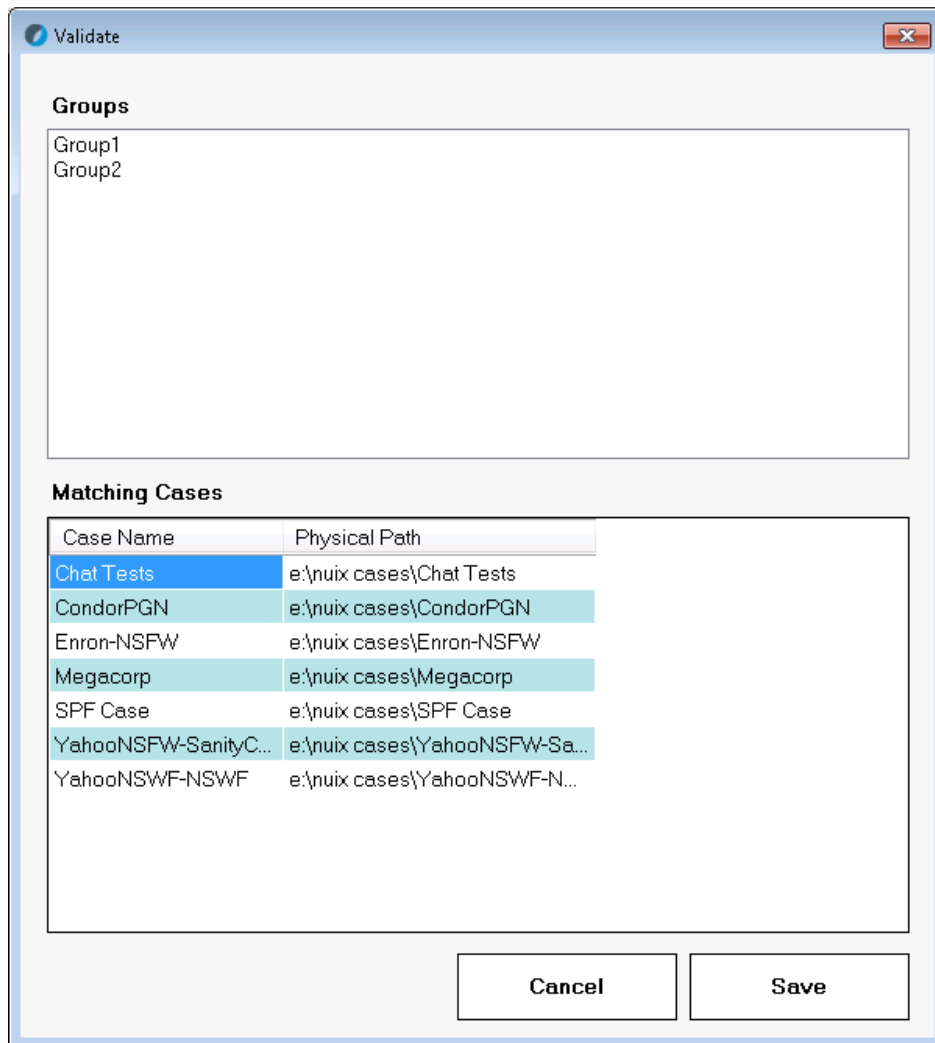


Figure 12: Matching Cases

7. If the validation preview is acceptable, click **Save**.
8. Repeat steps 1 - 5 as needed to configure the import settings for each directory.

## Deleting a Directory Mapping

1. Select a configured Directory.
2. Click "Delete". A warning will display to ensure you want to perform this action.
3. Click "OK" to confirm the deletion of the selected directory configuration settings.

## Group Templates

The toolkit includes the option to create a Investigate group from the command line. The groups template screen enables you to save the securities to apply to the created group.

**Note** A Default template will exist and this template cannot be deleted

## Creating a Template

1. Select Group Templates



2. Select the New Button
3. Enter a Template Name
4. Select the appropriate checkboxes for the needed security options
5. Select the Save button to save the Template to the configuration file

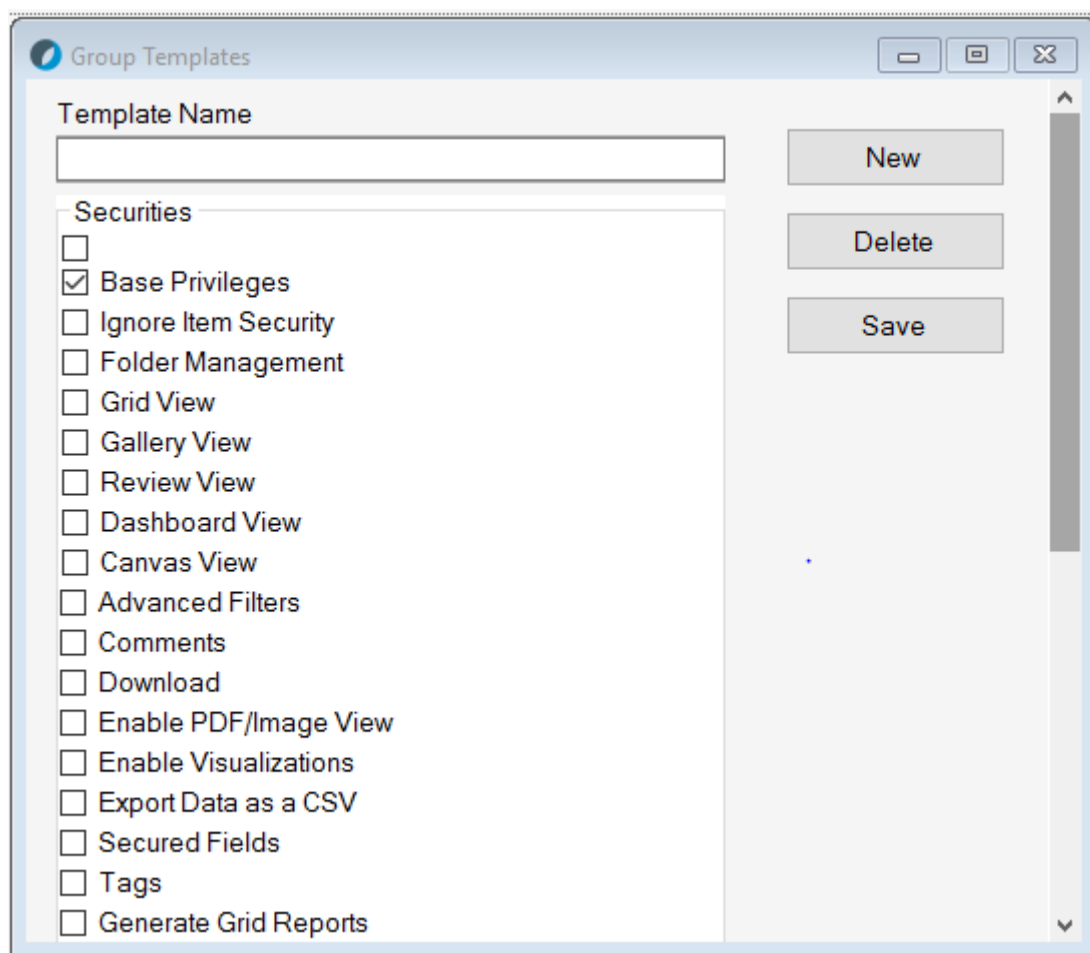


Figure 13: Group Templates

## Modify a Template

1. Select the template from the drop down list
2. Select the appropriate checkboxes for the needed security options
3. Select the Save button to save the changes to the configuration file

## Delete a Template

1. Select the template from the drop down list
2. Select the Delete button to remove the template from the configuration file

# Synchronization

Once configuration of the Investigate Toolkit has been completed, you can start running the synchronization.

## LDAP Synchronization

When LDAP synchronization is performed, the following actions will take place.

- For each User Type configured, the selected Active Directory users will be imported into Investigate and assigned the appropriate user level (User or Administrator).
- Users who have been moved into a new group within the domain controller will have their user type modified in Investigate
- Users removed from all groups will be either Locked or Deleted according to what was defined in the Global Settings.
- Manually created users will not be affected by the synchronization process.

### Warning

If a user is included in multiple user groups within Active Directory, they will be given access at the lowest level listed.

- For each Group that is configured, Domain Controller users that are returned by the LDAP query that also correspond to a Investigate user will be made members of the selected Investigate group.

### Note

If a user does not exist in Investigate, a warning will be logged and no further action will be taken.

If enabled in the Global Settings, all user changes will be logged to the Audit Log.

## Directories Synchronization

When Directory synchronization is performed, the following actions will take place.

- For each configured directory, any cases that are located within the specified directory will be added to the configured Investigate groups.
- Cases that have already been assigned a group will be skipped. This is done to prevent the process from overwriting changes made to permissions manually.

### Warning

If you remove all groups from a case, this process will add the case back to the configured groups. To avoid this, you can create a group with no members and add the case to this group.

- When Investigate scans for cases in the inventory locations that are defined in the Inventory Management configuration, the system will scan down four levels within the directory structure before stopping. This allows you to create a number of sub-directories under the root location and link each of these to one or more Investigate groups.
- If enabled in the Global Settings, all case changes will be logged to the Audit Log.

## Running the Synchronization

### Manual Synchronization

To manually perform a synchronization, click LDAP Sync or Directories Sync from the main page of the toolkit.

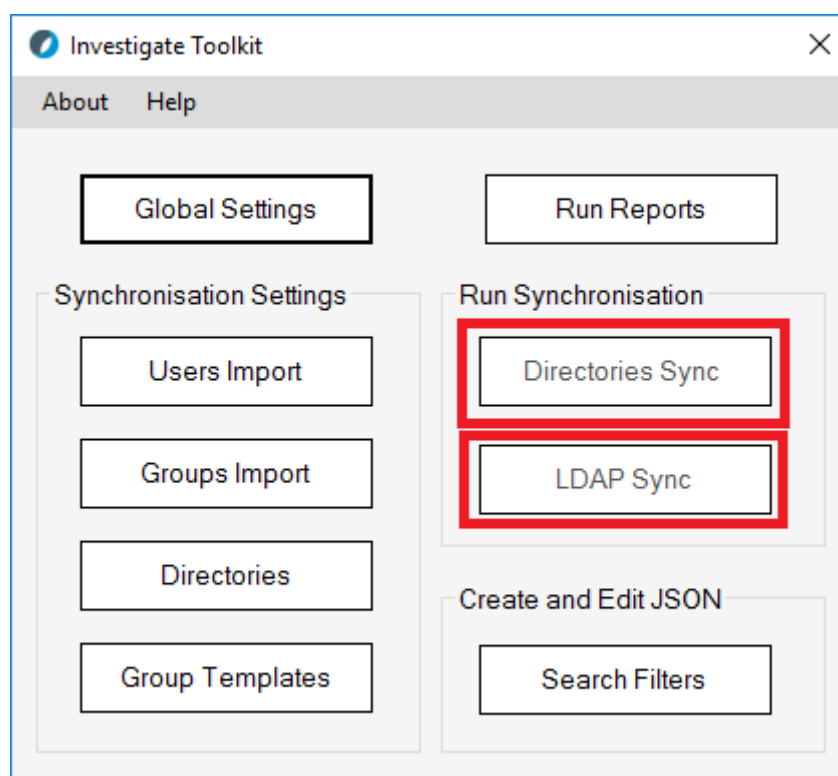


Figure 14: Manual Synchronization

## Silent Synchronization

Synchronization can also be performed silently by running the executable *WebReview\_Toolkit.exe* with the appropriate switches. This allows Synchronization to be run as a scheduled task using Windows Task Scheduler.

Synchronization Type	Switches
LDAP Synchronization	"--ldap" or "-l"
Directories Synchronisation	"--directories" or "-d"

### Note

The switches can be combined to run more than one Synchronization process from the same scheduled task.

# Reporting

Reporting can be run at any time and produces either a number of CSV formatted reports or a single Excel report with multiple tabs. All reports that are created include a timestamp within the filename to ensure they are not overwritten.

## Data Reported

### Users

The Users report/tab provides a listing of all users within Investigate and includes the following information:

- User ID
- User Name
- LDAP DN Value
- Role
- Locked (true/false)
- Created
- Last Log On

#### Note

Audit Reports only contain The number of days of security event history retained is set in the User Management configuration page. By default it is set to 30 days

### Groups

The Groups report/tab provides details for all Investigate and Director security groups, including:

- Group permissions
- Users assigned to the group
- Cases assigned to the group

### Cases

The Cases report/tab provides a listing of the cases currently available within Investigate and includes the following information:

- Case name
- Investigator
- Case description
- Creation date
- IMS URL
- Physical path on the server
- Compound Case (true/false)
- Elastic Search Case (true/false)

### Audit Events

The Audit Events report/tab provides details of the last four weeks of Audit Events. At this time, only Login Attempts and User Unlocked events are recorded by Investigate. The following details are included in the report:

- Event ID
- User name of the user performing the action
- Origin IP (if available)
- Date and Time of the event
- Event Type
- Result (success/failure of login event)
- User name of the user unlocked (for unlock event)

# Running Reports

## Manual Reporting

The following steps can be used to run the report functionality manually.

1. Select **Run Reports** from the main page of the toolkit to open the Generate Reports window.

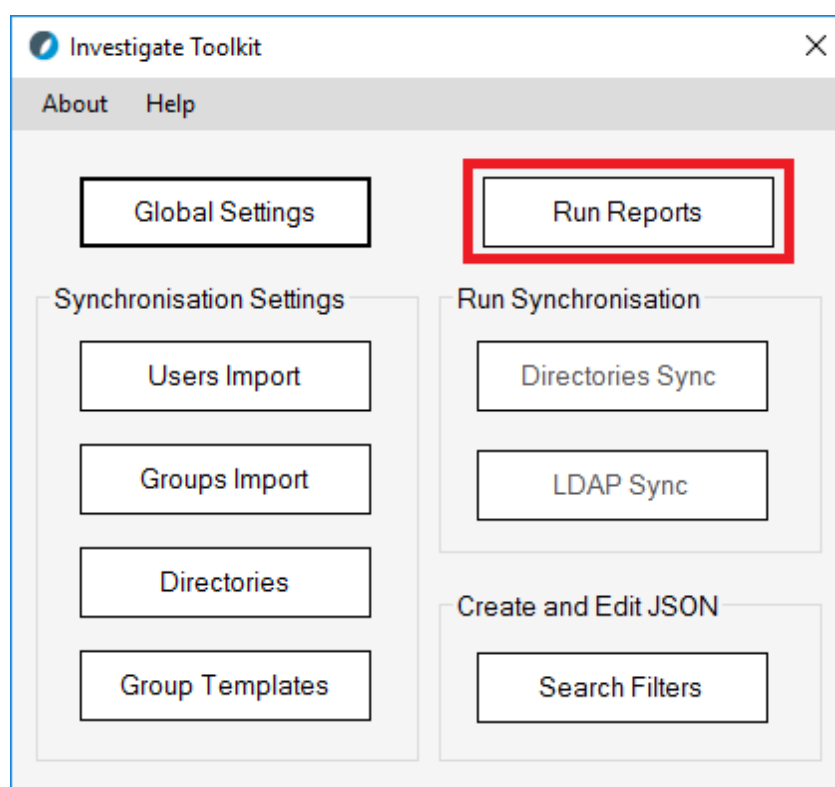
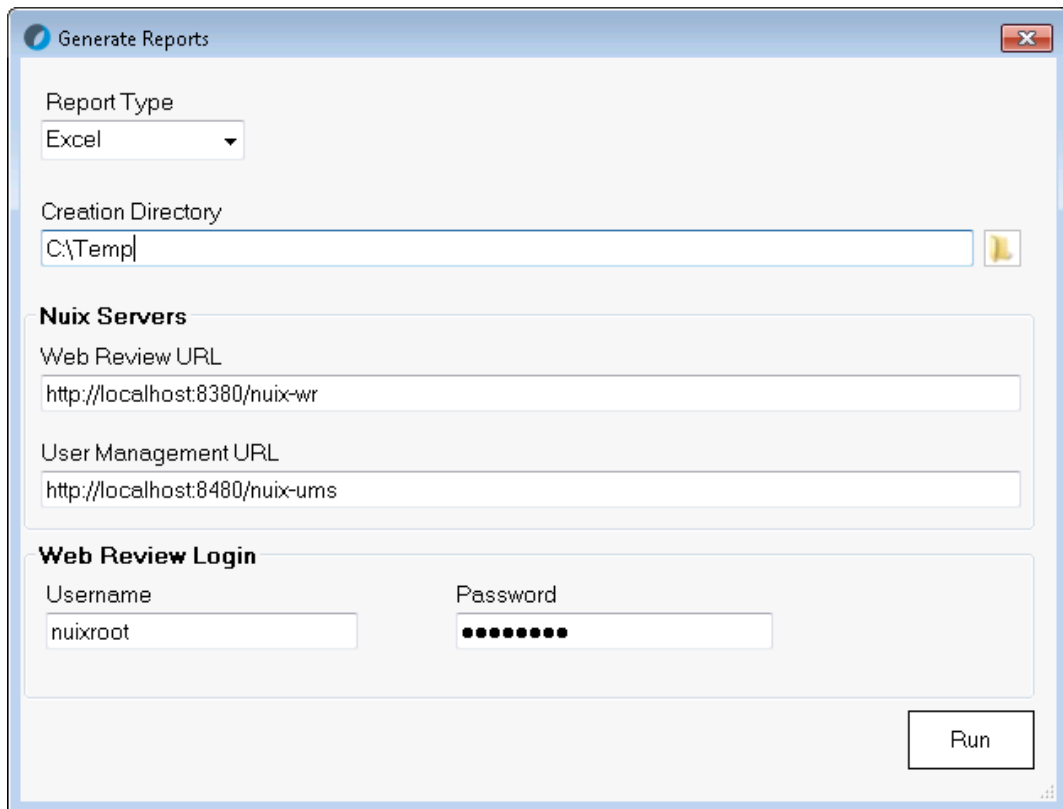


Figure 15: Run Reports

2. Global Settings have been previously configured, all fields will be prepopulated. Otherwise, complete the fields in order to generate reports.
  - a) Select either Excel or CSV from Report Type
  - b) Select the directory the report(s) will be created in.
  - c) Enter the Investigate URL
  - d) Enter the User Management URL
  - e) Enter the Username and Password for a Investigate administrator account
3. Select the Run button
4. A dialog box will advise once the report generation has completed



The 'Generate Reports' dialog box contains the following fields and controls:

- Report Type:** A dropdown menu currently set to 'Excel'.
- Creation Directory:** A text input field containing 'C:\Temp' with a folder selection icon to its right.
- Nuix Servers:** A section containing two text input fields:
  - Web Review URL:** Contains 'http://localhost:8380/nuix-wr'.
  - User Management URL:** Contains 'http://localhost:8480/nuix-ums'.
- Web Review Login:** A section containing two text input fields:
  - Username:** Contains 'nuixroot'.
  - Password:** A masked field represented by ten dots.
- Run:** A button located at the bottom right of the dialog.

Figure 16: Generate Reports

## Silent Reporting

To generate reports silently, run the toolkit executable, *WebReview\_Toolkit.exe*, with the `--report` or `-r` switch. This allows for the reporting to be scheduled using Windows Task Scheduler.

### Note

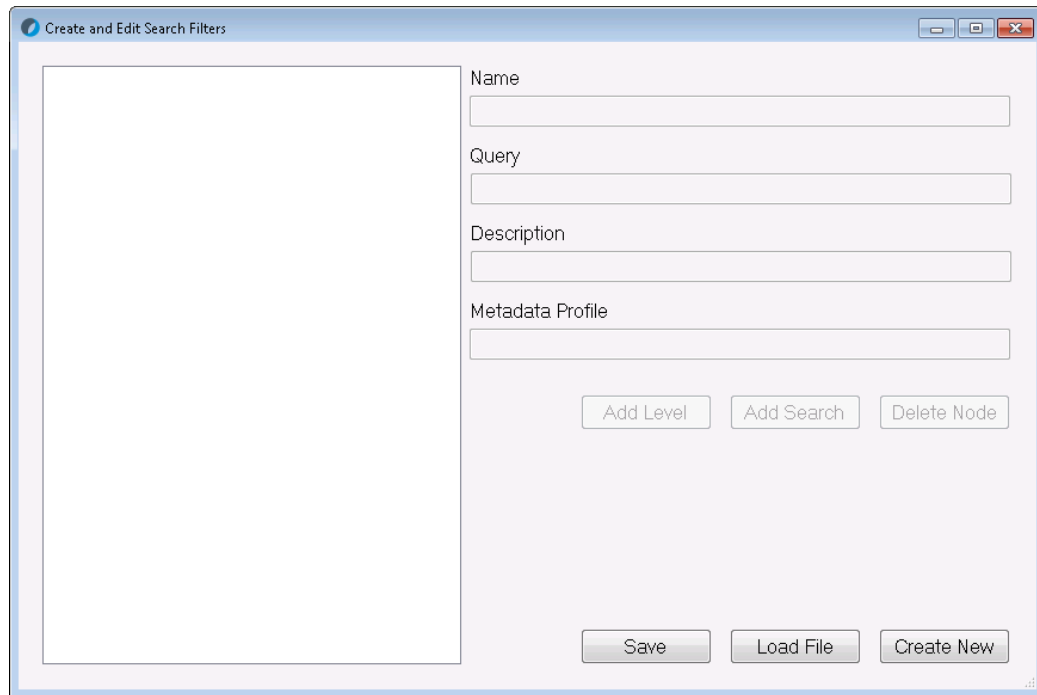
Both synchronization and reporting switches can be added to run both processes from the same scheduled task.

# Create and Edit JSON

This section provides a GUI for creating and editing the JSON files used with Investigate

## Search Filters

1. Select the “Search Filters” button from the main screen
2. The “Create and Edit Search Filters” form will display



**Figure 17: Create and Edit Search Filters**

3. The “Create and Edit Search Filters” form will display
4. Open a Search Filter
  - a) Select “Create New” to start a new Search Filter
  - b) Select “Load File” to open an existing Search Filter

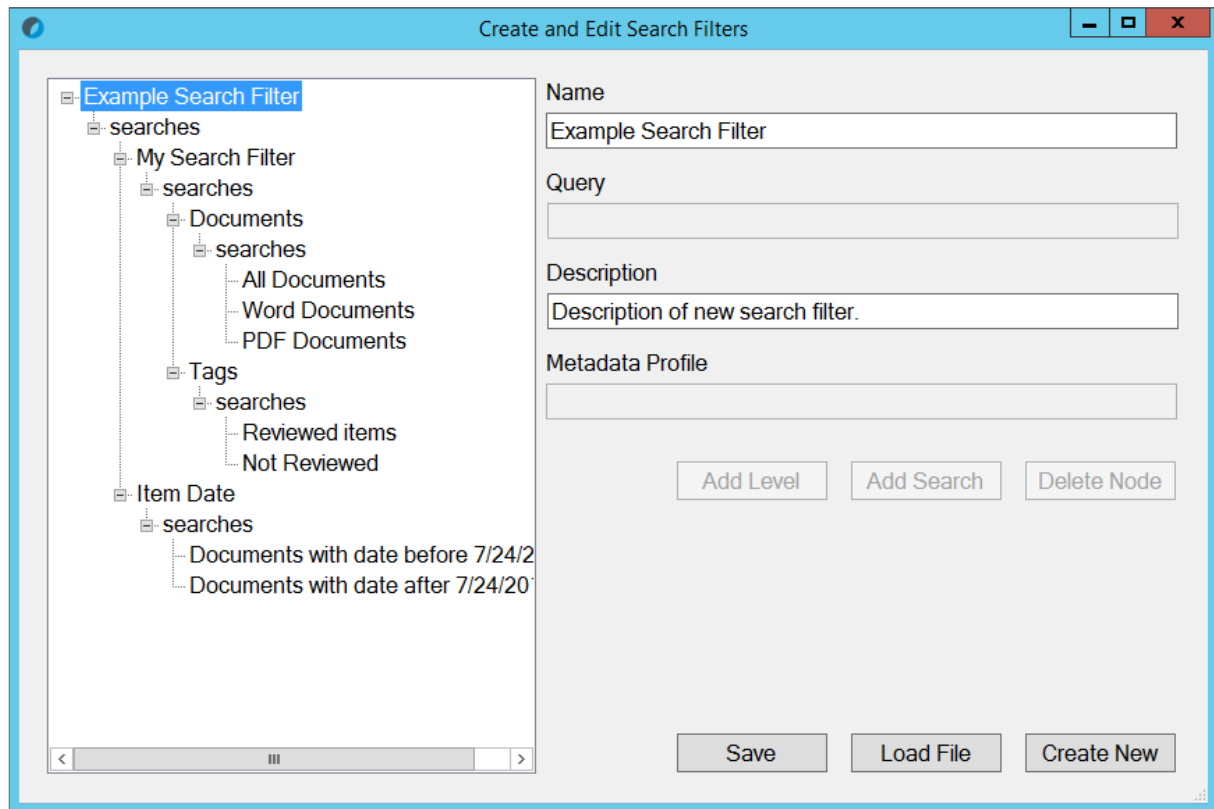


Figure 18: Loaded Search Filter

5. Select the nodes in the Tree View panel and edit the values in the text boxes
6. Add new nodes using the “Add Level” or “Add Searches” Buttons. The form will only enable the buttons as appropriate to ensure a valid Search Query JSON file is being created
7. Edit or enter the values in the text fields. The form will only enable the fields which are valid for the current selection and perform basic validation.
  - Name: Required for all nodes
  - Query: Required for searches. This needs to be a valid Nuix query
  - Description: A description of the Search Filter. Only added to the root node
  - Metadata Profile. This is the profile which will be displayed to user. Enter the exact name of a Metadata Profile which has been made available with Investigate

**Warning**

The Nuix Query and Metadata Profile entries are not validated against Nuix and you need to ensure that these are valid entries

8. Save the Search Query using the “Save” button. This will open a window for you to select the save path.

**Note**

The file extension used does not matter



# Create a Security Group

The toolkit allows you to create a Investigate security group from the command line. To perform this action use the following syntax

```
WebReview_Toolkit.exe [--group or -g] [group name] [optional: template]
```

Where a template is not included the default template is used.

# Appendix: LDAP

The connection to Active Directory relies on a LDAP connection string to create the connection and filters to select the appropriate group(s). The following provides a short guide to creating these LDAP strings

## Connection Strings

The connection string comprised of the server's name and the fully-qualified path of the container object.

- The connection starts with the URI `LDAP://`
- Add the name of the domain controller
- Follow this with the fully qualified DN of the container

Using the above rules the users container on the domain controller `dc1.corp.domain.com` would create the following connection string

`LDAP://dc1.corp.domain.com/CN=Users,DC=corp,DC=domain,DC=com`

More information on LDAP URLs can be found [here](#)

## Filters

The connection string above would return all members of the Users container from the domain controller. To limit this list so that only appropriate users are returned a LDAP search filter is used.

Some examples of LDAP filters are:

Filter	Result
<code>(objectcategory=person)</code>	Return only users and not groups or other objects
<code>(&amp;(objectcategory=person)(memberof=CN=WRA_Users,CN=Users,DC=corp,DC=domain,DC=com))</code>	Return users from the group WRA_Users
<code>(&amp;(objectcategory=person)((memberof=CN=WRA_Users,CN=Users,DC=operations,DC=nuix,DC=com)(memberof=CN=WRA_Admin,CN=Users,DC=operations,DC=nuix,DC=com)))</code>	Return all users from both the groups WRA_Users and WRA_Admin

More information on LDAP search filters can be found [here](#)

# Appendix: Search Filter Standards

## Root Node

An object holding the Search Query metadata and an array of objects

- Must have a name object
- Must have a description object
- Must contain a Searches array

## Searches Array

An array of objects

- Must contain at least one the following. Can contain combinations of both
  - Level
  - Query

## Level

An object containing metadata for a series of queries or another sub-level

- Must have a name object
- Must contain a Searches array
- Can contain a metadata profile

## Query

An object defining a single Nuix query

- Must contain a name object
- Must contain a Nuix Query object
- Can contain a metadata profile

# Appendix: LDAPS Connections

To use LDAPS with the Investigate Toolkit you must make the SSL certificate available to both Windows and the User Management service.

1. Obtain the Domain Controllers Self-Signed SSL Server Certificate
2. Import the certificate into the Windows "Trusted Root Certification Authorities"
  - a) Double click on the certificate file
  - b) Select "Install Certificate"
  - c) Select "Local Machine"
  - d) Select "Next"
  - e) Select "Place all certificates in the following store"
  - f) Select "Browse"
  - g) Select "Trusted Root Certification Authorities"
  - h) Select "OK"
  - i) Select "Next"
  - j) Select "Finish"
  - k) You will get a message advising the action has been successfully completed
  - l) Close the window
3. Import the certificate into the User Management Service (UMS) keystore
  - a) Open a command prompt
  - b) Navigate to the UMS Java bin directory. The default location is  
`C:\Program Files\Nuix\Web Platform\Nuix UMS\jre\bin`
  - c) Run the following command  
`keytool -import -alias root -keystore ../lib/security/cacerts -trustcacerts -file <path-to-ssl-certificate>/ldap-server.cer`
  - d) Enter the password `changeit`