

IdFix - Directory Error Remediation Guide

Preparation and Operations

**Published:** June 2015

MICROSOFT MAKES NO WARRANTIES, EXPRESS OR IMPLIED, IN THIS DOCUMENT.

Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, no part of this document may be reproduced, stored in or introduced into a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), or for any purpose, without the express written permission of Microsoft Corporation.

Microsoft may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from Microsoft, our provision of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.

The descriptions of other companies’ products in this document, if any, are provided only as a convenience to you. Any such references should not be considered an endorsement or support by Microsoft. Microsoft cannot guarantee their accuracy, and the products may change over time. In addition, the descriptions are intended as brief highlights to aid understanding, rather than as thorough coverage. For authoritative descriptions of these products, please consult their respective manufacturers.

© 2013 Microsoft Corporation. All rights reserved. Any use or distribution of these materials without express authorization of Microsoft Corp. is strictly prohibited.

Microsoft and Windows are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

The names of actual companies and products mentioned herein may be the trademarks of their respective owners.

Contents

[Preparation and Operations 1](#_Toc417035387)

[1 Overview 6](#_Toc417035388)

[2 Preparation 7](#_Toc417035389)

[2.1 Functionality 7](#_Toc417035390)

[2.2 Requirements 8](#_Toc417035391)

[2.2.1 Hardware Requirements 8](#_Toc417035392)

[2.2.2 Software Requirements 8](#_Toc417035393)

[2.2.3 Identity Management Systems Conflicts 9](#_Toc417035394)

[2.3 Active Directory Impacts 9](#_Toc417035395)

[2.3.1 Multi-tenant 9](#_Toc417035396)

[2.3.1.1 Attributes that may be updated 9](#_Toc417035397)

[2.3.1.2 Attribute Synchronization Rules 9](#_Toc417035398)

[2.3.1.3 Active Directory Attribute Values 10](#_Toc417035399)

[2.3.2 Dedicated 10](#_Toc417035400)

[2.3.2.1 Attributes that may be updated 10](#_Toc417035401)

[2.4 Installation 10](#_Toc417035402)

[3 Operation 11](#_Toc417035403)

[3.1 Running the Tool 11](#_Toc417035404)

[3.2 Remediation Strategy 15](#_Toc417035405)

[3.2.1 Query/Sort/Fix 15](#_Toc417035406)

[3.2.2 Suggested Update Values 17](#_Toc417035407)

[3.2.2.1 Suggestions for duplicates 17](#_Toc417035408)

[3.2.2.2 Suggestions for format errors 17](#_Toc417035409)

[3.3 Error Explanations 17](#_Toc417035410)

[3.3.1 Character 18](#_Toc417035411)

[3.3.2 Format 18](#_Toc417035412)

[3.3.3 TopLevelDomain 18](#_Toc417035413)

[3.3.4 DomainPart 18](#_Toc417035414)

[3.3.5 LocalPart 18](#_Toc417035415)

[3.3.6 Length 18](#_Toc417035416)

[3.3.7 Duplicate 18](#_Toc417035417)

[3.3.8 Blank 18](#_Toc417035418)

[3.3.9 MailMatch 19](#_Toc417035419)

[4 Appendix 20](#_Toc417035420)

[4.1 New Functionality in this Release 20](#_Toc417035421)

[4.1.1 Settings 20](#_Toc417035422)

[4.1.2 Multiple Forests 20](#_Toc417035423)

[4.1.3 Generic LDAP 20](#_Toc417035424)

[4.1.4 Ports 20](#_Toc417035425)

[4.2 Answers to Frequently Asked Questions 20](#_Toc417035426)

[4.2.1 Feedback 20](#_Toc417035427)

[4.2.2 Performance 20](#_Toc417035428)

[4.2.3 Number of errors shown 21](#_Toc417035429)

[4.2.4 Temporary files 21](#_Toc417035430)

[4.2.5 Directory Exceptions 21](#_Toc417035431)

[4.2.6 Don’t see updates in other domains 21](#_Toc417035432)

[4.2.7 FAIL (ACTION) 21](#_Toc417035433)

[4.2.8 Double Byte Characters 22](#_Toc417035434)

[4.2.9 Sorting 22](#_Toc417035435)

[4.2.10 Export Data 22](#_Toc417035436)

[4.2.11 Import Data 22](#_Toc417035437)

[4.2.12 Multiple Forests - GAL Synchronization 22](#_Toc417035438)

[4.2.13 Multiple Forests – Resource Forest Topology 22](#_Toc417035439)

[4.3 Supported Errors 23](#_Toc417035440)

[4.3.1 Multi-Tenant Errors 23](#_Toc417035441)

[4.3.2 Dedicated Errors 25](#_Toc417035442)

# Overview

The Office 365 Customer Experience (CXP) team is working to reduce the time required to remediate Identity issues when on-boarding to Office 365. A portion of this effort is intended to address the time involved in remediating the Active Directory errors reported by the directory synchronization tools. The focus of IdFix is to enable the customer to accomplish this task in a simple, expedient fashion without relying on subject matter experts.

To date, processes used to remediated Active Directory issues in customer environments have been inconsistent at best. Each customer has relied upon interpretations of the guidance, expensive consulting, and the varied skill sets they have local to their organizations. The result has been long delays in correcting errors with corresponding delays in deployment and associated customer dissatisfaction. *Microsoft has recognized that customers need a basic tool to alleviate this pain.*

The Microsoft Office 365 IdFix tool provides customers the ability to identify and remediate the majority of object synchronization errors in their Active Directory forests in preparation for deployment to Office 365. Analysis from the Support cases per month shows that roughly 60% of all errors seen daily fall into duplicate or malformed proxyAddresses and userPrincipalName. The utility does not fix all errors, but it does find and fix the majority. This remediation will then allow them to more successfully synchronize users, contacts, and groups from the on-premises Active Directory into the Microsoft Office 365 environment.

**Note:** IdFix may identify errors beyond those that emerge during synchronization. The most common example is compliance with rfc 2822 for smtp addresses. Although invalid attribute values can be synchronized to the cloud the best practice recommendation from the product group is that these errors be corrected.

# Preparation

Depending on the number of objects in the on-premises Active Directory, there may be a large number of objects to synchronize. Even a low failure rate can result in a large number of objects that must be manually corrected. This can significantly delay a deployment and increase project expense.

The remediation effort is focused on directory synchronization errors which may be raised even if the on-premises environment seems to be operating normally. Remember that the directory synchronization tools check for values that could potentially cause issues with cloud services that may not cause issues in the on-premises environment.

## Functionality

This document describes how to use the IdFix tool to perform the discovery and remediation of the objects and their attributes from the on-premises Active Directory environment and is intended for the Active Directory administrators responsible for supporting the Office 365 service. The Administrator using the tool should understand the implications of modifying directory objects and attributes.

IdFix queries all domains in the currently authenticated forest and displays object attribute values which would be reported as errors by the supported directory synchronization tool. The datagrid supports the ability to scroll, sort, and edit those objects in a resulting table to produce compliant values. Confirmed values can then be applied to the forest with the ability to undo updates. *Transaction rollback is supported.*

In the case of invalid characters, a suggested “fix” is displayed where it can be determined from the existing value. Changes are applied only to records for which the customer has set an ACTION value. *Confirmation of each change is enforced.*

**Note:** Suggested values for formatting errors start with the removal of invalid characters and then the value must be updated by the user. It is beyond the scope of this utility to determine what the user really wanted when a mistake in formatting is detected.

Not all objects should be made available for editing as some could cause harm to the source environment; e.g. critical system objects. These objects are excluded from the IdFix datagrid. *Well Known Exclusions* as defined by the *Deployment Guide* are supported*.*

Data can be exported into CSV or LDF format for offline editing or investigation. *Save to File is supported.*

*Import of CSV is supported.* There are caveats with this feature. The function relies upon the distinguishedName and attribute to determine the value to update. The best way to do this is to export from a query and change the Update. Keep the other columns as they were and do not introduce escape characters into the values. See section 4.2.12 for additional details.

Since IdFix makes changes in the customer environment, logging is included. *Verbose logging is enabled by default.*

Support for both Multi-Tenant and Dedicated versions of Office 365 are enabled in this release. The rule sets are selected via the Settings icon on the menu.

**Note:** Additional functionality will be considered for future releases, and suggestions for improvement are very much appreciated.

## Requirements

The hardware, software, and other requirements and considerations for running IdFix are covered in this section.

### Hardware Requirements

A physical or virtual machine is required in order to run IdFix. The computer should meet the following specifications:

* 4 GB ram (minimum)
* 2 GB of hard disk space (minimum)

### Software Requirements

Table 2 shows the software requirement for the workstation running the tool, as well as the target Active Directory forest. Note that IdFix does not need to be installed on the Exchange or Active Directory server. It merely needs to be installed on a workstation in the forest and have access to a Global Catalog server.

Table 2. IdFix Software Requirements

| Software | Description |
| --- | --- |
| IdFix Workstation | |
| Operating System | The application has been tested on Windows Server 2008 R2 and Windows 7 for x64 bit versions. |
| .NET Framework 4.0 | .NET Framework 4.0 or higher must be installed on the workstation running the application. |
| Active Directory | Queries are via native LDAP and have been tested with Windows Server 2008 R2, but all versions should be expected to work. |
| Exchange Server | The messaging attributes retrieved are version independent and should work with Exchange 2003 or newer. |
| Permissions | The application runs in the context of the authenticated user which means that it will query the authenticated forest and must have rights to read the directory. If you wish to apply changes to the directory the authenticated user needs write permission to the desired objects. |

### Identity Management Systems Conflicts

It is important that any identity management system in the on-premises Active Directory environment be evaluated to determine if it creates any conflicts with IdFix. The risk is after correcting an error, an on-premises identity management system may update the attribute again, returning it to its original error state. Before implementing directory synchronization, it may be necessary to review or modify portions of existing identity management systems if they are repeatedly generating invalid attribute values.

## Active Directory Impacts

This section describes the updates that may be applied to attributes in the customer's on-premises Active Directory environment.

### Multi-tenant

#### Attributes that may be updated

* mail
* mailNickName
* proxyAddresses
* sAMAccountName
* targetAddress
* userPrincipalName

#### Attribute Synchronization Rules

See the following support article for information on the attributes that can be included in synchronization.

[List of attributes that are synchronized to Office 365 and attributes that are written back to the on-premises Active Directory Domain Services](http://support.microsoft.com/kb/2256198)

#### Active Directory Attribute Values

IdFix checks several Active Directory attributes for the types of errors included in the [Planning Directory Synchronization – Active Directory Cleanup](http://technet.microsoft.com/en-us/library/hh852469.aspx).

### Dedicated

#### Attributes that may be updated

* displayName
* mail
* mailNickName
* proxyAddresses
* targetAddress

## Installation

**►To install the IdFix tool**

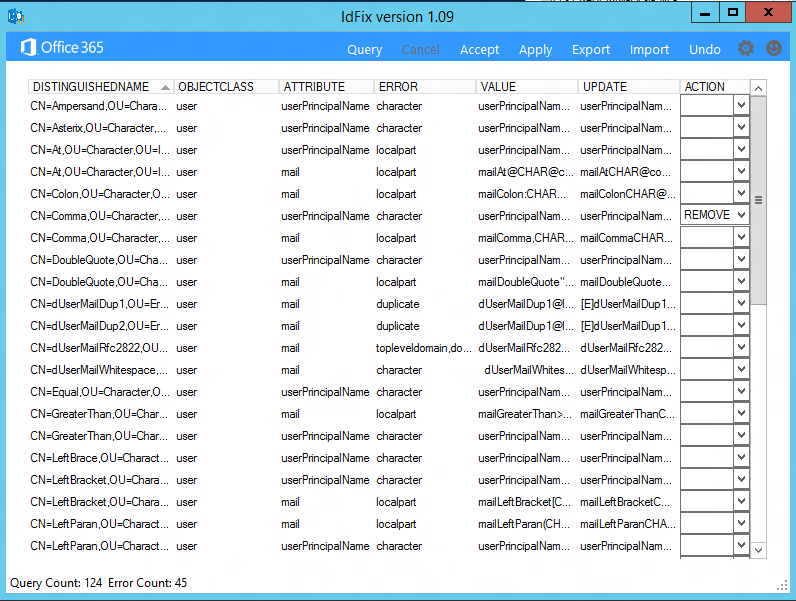
Extract the zip, copy all the files in the IdFix folder to a folder on the local hard drive of a workstation that meets all stated requirements.. Rename the executable file to end in an EXE extension. There are no other dependencies. The location of the program files is arbitrary.

* A new verbose log is created each time you run the application.
* All changes applied to the forest are saved in separate Undo files with a date and time stamp.

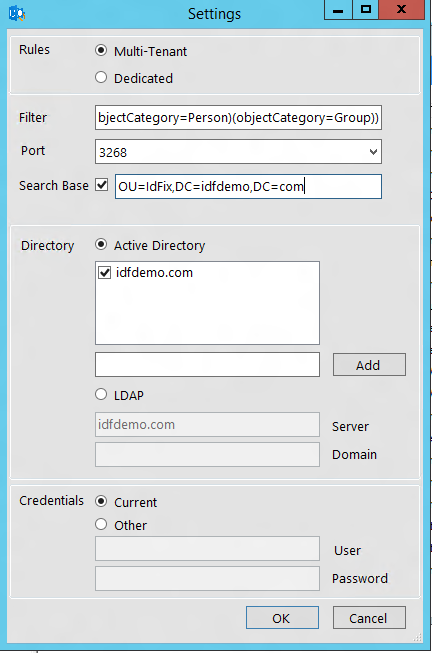
**Note:** Although IdFix tracks its own updates, it is not able to track updates made by other machines or applications.

# Operation

## Running the Tool



1. Log-on to the workstation where you installed IdFix using an account which can read and, if desired, write changes to your on-premises Active Directory objects.
2. Directory synchronization rule sets are different depending on which version of Office 365 is in use. The ***Settings***icon allows you to choose relevant options for the next query.
   1. Multi-Tenant or Dedicated/ITAR rule sets in order to detect attribute values known to cause directory synchronization errors relevant to the version of Office 365 in use.
   2. The scope of the query can be limited by altering the Filter value with a valid LDAP syntax value.
   3. The Search Base to start searching can be adjusted by selecting the Search Base checkbox and inputting a valid DN in the SearchBase field. When the check box is first checked, the default DN of the root domain of the forest is set in the text box for easy editing. The text box can then be edited to have a container to serve as the Search Base. If multiple forests are selected, the Search Base is ignored.
   4. Port can be set to 3268, 389, or 636. The default value when the application is first started is 3268. This allows the query to return values from all trees in the default forest. While it is unusual for forests to contain more than one tree it does happen. You will notice that after updates are applied the port will automatically change to 389. This is because writes must be applied to the writeable naming context which does not support 3268 as a valid option. Port 389 is the default for generic LDAP queries and 636 can be selected if you require LDAP over SSL.
   5. The Directory option specifies whether the query will be targeted at Active Directory or generic LDAP. Multiple forests are supported and can be added through the Add button. Forests can be removed from the query by unchecking the value in the list. Generic LDAP does not support multiple instances at this time.
   6. Credentials will use the currently authenticated user by default. If accessing a generic LDAP source you will need to enter the user value in the format required by the target system.



1. ***Query***for relevant directory synchronization errors. IdFix queries all objects with a filter for applicable attributes. IdFix updates the status line on the bottom of the dataGridView and writes all values to the log.
2. ***Cancel***terminates a running query if the user does not wish to continue.
3. IdFix applies rules against the required AD attributes to determine which objects **must be** remediated and presents you with any detected error conditions.
   1. IdFix displays items with information related to the object in question and the error conditions. Objects are identified by the distinguishedName with the associated error type and value that is in error.
   2. Where feasible, IdFix presents a recommendation for corrective data in the **UPDATE** column.

**Note:** Recommendations are based on a “best effort” approach for the specific object in question. Since recommendations are object specific, they are not checked against the existing data set and may introduce additional errors.

* 1. For certain types of errors (duplicates and format errors), a recommendation for correction may not be provided. For example, if a userPrincipalName ended in a non-routable top level domain then the user must determine what top level domain they would prefer. Corrective information must be manually entered to correct the issue.
  2. In the event multiple errors are associated with a single attribute, errors are combined into a single line item.
  3. If a blank datagrid is displayed after execution, then no errors were returned. This is a good thing.

1. To correct the object attribute values, select one of the following ACTION options from the drop down list:

* **COMPLETE -** The original value is acceptable and should not be changed despite being identified as being in an error state. For example, two users may have a proxyAddress identified as duplicate. Only one can use the value for mail delivery. The user with the correct value should be marked as COMPLETE, while the other user is marked as REMOVE.
* **REMOVE -** The attribute value will be cleared from the source object. In the case of a multi-valued attribute; e.g. proxyAddresses, only the individual value shown will be cleared.
* **EDIT** - The information in the UPDATE column will be used to modify the attribute value for the selected object. In many cases, a valid update value has been predetermined. In these cases, you can mark the ACTION as EDIT and go on to the next error. If the predetermined update value is not desired, you can manually input the new value.
* **UNDO** – This value is only shown if the user has loaded a previously saved Update file. The sole operation that can be executed is to restore the original value.
* **FAIL** – This value is only shown if an update value has an unknown conflict with the directory rules. In this case, you may attempt to edit the value again. It may be necessary to analyze the values in the object using ADSIEDIT.

**Note: on empty ACTION** - Only errors with a customer selected Action will be considered for update. To reiterate; unless a specific choice is made IdFix will not perform any operation on the error.

1. The option to ***Accept*** all suggested updates is available.
2. After selecting the ACTION for one or more errors, choose the ***Apply***menu item to write the values to Active Directory. Successful writes are indicated by displaying “COMPLETE” in the ACTION column.
3. IdFix writes all UPDATE transactions to a transaction log. The following is an example.

4/17/2015 10:37:55 AM Initialized - IdFix version 1.08

4/17/2015 10:37:56 AM Loading TopLevelDomain List

4/17/2015 10:37:57 AM Ready

4/17/2015 10:38:02 AM Query

4/17/2015 10:38:02 AM RULES:Multi-Tenant SERVER:demo.com PORT:3268 FILTER:(|(objectCategory=Person)(objectCategory=Group))

4/17/2015 10:38:02 AM Please wait while the LDAP Connection is established.

4/17/2015 10:38:03 AM Query Count: 165 Error Count: 112 Duplicate Check Count: 333

4/17/2015 10:38:03 AM Elapsed Time: Query - 00:00:00.5625108

4/17/2015 10:38:03 AM Write split files

4/17/2015 10:38:03 AM Merge split files

4/17/2015 10:38:03 AM Count duplicates

4/17/2015 10:38:03 AM Write filtered duplicate objects

4/17/2015 10:38:03 AM Read filtered duplicate objects

4/17/2015 10:38:03 AM Read error file

4/17/2015 10:38:03 AM Elapsed Time: Duplicate Checks - 00:00:00

4/17/2015 10:38:03 AM Populating DataGrid

4/17/2015 10:38:03 AM Elapsed Time: Populate DataGridView - 00:00:00.0468759

4/17/2015 10:38:03 AM Query Count: 165 Error Count: 130

4/17/2015 10:38:15 AM Apply Pending

4/17/2015 10:38:18 AM Update: [CN=At,OU=Character,OU=IdFix,DC=demo,DC=com][user][mailnickname][character][mailNickNameAt@CHAR][mailNickNameAtCHAR][EDIT]

4/17/2015 10:38:18 AM COMPLETE

1. In the event of an unwanted correction, you may perform a transaction update Undo one level deep per UPDATE transaction.

* *Apply* generates a LDF file for the transactions that are applied
* To ***Undo*** a transaction, select the LDF file that contains the appropriate transaction and reload it into the table

**Note:** IdFix cannot track updates to objects or attributes that occur outside of the application. If you and someone else edit the same attribute, then the last change is the one committed to the object.

1. You have the ability to ***Export*** what’s in the table to review with others before taking corrective action, or to use as the source of a later bulk import using the ***Import*** option*.*
2. You have the ability to ***Import*** data from a CSV file to allow offline manual edits to be applied. Be very careful with manually edited files and use an Exported CSV file as a template. *Testing is strongly recommended and there is no guarantee that what you do offline will be correctly recognized by IdFix. See section 4.2 for additional information on Importing data.*
3. If the query returns more than 50,000 errors the menu items ***Next Block*** and ***Previous Block*** are displayed. The number of errors that can be displayed on the screen at one time is limited to avoid application exceptions resulting from exceeding physical memory.
4. You may always submit suggestions for improvement or support requests via the ***Feedback*** icon which will go directly to [IdFixSupport@Microsoft.com](mailto:IdFixSupport@Microsoft.com).

## Remediation Strategy

For small numbers of errors the order of error remediation may not matter. For larger numbers of errors it is recommended that a strategy be applied to minimize the time involved in completing the remediation task.

### Query/Sort/Fix

We’ve seen a number of consultants use the tool to find errors and then export the values and proceed to fix the errors manually. This is time consuming and actually introduces risk into the process. The tool was designed to find and fix errors from the interface. The greater amount of time between error detection and error correction increases the probability that changes will have occurred to the source environment rendering the error data stale.

Most of what you’ll see are simple errors and only a fraction actually need analysis. Start by eliminating those errors for which there is no alternative and progress to those that require a decision. *Always remember that you can Undo an update.*

1. Sort by error type – Click on the column header to sort.

2. Fix single type errors first – Scroll to the type you want to begin fixing. Start with single value errors like “character” rather than multiple value errors like “length, format, topleveldomain, character” which may require further review.

3. Character – Do these first as they will comprise a large percentage of the volume while requiring little if any review. Character errors are invalid for the attribute checked and the update value shows them removed. Bulk select, mark them Edit, and Apply (hereafter designated as BEA).

4. Format – Single value errors of “format” that eliminate issues with white space, trailing periods, etc. Commonly found with mailNickName. BEA.

5. Domain and TopLevelDomain – If it’s for UPN then you need to fix them. If it’s for a proxyAddress then ask if the namespace will be used in the tenant. If not, then ignore them. If the customer has used a non-routable domain then this may form the majority of your errors. Think about whether the namespace will be used. If the anser is yes, then we can Export, do a bulk edit, Import, and Apply.

6. Simple multiple value errors – Next look at things like “character, localpart”. Most of these will have an obvious mistake with the suggested value eliminating the problem so BEA.

7. By now you’re down to a much smaller result set. Rerun your Query so that you can just see what’s left to fix.

8. Duplicates – If they are UPN’s then fix them. The suggested flag in the update column; e.g. (E), will use other attributes in the object to make a best guess. If they are proxyAddresses will the namespaces be used in the tenant? If not they can be ignored though it can help to eliminate future problems if you avoid synchronizing invalid data to the tenant.

9. At this point you should be down to a handful of errors. Sort and conquer.

10. Again, remember that if you make a mistake that you can Undo the update. All updates are logged twice. In the Verbose log and the Update file.

Based on past experience this process should only take a couple of hours for even inexperienced resources to complete. As you become more comfortable with the update suggestions you may choose to just Accept and Apply which will use all suggested values. It’ll get rid of a large number of the simple errors so you can focus on those that require analysis. Our experience has shown that this is correct more often than manual choices.

### Suggested Update Values

In past versions we have not been able to provide a suggested value for duplicate and format errors aside from removal of invalid characters. With this release there should now be only a small number of errors that do not have a suggested UPDATE value.

#### Suggestions for duplicates

Based on a check of other attributes associated with the object we can often determine an update to remediate the error. ***While these are usually better than what is in place only the user can make final determination of accuracy.***

Suggestions for pure duplicate errors will be preceeded by one of three values (suggestion flag), e.g. [E][john.doe@contoso.com](mailto:john.doe@contoso.com). Keep in mind that the suggestion flag will not be inserted in the directory. Only the value following the suggestion flag will be applied.

* **[C]** – suggested action COMPLETE. The value is probably correct and may not need to be edited.
* **[E]** – suggested action EDIT. The value should be changed to avoid conflict with another value in the forest.
* **[R]** – suggested action REMOVE. The value is a smtp proxy on a non-mail enabled object and can probably be safely removed.

**NOTE:**  *These suggestions apply to pure duplicate errors.*

#### Suggestions for format errors

The following errors have the suggested value assembled from layered checks.

* Rfc2822
  + topleveldomain – the top level domain is not internet routable; e.g. .local
  + domainpart – remove invalid characters
  + localpart – remove invalid characters
  + format – above 3 didn’t resolve the issue (valid characters used incorrectly)
* mailNickName
  + Remove leading or trailing periods

## Error Explanations

For details on the errors that apply to each attribute see the Supported Errors section in the Appendix.

### Character

The Value contains a character which is invalid. The suggested Update will show the value with the character removed.

### Format

The Value violates the format requirements for the attribute usage. The suggested Update will show the Value with any invalid characters removed. *If there are no invalid characters the Update and Value will appear the same*. It is up to the user to determine what they really want in the Update. For example SMTP addresses must comply with rfc 2822 and mailNickName cannot start or end with a period.

### TopLevelDomain

This applies to values subject to rfc2822 formatting. If the top level domain is not internet routable then this will be identified as an error. For example a smtp address ending in .local is not internet routable and would cause this error.

### DomainPart

This applies to values subject to rfc2822 formatting. If the domain portion of the value is invalid beyond the top level domain routing this will be generated.

### LocalPart

This applies to values subject to rfc2822 formatting. If the local portion of the value is invalid this will be generated.

### Length

The Value violates the length limit for the attribute. This is most commonly encountered when the schema has been altered. The suggested Update will truncate the value to the attribute standard length.

### Duplicate

The Value has a duplicate within the scope of the query. All duplicate values will be displayed as errors. The user can Edit or Remove values to eliminate duplication.

### Blank

The Value violates the null restriction for attributes to be synchronized. Only a few values must contain a value. The suggested Update will leverage other attribute values in order to generate a likely substitute.

### MailMatch

This applies to Dedicated only. The Value does not match the mail attribute. The suggested Update will be the mail attribute value prefixed by “SMTP:”.

# Appendix

## New Functionality in this Release

### Settings

All Settings are now available through a single dialog. The values shown are based on defaults pulled from the locally connected forest. Users can override with different values if desired.

### Multiple Forests

The ability to query against multiple forests is now supported. Uniqueness checks are applied against the total query results.

### Generic LDAP

Non-AD sources are now supported. The list of attributes and rules applied are the same as those supported for AD. Customization of the attributes included in the query are not supported.

### Ports

Port can be set to 3268, 389, or 636. The default value when the application is first started is 3268. This allows the query to return values from all trees in the default forest. While it is unusual for forests to contain more than one tree it does happen. You will notice that after updates are applied the port will automatically change to 389. This is because writes must be applied to the writeable naming context which does not support 3268 as a valid option. Port 389 is the default for generic LDAP queries and 636 can be selected if you require LDAP over SSL.

## Answers to Frequently Asked Questions

### Feedback

Bug reports and desired feature requests can be sent to [IdFixSupport@Microsoft.com](mailto:IdFixSupport@Microsoft.com) where it will reviewed. The address can also be found in a dialog box launched from the Feedback menu (smiley face) icon.

### Performance

IdFix performance will vary based on the hardware utilized and the network latency to the target server. Machines should have the minimum RAM specified and will benefit by using faster hard drives since temporary files are written to disk during the Query. High latency connections to a DC are discouraged and the best performance will be experienced by running the application directly on the target server.

### Number of errors shown

Customers with more than 50,000 errors returned faced the possibility of exceeding physical memory in attempting to display all data at one time. To alleviate this issue, errors are broken into blocks of 50,000. Exceeding the block size enables the More Errors options of View Next Block and View Previous Block.

### Temporary files

Large volumes of data may be parsed in the search for duplicate values. For instance a user may have up to six (6) attributes that must be checked and the proxyAddresses field can have many values. The duplicate check count may routinely exceed five (5) times the number of objects returned. For this reason, data must be written to disk to avoid the out of memory exception on most workstations. *Do not delete the temporary files while running.* This will trigger an exception and may cause unpredictable results.

### Directory Exceptions

There are 60 separate LDAP return codes and four (4) types of directory exceptions that can occur when contacting a directory server. These should be gracefully handled with a message box and an error written to the log. Client-server timeout is one example where the condition may be sporadic. *To alleviate this issue, the default LDAP timeout interval has been increased from 30 seconds to two (2) minutes.* This is a server side limitation, and the application respects all server side limits. If this should occur, then wait for a period of time when the GC is not so heavily utilized and/or launch the application from a lower latency location. For example, directly on a global catalog server.

### Don’t see updates in other domains

If the response to an update was COMPLETE, then the value has been applied to the directory. However, you may need to wait for replication to complete. Attempting to apply the update multiple times in a row may result in an exception stating the server is unwilling to process the request. Run Query again and you should observe the error has been resolved.

### FAIL (ACTION)

Extensive efforts have been made to make the schema and value limits of the Active Directory unobtrusive. With that caveat, it is still possible for the value entered in the UPDATE column to conflict with a directory rule within AD. If the ACTION value on a row turns to FAIL then there is an unknown conflict between the UPDATE column and the attribute values stored in the directory. These conflicts will require that the attribute values currently stored be examined more closely and may require ADSIEDIT in order to resolve.

### Double Byte Characters

IdFix has not been localized and double byte characters have not been tested in the application. Please send any errors of this type to [IdFixSupport@Microsoft.com](mailto:IdFixSupport@Microsoft.com) for further investigation.

### Sorting

The data columns can be sorted by clicking on the column header as is standard in dataGridView UX behavior. Clicking again will reverse the sort.

### Export Data

Exporting of data is facilitated via the Export icon.

### Import Data

The ability to Import a CSV file is now supported. This feature is a use at your own risk option. While we’ve created error and format handling functions in order to help populate the datagrid correctly there is no way to insure that incorrect errors are not introduced by manually editing the file.

Consider these best practice recommendations:

* Use Excel to view and edit the source file.
* Do not change the number of columns, headings, or any field values other than Update or Action.
* Do not save the file with any format other than CSV.
* Do not use escape characters in the field values.

### Multiple Forests - GAL Synchronization

If the customer has configure GAL synchronization between multiple forests then duplicate errors will be generated. For example, a user in Forest A has a corresponding contact in Forest B using the same mail and/or proxyAddress. Since the uniqueness check reports on the total query results these will be flagged as duplicates. There is no way for the application to know that this duplication is intentional versus an object that has unintentional duplication. It will be up to the user to recognize the scenario and ignore the error.

### Multiple Forests – Resource Forest Topology

A resource forest topology uses an authentication account in one forest to access a mailbox enabled account in another forest. If the messaging attributes are present on both objects then the application will return a duplicate error. For example, a user in Forest A has a corresponding mailbox enabled user in Forest B using the same mail and/or proxyAddress. Since the uniqueness check reports on the total query results these will be flagged as duplicates. It will be up to the user to recognize the scenario and ignore the error.

## Supported Errors

### Multi-Tenant Errors

* All objects

Well known exclusions

* + - Admini\*
    - CAS\_{\*
    - DiscoverySearchMailbox\*
    - FederatedEmail\*
    - Guest\*
    - HTTPConnector\*
    - krbtgt\*
    - iusr\_\*
    - iwam\*
    - msol\*
    - support\_\*
    - SystemMailbox\*
    - WWIOadmini\*
    - \*$
    - HealthMailbox\*
    - Exchange Online-ApplicationAccount\*

distinguishedName contains “\0ACNF:”

contains IsCriticalSystemObject

* DEPRECATED - c

the ISO3166-1 two letter alpha designation for country will be validated as well as the associated country name (co)

* DEPRECATED - co

the ISO3166-1 country name will be validated as wel as the associated two letter alpha designation for country (c)

* DEPRECATED - displayName

not blank

no questionable chars ? @ + \

less than 256

* DEPRECATED - givenName

no questionable chars ? @ + \

less than 64

* mail

rfc2822 & routable namespace (smtp only)

no duplicates

less than 256

* mailNickName

invalid chars whitespace \ ! # $ % & \* + / = ? ^ ` { } | ~ < > ( ) ' ; : , [ ] " @

may not begin or end with a period

no duplicates

less than 64

* proxyAddresses

DEPRECATED - invalid chars whitespace

rfc2822 & routable namespace (smtp only)

no duplicates

single value maximum number of characters: 256

* sAMAccountName (only if no userPrincipalName value)

invalid chars \ " | , / [ ] : < > + = ; ? \*

no duplicates

less than 20

* DEPRECATED - sn

no questionable chars ? @ + \

less than 64

* targetAddress

DEPRECATED - invalid chars whitespace

rfc2822 & routable namespace (smtp only)

DEPRECATED - no duplicates

less than 256

* userPrincipalName

invalid chars whitespace \ % & \* + / = ? ` { } | < > ( ) ; : , [ ] "

rfc2822 & routable namespace format

no duplicates

less than 64 before @

less than 256 after @

### Dedicated Errors

* All objects

Well known exclusions

* + - Admini\*
    - CAS\_{\*
    - DiscoverySearchMailbox\*
    - FederatedEmail\*
    - Guest\*
    - HTTPConnector\*
    - krbtgt\*
    - iusr\_\*
    - iwam\*
    - msol\*
    - support\_\*
    - SystemMailbox\*
    - WWIOadmini\*
    - \*$

distinguishedName contains “\0ACNF:”

contains IsCriticalSystemObject

* displayName

not blank (group)

no leading or trailing white space

less than 256

* mail

no white space

rfc2822 & routable namespace

no duplicates

less than 256

* mailNickName

not blank (contact and user)

invalid chars whitespace \ ! # $ % & \* + / = ? ^ ` { } | ~ < > ( ) ' ; : , [ ] " @

may not begin or end with a period

less than 64

* proxyAddresses

DEPRECATED - no leading or trailing white space

rfc2822 & routable namespace (smtp only)

no duplicates

single value maximum number of characters: 256

* targetAddress

not blank (contact and user without homeMdb)

DEPRECATED - invalid chars whitespace

rfc2822 & routable namespace (smtp only)

DEPRECATED - no duplicates

less than 256

value = mail (contact and user [if no homeMdb])