Kofax Communication Server

LDAP Directory Synchronization Technical Manual

Version: 10.2.0

KOFAX

© 2018 Kofax. All rights reserved.
Kofax is a trademark of Kofax, Inc., registered in the U.S. and/or other countries. All other trademarks are the property of their respective owners. No part of this publication may be reproduced, stored, or transmitted in any form without the prior written permission of Kofax.

CONTENTS

1. LDAP Dirsync

1.1 Background

Kofax Communication Server comes with an integrated multi-purpose directory. The directory is used for inbound routing of messages as well as for outbound addressing using short names. Use of the directory is optional but in most installations the key to tight, full featured integration with a wide range of email, ERP and collaboration platforms.

In order to make Communication Server as maintenance free as possible, Kofax offers Directory synchronization. Directory synchronization allows full management of directory information within the existing corporate meta-directory while leveraging the flexibility and benefits of the TCOSS directory.

Directories supported today include Novell Directory Server (NDS), Microsoft Exchange and Lotus Notes. Additionally open interfaces are provided to integrate Kofax Communication Server with virtually every existing directory, either via simple ASCII-file import, the ActiveX based TFC (Kofax Communication Server Foundation Classes) or, for host based applications, via IBM-MQ.

LDAP, the Lightweight Directory Access Protocol, has meanwhile established itself as the industry standard for searching and retrieving information from directories of different vendors.

Now that global corporations are more and more consolidating their directories, LDAP also becomes the protocol of choice for server to server directory integration. Both Microsoft Active Directory and iPlanet Directory Server (formerly Netscape Directory Server) use the LDAP protocol to replicate information between multiple sites.

With **LDAP Directory Synchronization** Kofax Communication Server now provides full support for **Microsoft Active Directory** and **iPlanet/Netscape Directory Server** as well as a solid basis for support of future LDAP based directories. Additionally, the import of LDIF files is supported.

Important! The Kofax Communication Server and its components formerly used the name TOPCALL. Some screen shots and texts in this manual may still use the former name.

1.1.1 General Information About LDAP

The LDAP information model is based on entries. A directory entry contains information about some object (e.g., a person). Entries are composed of attributes, which have a type and one or more values. Attributes hold information about a specific descriptive aspect of the entry. Each attribute has a syntax that determines what kinds of values are allowed in the attribute (e.g., ASCII characters, a jpeg photograph, etc.).

Entries are organized in a tree structure, usually based on political, geographical, and organizational boundaries. Each entry is uniquely named relative to its sibling entries by its relative distinguished name (RDN) consisting of one or more distinguished attribute values from the entry.

The directory schema is a database holding formal definitions about the attributes and object classes that can be used. Object classes define the types of attributes an entry can contain. Most object classes define a set of required and optional attributes.

The existing set of classes and attributes should meet the needs of most applications. However, the schema is extensible, which means that you can define new classes and attributes.

LDAP provides operations to authenticate, search for and retrieve information, modify information, and add and delete entries from the directory tree.

1.1.2 Unicode Support

The following dirsync types offer full Unicode support:

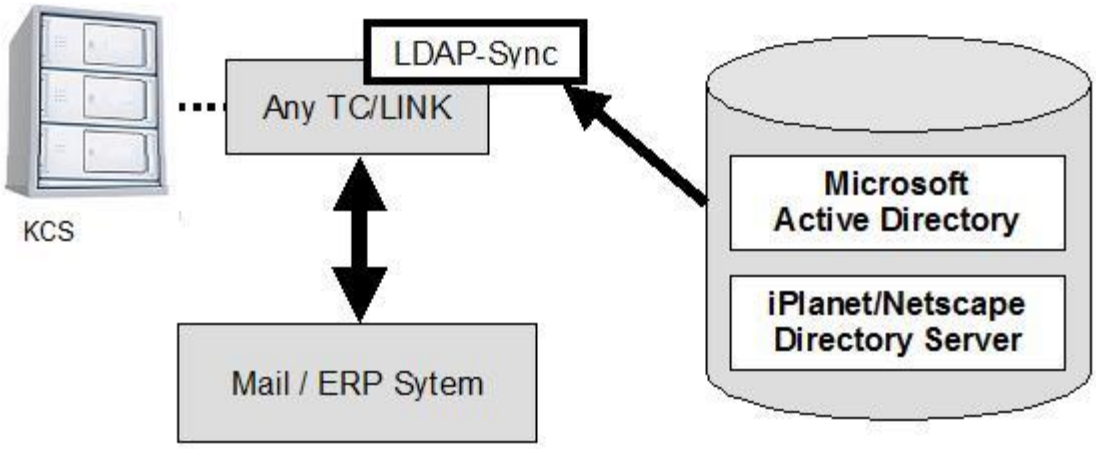
- Active Directory Dirsync
- LDIF Dirsync

See also: *Unicode Installation Guide*.

1.2 Benefits and Strengths

- Administrate the KCS user and recipient directory from within Microsoft Active Directory or iPlanet/Netscape Directory Server.
- This means: Single point of administration for all Unified Messaging (fax, voice, SMS, etc).
- Flexible mapping of fields/attributes from the LDAP directory to the KCS directory
- Optional use of custom fields for KCS specific attributes like cost center or default template (by extending the schema)
- Use LDAP directory synchronization together with any of the Mail or ERP environments currently supported by Kofax Communication Server (Lotus Notes, Microsoft Exchange, SAP, IBM-MQ, etc).

1.3 Structure of the Product



LDAP Dirsync is part of the Kofax Communication Server. TC/LINK can be configured to do an LDAP Dirsync instead of the native dirsync with the connected mail system. This means that any link type can be used for LDAP dirsync. Each TC/LINK instance can use its own LDAP dirsync options.

LDAP dirsync is implemented in a separate DLL, which is regularly used by TCLINK.EXE.

1.4 Functionality

- Automatically replicates users and recipients to the KCS directory.
- Supports standard KCS directory synchronization features:
  -> flexible mapping of attributes between KCS directory and LDAP directory, including concatenation of LDAP fields to single fields of the KCS user profile,
  -> configurable syntax for KCS user ids,
  -> configurable dirsync schedule (immediate or periodic)
- Supported in combination with any TC/LINK. During installation, LDAP synchronization for Microsoft Active Directory and iPlanet/Netscape Directory Server and LDIF Import can be selected as an alternative to native directory synchronization.
- Each TC/LINK installation can specify a unique LDAP directory server with fully independent configuration options.
- LDAP directory schema can be extended with KCS specific fields.
- Standard KCS link configuration and error handling mechanisms.

This documentation explains how LDAP dirsync leverages general TC/LINK dirsync features and gives details about LDAP directory specific dirsync implementations.

Features that are specific to Active Directory, Netscape/iPlanet Directory server or LDIF Import will be discussed in a later section of this document.

For a detailed description of standard TC/LINK dirsync, please consult the latest TC/LINK manual.

1.4.1 KCS Users and Recipients

LDAP dirsync can create two different types of KCS directory entries: users and recipients.

KCS users shall be created for LDAP directory entries that have a mailbox on a mail system that is connected to the Kofax Communication Server via TC/LINK. Thus, the mailbox owner can use standard KCS utilities to view the status of the send orders created on TCOSS, use default send options and a default coversheet, add documents from the FIS folder, receive Voice Mail in his mail inbox, access the TCOSS archive etc.

KCS recipients can be created for address book entries: People whom the customer can send messages, but who do not have a mailbox on the customer's mail system.

Please note that in standard installations it is sufficient to synchronize users only.

As LDAP servers are not necessarily connected to a specific mail server, TC/LINK offers a flexible mechanism to distinguish between users and recipients:

- 2 registry keys (*Dirsync**UserFilter*, *Dirsync**RecipientFilter*) allow to specify the LDAP filter used to query for users and recipients. Recommendations for the filter settings are part of the Directory server specific documentation. The filters must use LDAP search filter syntax (defined in RFC 2254).
- You can define separate dirsync templates for users and recipients (registry keys *Dirsync**UserTemplate*, *Dirsync**RecipientTemplate*).
- Synchronization of users can be enabled / disabled via registry key *Dirsync**UserExport*.
- Synchronization of recipients can be enabled / disabled via registry key *Dirsync**RecipientExport*.

Notes:

You might as well use these configuration keys to distinguish between two groups of users. In this case, you would configure two different filters and use two different KCS user profiles as templates. Although the registry keys are called "UserTemplate" and "RecipientTemplate", the actual type of the resulting KCS object depends on the type of the dirsync template.

It is possible to define the dirsync template separately for every LDAP directory entry: If registry key *Dirsync**TemplateAttribute* contains the name of an LDAP attribute, dirsync assumes that the dirsync template name is stored in this attribute. If the attribute is empty or does not exist for a certain LDAP directory entry, dirsync uses the template configured in *Dirsync**UserTemplate* or *Dirsync**RecipientTemplate* as a fallback.

1.4.1.1 Short Overview of the LDAP Search Filter Syntax

LDAP search filters use one of the following formats:

- <filter>=(<attribute><operator><value>)
- <filter>=(<operator><filter><filter>)

Some operators that are frequently used for search filters are listed in the following table:

=	Equal to
~=	Approximately equal to
<=	Lexicographically less than or equal to
>=	Lexicographically greater than or equal to
&	AND
|	OR
!	NOT

See RFC 2254 for full description (available at http://www.ietf.org/rfc/rfc2254.txt?number=2254).

1.4.2 Attribute Mapping

Attribute mapping is done via dirsync templates, as described in the TC/LINK manual. A dirsync template is a KCS user or recipient entry that holds placeholders for foreign directory attributes. A single TCOSS attribute may contain several placeholders. When dirsync creates a TCOSS object, the template is used as a basis and the placeholders are replaced by the real attribute values.

For performance and compatibility reasons, dirsync does not request all attributes from the LDAP directory. Instead, you must configure a set of required attributes, either via Setup or via a registry editor. The list of required attributes is stored in registry keys *Dirsync\List00* to *Dirsync\List99.*

These registry keys contain the LDAP display names of the attributes.

As a rule, you should only use LDAP attributes that are character strings.

If the LDAP attribute contains multiple values, LDAP dirsync only uses the first value. Exceptions to this rule may be defined in the directory server specific part of this documentation.

The LDAP attribute “name” cannot be used for dirsync, because the dirsync variable $name$ is reserved for the TCOSS user name.

Please consult the directory server specific chapters for information about allowed and recommended LDAP attributes.

1.4.3 Mail System

Every user / recipient on the Kofax Communication Server is marked as belonging to a mail system. Users created via a native TC/LINK dirsync belong to the mail system of the TC/LINK that created them (e.g. MS Exchange, Lotus Notes, etc.). With LDAP dirsync, the mail system of TCOSS users is not necessarily correlated with the link type. It is possible that the LDAP server holds a meta directory with users from different mail systems.

Therefore, LDAP dirsync takes the mail system from the field “user belongs to” defined in the dirsync template. In future versions of TCFW, additional mail systems will be implemented (e.g. X400, Internet, SMS).

As a side-effect of this solution, Dirsync may be unable to check if the mail system matches when a user is deleted: When the Directory server marks an entry for deletion, most attributes of the entry are removed (e.g. also the attribute holding the dirsync template name).

This implies that registry key *USRIO\ChangeAllUsers* must not be set to 0 if one link instance synchronizes users from different mail systems. Instead, set *USRIO\ChangeAllUsers* to 1 (dirsync ignores Dirsync Allowed flag and mail system of the KCS user) or 2 (dirsync ignores mail system only).

1.4.4 KCS User ID Syntax

The name of the KCS directory entries created by dirsync must be unique. It will be composed from attributes of the LDAP directory entry. You can either use a LDAP attribute that is guaranteed to have a unique value or choose a combination of LDAP attributes that is unique within the customer’s system.

The formula for creation of KCS directory entry names (user ID or recipient ID) is configured during Setup and is stored as a string value in registry key *Dirsync\UserIDFormula*. The string contains LDAP attribute names surrounded by brackets (e.g. [surname]). These attribute names are interpreted as placeholders for the corresponding LDAP attributes of the LDAP directory entry. All other components of the formula are used as they are.

Examples:

[surname] [initials]. [givenName]

[employeeID]/[department]-[company]

Which LDAP attributes are used in a specific LDAP directory depends on the Directory server and on the customer’s system architecture.

Normal attributes (like surname, employeeID etc) are not guaranteed to have unique values. It depends on the Directory server, which LDAP attribute is unique for a user.

Please consult the directory server specific chapters in this documentation for information about allowed and recommended LDAP attributes.

1.4.5 Dirsync Schedule

To keep the KCS user and recipient store consistent with the LDAP directory, it will be necessary to synchronize directory changes at regular intervals.

Setup offers two options for a periodic dirsync:

- Daily dirsync at a specific time (e.g. 3am)
- Dirsync at a specific interval (e.g. every 5 minutes).

The actual interval depends on message throughput (dirsync is not done while a message is being transferred).

Normally, periodic dirsync is an update dirsync: only changes after last dirsync are stored.

In some scenarios, it is necessary to have a periodic full dirsync. This is possible by setting registry key *PeriodicFull* to 1.

Immediate dirsync:

Additionally, TC/LINK can be configured to do an immediate dirsync. This can be either a full dirsync (all directory entries) or an update dirsync (request directory entries that were changed after the last dirsync).

If you choose an immediate dirsync in Setup, it will be done at the next TC/LINK startup. You can also force an immediate dirsync while TC/LINK is running, by setting registry key *Dirsync\Immediate* to 1 (full) or 2 (update). TC/LINK resets this registry key to 0 (no immediate dirsync) if the dirsync was successful.

Weekly full dirsync:

A weekly full dirsync can be configured. There is no dependency between this weekly dirsync and the other dirsync types.

Weekly full dirsync makes sense together with the FullDirsyncDeletes feature. You can choose one time interval per week, when a full dirsync is done and objects that went out of dirsync scope are automatically deleted. Use registry value *Dirsync\WeeklyFullAt* to define a time window, using the following syntax:

<DayFrom><HourFrom>-<DayTo><HourTo>

Possible values for <DayFrom> and <DayTo> are:

0	Sunday
1	Monday
2	Tuesday
3	Wednesday
4	Thursday
5	Friday
6	Saturday

<HourFrom> and <HourTo> specify hours from 00 to 23.

Examples:

600-023 dirsync during the weekend (between Saturday 00:00 and Sunday 23:59)

000-011 dirsync on Sunday morning (between 00:00 and 11:59)

After weekly full dirsync, TC/LINK stores the next possible full dirsync time (after the end of the current time window) in registry value *Dirsync\WeeklyDirsyncAfter*.

Setup does not create the registry values for configuring weekly dirsync, you must create the value WeeklyFullAt manually. Also, make sure that the value WeeklyDirsyncAfter does not exist. If the value exists but does not have the proper format (e.g., if it's empty), weekly dirsync will not start.

Syntax Check:

If configuration value Dirsync\WeeklyFullAt does not consist of two 3-digit numbers separated by a '-' character, TC/LINK disables the weekly full dirsync by setting the registry value to an empty string.

If the syntax is correct, but the values are incorrect (e.g. 700-024), TC/LINK uses the nearest valid value (e.g. 600-023 for the previous example).

1.4.6 Configuration

LDAP Dirsync options can be changed via a registry editor. All LDAP dirsync specific options are stored in a subkey Dirsync below the registry subkey of the link instance.

General registry keys for LDAP Dirsync (used for Netscape and Active Directory)

Registry Key	Type	Default	Description
Dirsync\Type	DWORD	0	0 = no dirsync (disables native dirsync for MX and LN 1) 1 = native dirsync (only valid for MX, LN, FI and MQ) 2 = Microsoft Active Directory 3 = iPlanet / Netscape Directory 4= LDIF Import
Dirsync\Immediate	DWORD	0	0 = no immediate dirsync 1 = immediate full dirsync 2 = immediate update dirsync
Dirsync\Periodic	DWORD	0	Intervals for update dirsync 0 = no periodic dirsync 1 = daily update dirsync 2 = periodic dirsync with shorter intervals
Dirsync\PeriodicFull	DWORD	0	0: periodic update dirsync 1: periodic full dirsync
Dirsync\Time	SZ	030000	Time for daily update dirsync (valid if Periodic is 1) and for update of TCOSS system files (if Topcall\UpdateSystemFiles = 1) Format: hhmmss
Dirsync\Interval	DWORD	300	Interval for update dirsync (in seconds) (valid if Periodic is 2)
Dirsync\LastDirsyncAt	SZ		Date and time of last dirsync, in syntax YYYYMMDD:hhmmss
Dirsync\LastUpdateSys	SZ		Date and time of last update of TCOSS system files (if configured)
Dirsync\UserExport	DWORD	0	1: synchronize users 0: do not synchronize users
Dirsync\UserTemplate	SZ		TCOSS template for users
Dirsync\RecipientExport	DWORD	0	1: synchronize recipients 0: do not synchronize recipients
Dirsync\RecipientTemplate	SZ		TCOSS template for recipients
Dirsync\TemplateAttribute	SZ		LDAP attribute containing the TCOSS template name (attribute contents overrides UserTemplate and RecipientTemplate)
Dirsync\UserIDFormula	SZ		Formula for KCS user id, can hold LDAP attribute names in [brackets] Default value depends on dirsync type. See below.
Dirsync\List01 to List99	SZ		Requested attributes (LDAP attribute names)
Dirsync\FullDirsyncDeletes	DWORD	0	Enable deletion of unused shadow users after every full dirsync
Dirsync\FullDirsync DeletesMailSystem	DWORD	0	Additional option, described in section 1.4.8
Dirsync\DLL	SZ	TCLAD or	Dirsync DLL base name (without extension and path). Must be in

[1] With FI and MQ, dirsync cannot be disabled.

		TCLPD	the TCLP working directory. Default value depends on dirsync type.
Dirsync\WeeklyFullAt	SZ		Specifies interval for additional weekly full dirsync Syntax: WHH-WHH (W = day of week, starting with 0 = Sunday) (HH = hour, from 00 to 23)
Dirsync\WeeklyDirsyncAfter	SZ		Time stamp written after weekly full dirsync. Tells TCLINK when the next check for weekly full dirsync is allowed. Used internally. This value is read during runtime.

Registry keys *Immediate*, *Periodic*, *Interval* and *FullDirsyncDeletes* can be changed at runtime. To make changes to other keys effective, you must restart the link.

1.4.7 Error Handling

The following errors may occur while writing a single user or recipient to TCOSS:

Code	Description	Remark	Standard Handling (LDAP Dirsync)
3501	Dirsync preparation error (e.g. memory allocation failure)		retry next DS time
3502	No name found in string		ignore
3503	No template found in string		ignore
3504	Template not existing		ignore
3505	Dirsync allowed flag not set		ignore
3506	wrong function (Modify, Add, Delete allowed)		retry next DS time
3507	Tried to touch user from different mail system		ignore
3508	obsolete	replaced by 3509 and 3510	
3509	Group not existing	new	retry next DS time
3510	Representative not existing	new	retry next DS time
3511	Connection to TCOSS lost	new	retry next DS time
3512	Maximum store capacity reached	new	retry next DS time
3513	Other TCOSS errors	new	retry next DS time

LDAP dirsync uses the standard TC/LINK error handling mechanisms:

All errors are logged to the application event log and written to the trace file. There is an individual event log warning for every failed user or recipient. Additionally, a final event log warning contains the number of errors.

Some errors are ignored by default: they are written to the event log but do not trigger a dirsync retry. Examples: dirsync not allowed for a user, different mail system.

Errors that are not ignored lead to a dirsync retry at the next configured Dirsync time (e.g. next day, or after the configured interval).

1.4.7.1 Option to Ignore Specific Errors

You can choose to ignore all errors mentioned above, by setting registry key *General\ReportDSErrors* to 0.

To ignore specific errors only, use the new registry key *Dirsync\IgnoredErrors* (REG_SZ). It contains a comma separated list of error codes that shall be ignored.

Default: errors 3502, 3503, 3504, 3505 and 3507 are ignored

Both options must be handled with care, because ignoring an error leads to a missing shadow user.

Errors that are not mentioned in the list (e.g. no dirsync license, LDAP server access problems) are not configurable and always lead to a dirsync retry.

If dirsync fails for any reason, TC/LINK still continues transferring messages.

Maximum diagnostic trace output will be available at trace level 100 decimal (registry key *General**Tracelevel*).

1.4.8 Automatic Deletion of Unused Shadow Users (FullDirsyncDeletes)

With registry key *FullDirsyncDeletes* set to 1, the full dirsync automatically deletes shadow users for mailboxes that went out of dirsync scope. This operation is done after every successful full dirsync (if no errors or only ignored errors occurred).

When you enable this option for the first time, you should perform the following steps:

- TC/LINK uses the link group and the date and time of the last dirsync to recognize which objects must be deleted. If several instances of TC/LINK are used for LDAP dirsync, check to which link group they belong (registry key *General**LinkGroup*).

  Using several links with identical dirsync settings is not recommended because this is unnecessary overhead. If, in spite of this, there are multiple links that do dirsync with identical settings, they must belong to the same link group, and the FullDirsyncDeletes feature must be enabled for all of them.

  If there are instances with different dirsync settings they must belong to a different link group, otherwise their shadow users may be deleted by mistake.

- Set registry key *Dirsync**FullDirsyncDeletes* to 1. You need not restart the link.

- Do a full dirsync by setting registry key *Dirsync**Immediate* to 1 (if there are multiple links with identical settings, you only have to do it in one instance). You need not restart the link.

After changing the dirsync scope or making large changes in the LDAP directory, you can trigger a full dirsync (and deletion of unused shadow users) by setting *Dirsync**Immediate* to 1.

When deleting a shadow user, TC/LINK writes the following event log entry:

Code	Severity	Description	Corrective Action	Parameters
5145	Information	Full dirsync deleted user / recipient %1.	This TCOSS object was deleted because it had left the dirsync scope.	%1: user/recipient ID

If the mail user entered the dirsync scope of another link, it will be subject of the other link's dirsync. The shadow user will not be deleted by the original link after the other link changed the object.

If both actions (link 1 deleting the user, link 2 updating it) occur simultaneously, one of them will fail.

In previous releases, LDAP full dirsync deleted even objects that were part of the dirsync scope but could not be changed for some reason (e.g. mail system changed, invalid group, dirsync not allowed).

Now, objects for who dirsync failed are not deleted. Instead, LDAP dirsync removes the "stamp" that marks these objects as dirsynced by this link group.

Additionally, users or recipients with "dirsync disabled" are not deleted.

If you copy a shadow user via TCFW (by changing the name of an existing shadow user), you should clear the "dirsync enable" flag, in order to prevent deletion of this user.

Special option for upgrade from Exchange 5.5 dirsync to Active Directory dirsync

If the position of users in the Exchange organization changes during an upgrade from Exchange 5.5 to Exchange 2000 or 2003, dirsync cannot correlate the existing shadow user profiles with the new users.

The old user profiles must be deleted. Up to now, it was not possible to delete them automatically, even if the "FullDirsyncDeletes" feature was enabled before and after the upgrade.

Now, a new dirsync option allows automatic deletion of all Exchange shadow user profiles that were created via dirsync and are not maintained by full dirsync anymore.

For this purpose, you must create the registry value *Dirsync\FullDirsyncDeletesMailSystem* (REG_DWORD) via a registry editor and set it to 7. (7 is the TCSI constant for the Exchange mail system). Additionally, registry value *Dirsync\FullDirsyncDeletes* must be set to 1.

When TCLINK encounters this situation after a full dirsync, it deletes all Exchange user profiles that were created by any link and were not part of this full dirsync, - of course only if dirsync is allowed for the user.

1.4.9 Creating Custom Attributes (Schema Extensions)

It is possible to add new object classes and attributes to the LDAP schema. In the context of LDAP dirsync, this may be needed if it is not possible to use existing user attributes for KCS user properties. For example, you could create an attribute that holds the TCOSS default template name.

The process of creating or modifying LDAP object classes and attributes is called “Extending the Schema”. This process is described in the Directory Server specific chapters of this document.

1.5 Prerequisites

Any TC/LINK plus either:

- Microsoft Active Directory (part of the Windows Server family)
- iPlanet/Netscape Directory Server version 4.1 or higher

Other LDAP servers may be supported in future versions.

See the TC/LINK manual for general requirements of KCS links.

LDAP dirsync needs a standard dirsync (TC/DS) license.

1.5.1 TCOSS Requirements for Large Synchronization Operations

The user store of the Kofax Communication Server has to be configured to maintain the required number of user entries. Use the TCDISK utility program to change disk space and allowed number of user entries.

There are also two entries in the common config parameters (sysconfig): In line 13, positions 5-8 the numbers of user and recipient entries are specified. In fact space for the KCS user-id is reserved for that amount of entries, so for long user-IDs as for the Directory Server distinguished names you should even configure more entries than you actual need. Keep also in mind, that for every user entry a recipient entry is generated.

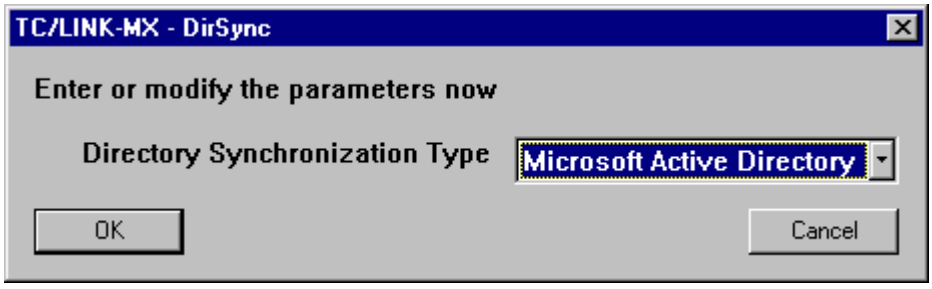
For more information please see the TCOSS System and Config Manual.

1.6 Installation

For installation, use the Kofax Communication Server Setup (Links group). During installation of any link type, an additional option is provided for configuration of Directory Synchronization.

This chapter contains only installation steps that are common for all LDAP servers.

1.6.1 Dirsync Type



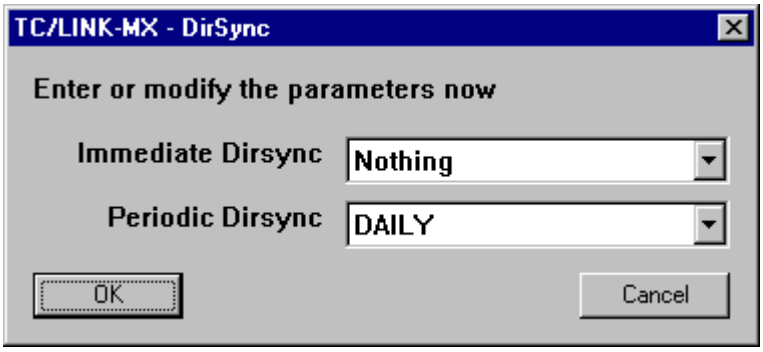
Directory Synchronization Type (registry: Dirsync\Type):

Available choices are:

- None
- Native
- Microsoft Active Directory
- IPlanet/Netscape Directory
- LDIF Import

Option Native will only have effect if the particular TC/LINK supports native directory synchronization (LN, MX, FI and MQ).

1.6.2 LDAP Dirsync Options



Immediate Dirsync (registry: Dirsync\Immediate):
Here you can order one immediate dirsync after the next start of TCLINK. Possible values:

- Nothing (default)
- Everything
- Changes

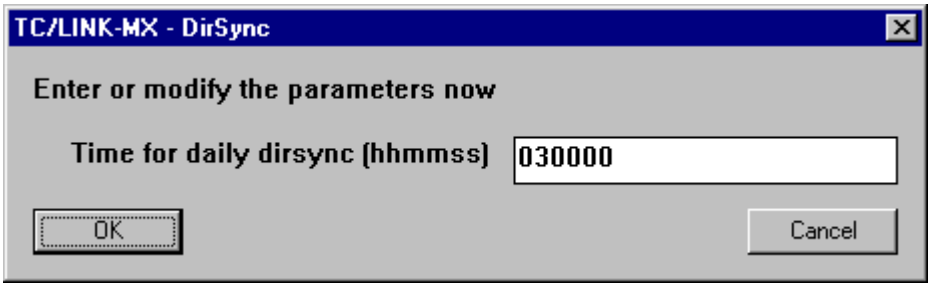
Periodic Dirsync (registry: Dirsync\Periodic):

Here you can configure a periodic update dirsync. Possible values:

- OFF (default)
- Daily
- Shorter Intervals

1.6.2.1 Daily Dirsync

If you selected a daily dirsync, a dialog box lets you enter the exact time of day:



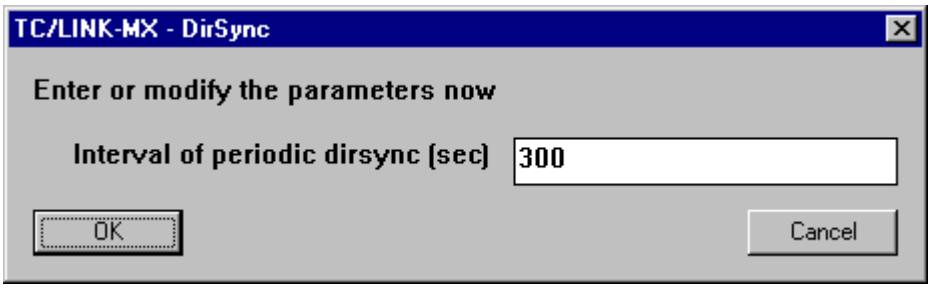
Time (hhmmss) for daily dirsync (registry: Dirsync\Time):

Enter a time (hh=hours: 00 - 23, mm=minutes: 00 - 59, ss=seconds: 00 - 59).

Daily update dirsync will take place at time specified here.

Default: 030000 (3am)

1.6.2.2 Periodic Dirsync with Shorter Intervals



Interval for periodic dirsync (sec) (registry: Dirsync\Interval):

Only valid if you selected shorter dirsync intervals. Please specify how many seconds TC/LINK shall wait between subsequent dirsyncs. The configured interval is not allowed to exceed 24 hours.

The actual interval used by TC/LINK depends on message throughput (no dirsync during message transfer). Default: 300 sec

Note: If TC/LINK is configured to update system files, this is by default only done once per day (at the time configured in DIRSYNC\Time, default is 3 am). The reason is that update of system files has a severe impact on TC/LINK performance. But you can force TCLINK to update the system files after every successful dirsync by setting registry value *Topcall\UpdateSystemFiles* to 2.

1.7 Compatibility

See prerequisites for supported directory servers.

1.8 Performance

- Min. 10.000 replications per hour (Mod 2xx-PRO, no other load on both KCS and LDAP server)
- Multiple TC/LINKs per server may be replicating different sub-trees of the master directory.
- Manual fail over required in case of hardware failure.

1.9 Conformance to Laws and Directives

Standard LDAP protocol is used for directory access and replication of information.

1.10 Restrictions

The actual synchronization algorithm is not part of the LDAP standard and therefore proprietary to each Directory Server. Currently Kofax Communication Server supports the proprietary LDAP synchronization protocols of Microsoft Active Directory and iPlanet/Netscape Directory Server. Support of other LDAP directory servers is optionally made available upon request.

1.11 Security Aspects

LDAP communication between Kofax Communication Server and directory server is via a standard TCP/IP connection within the corporate network. It also supports SSL/TLS connection encryption for active directory.

Login information required to gain access to the LDAP server is stored in encrypted form on the TC/LINK server. Access to the TC/LINK server is restricted via standard Windows logon. The server itself is normally located within a restricted area (server room).

1.12 Possible Future Enhancements

- Support of other LDAP directory servers

1.13 Further Documents

Common link configuration is described in the TC/LINK manual.

1.14 Implementation Issues

- Directory synchronization for each LDAP server is implemented in a separate DLL (TCLAD.DLL, TCLPD.DLL, TCLDIF.DLL)
- TCLINK.EXE loads the DLL according to the per instance TC/LINK configuration (registry)
- The interface between TCLINK.EXE and DLL's is described in the TC/LINK implementation description.

1.15 Deviations from IPD and / or Standard Requirements

Parallel synchronization of same directory subtree is possible for failover operation (same configuration!).

Fax pin code shall not be dirsynced (updated only via TCFW and TC/VoiceMail).

Active Directory: Creation of custom attributes not documented and not recommended.

2. LDAP Dirsync with Windows Active Directory

2.1 Background

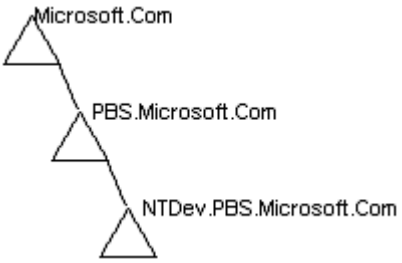
Active Directory is the directory service used in Windows and is the foundation of Windows distributed networks. Active Directory provides secure, structured, hierarchical storage of information about the interesting objects in an enterprise network; such as users, computers, services, and so on. The directory provides rich support for locating and working with these objects.

Active Directory is primarily a namespace, as is any directory service. A namespace is any bounded area in which a given name can be resolved. Name resolution is the process of translating a name into some object or information that the name represents. Active Directory forms a namespace in which the name of an object in the directory can be resolved to the object itself.

The Active Directory is physically stored on the domain controllers. Every domain controller holds a set of directory database partitions.

2.1.1 Domains, Domain Trees

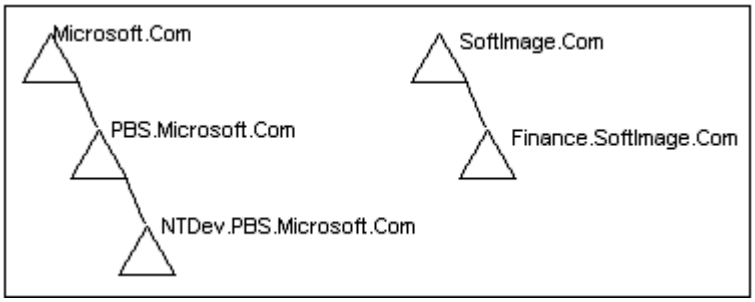
A domain is a single security boundary of a Windows computer network. Active Directory is made up of one or more domains. On a standalone workstation, the domain is the computer itself. A domain can span more than one physical location. Every domain has its own security policies and security relationships with other domains. When multiple domains are connected by trust relationships and form a contiguous namespace, you have a domain tree.



2.1.2 Forests

A forest is a set of one or more domain trees that do not form a contiguous namespace. There are trust relationships between all trees in a given forest.

The single domain controllers in the forest store only user profiles of their own domains, whereas Global Catalog Servers hold a directory with all user profiles of the forest (see section 2.1.4 for details). You can set up Active Directory Dirsync to work with single domains (1 link per domain) or with the complete forest (1 link connected to a Global Catalog server).



2.1.3 Domain Controller

A domain controller is a computer that is running Windows Server and hosts Active Directory. Domain controllers are responsible for authenticating domain user logons. A domain controller holds a writable replica of the following directory partitions:

- the Domain directory partition, which stores users, groups, computers and other objects for the local Windows domain. Updates to this partition are replicated only to domain controllers within the domain and (partially) to Global Catalog Servers (see below).
- the Schema container, which stores class and attribute definitions for all existing and possible Active Directory objects. Updates to this container are replicated to all domain controllers in the forest.
- The Configuration container, which holds information about sites, services, and directory partitions. Updates to this container are replicated to all domain controllers in the forest.

A Windows domain can deploy many domain controllers, and all domain controllers can accept Active Directory changes.

2.1.4 Global Catalog Servers

A Global Catalog server is a domain controller that stores the three writable directory partitions mentioned above, as well as a partial, read-only copy of all other domain directory partitions in the forest. This copy is called the Global Catalog (GC). It holds a replica of every object in Active Directory but with only a small number of their attributes. The attributes in the GC are those most frequently used in search operations (such as a user's first and last names or login names) and those required to locate a full replica of the object. The GC allows users to quickly find objects of interest without knowing which domain holds them and without requiring a contiguous extended namespace in the enterprise.

The first domain controller in a forest is automatically designated as a Global Catalog Server. Thereafter, another domain controller can be designated as a Global Catalog in the NTDS Settings Properties dialog box in Active Directory Sites and Services.

2.1.5 Active Directory Replication

Replication of updates is triggered when a user updates an object on a domain controller. When an update occurs, a timer is started and after a set period the (source) domain controller notifies the adjacent (destination) domain controllers. After being notified that there are changes, the destination domain controller contacts the source domain controller to request the changes.

To determine what changes need to be propagated to other domain controllers, Active Directory replication uses update sequence numbers (USNs). USNs are 64-bit numbers that are assigned by a counter that is local to each domain controller. Every attribute of every object in the Active Directory has its own USN number. An object's usnChanged attribute is the maximum local USN among all attributes of the object. The highestCommittedUsn attribute of a domain controller is the maximum local usnChanged among all objects stored in the Active Directory partitions of this domain controller.

All these USNs are local to the domain controller and are not replicated.

Therefore, it is meaningless to compare a USN assigned on one domain controller to a USN assigned on a different domain controller.

The up-to-date-ness vector is a value that a domain controller maintains for tracking the updates that are received from all other domain controllers. This vector contains the maximum USN number received from every source domain controller. When a destination domain controller requests changes for a directory partition, it provides its up-to-date-ness vector to the source domain controller. On the bases of this value, the source domain controller can determine if the destination has an up-to-date value for an attribute.

2.2 Functionality

2.2.1 Binding to Active Directory

Automatic lookup of domain controller:

With default configuration, Dirsync can use any domain controller of the local domain (i.e. the domain where the TCLINK.EXE process user belongs to).

If Dirsync shall import users from a different domain, you can configure the domain name in registry. TCLINK then uses only domain controllers from that domain.

You can also restrict Dirsync to using only a single domain controller.

At the first Dirsync after installation, a domain controller is selected according to configuration. After successful dirsync, the domain controller's name and other details (highestCommittedUsn, Invocation ID) are stored in the registry.

At every subsequent dirsync, TC/LINK tries to use the same domain controller. An update dirsync asks only for objects with a higher USN number.

If the previously used domain controller is not available, TC/LINK tries to connect to another matching domain controller. Dirsync keeps a list of already known domain controllers and their highestCommittedUsn numbers. When changing to an already known domain controller, an update dirsync asks only for changes that happened after the last contact with that domain controller. If this is the first contact to the domain controller, even an update dirsync imports all objects.

Specifying domain controller for dirsync:

In KCS Setup, you can optionally specify that only a single domain controller shall be used.

If a specific domain controller has been selected during Setup, dirsync will never try to locate a domain controller by itself, even if the specified domain controller is not available.

Credentials used for dirsync:

With default configuration, Dirsync uses the security context of the TCLINK process user.
When importing from a different domain or forest, you can configure the credentials to be used (domain, user id, password).

2.2.2 Dirsync Scope

AD dirsync can be done on a domain level, domain tree level, or global catalog level.

Domain level:

Users or recipients from a specific domain are synchronized.

All attributes can be used. Users from subdomains are not covered by dirsync.

Global Catalog level:

Users from the whole forest are synchronized.

The GC holds only a subset of attributes. A Kofax utility called "tcadutil" will be installed by Setup. You can use this utility to get a list of user attributes represented in the GC.

You can use the Active Directory Schema snap-in to add attributes to the global catalog. Nevertheless, you must be aware that this operation causes an immediate directory replication cycle, which may cause a lot of network traffic in a large organization. The Active Directory Schema snap-in can be installed from the Windows Advanced Server CD.

To search the global catalog, a domain controller containing a global catalog must be available in the LAN. If one is not available, dirsync is not possible.

Domain Tree level:

Users from a complete domain tree or from a specified Organizational Unit are synchronized.

This is implemented as a restricted search within the global catalog. Therefore, only the subset of attributes stored in the global catalog can be used. Additionally, dirsync is not possible if no domain controller holding a global catalog is available in the LAN.

2.2.3 KCS Users and Recipients

As a default, Active Directory dirsync creates KCS users for Exchange mailboxes and KCS recipients for Active Directory contacts (an equivalent to the custom recipients in former Exchange versions).

Nevertheless, you can use a completely different concept, by changing the LDAP filter expressions stored in registry keys *Dirsync\UserFilter* and *Dirsync\RecipientFilter*.

Default for *UserFilter*:

(|(mail=*)(proxyAddresses=*)(textEncodedORAddress=*))(&(objectCategory=person)(objectClass=User)(msExchHomeServerName=*))

Default for *RecipientFilter*:

(|(mail=*)(proxyAddresses=*)(textEncodedORAddress=*))(|(&(objectCategory=person)(objectClass=contact)))

For example, you can treat every Active Directory user as a “user”, by configuring *UserFilter* as:

(&(objectCategory=person)(objectClass=User))

You can also define additional subsets.

2.2.4 Server List

The native TC/LINK-MX dirsync algorithm offers an option to define a list of home servers. Dirsync ignores mailboxes from other home servers.

AD dirsync has a similar option. Registry key *Dirsync\ADServers* allows to specify a list of server legacyExchangeDN attributes.

Attention:

The complete legacyExchangeDN attribute of the server must be entered, e.g. :

“/o=E2KORG/ou=First Administrative Group/cn=Configuration/cn=Servers/cn=PCFS2000A”

2.2.5 Hidden Objects

By default, dirsync does not import objects hidden from the Exchange Global Address list. If hidden objects shall be imported, set registry value *Dirsync\ADSyncHiddenObjects* to 1.

2.2.6 Requested Attributes

You can use the utility “tcadutil.exe” (see 2.2.8) to get a list of possible attributes. With dirsync scope “Local Domain”, all attributes can be used. With all other dirsync scopes, you can only use attributes that are replicated to the Global Catalog (column “exported to GC” in the output of tcadutil.exe must be “yes”).

A special syntax can be used to retrieve a single email address from the multistring attribute proxyAddresses:

“proxyAddresses:<addresstype>” references the first email address with the given address type.

For instance, “proxyAddresses:SMTP” refers to the user’s first SMTP address

Attributes that are part of the KCS userid ($Name$ and all components of the *UserIdFormula*) or are used internally by TCLINK need not be specified in the *Dirsync\List* registry keys. They are requested automatically.

2.2.7 Globally Unique Identifiers (GUIDs)

With Exchange 5.5, the unique name of a mailbox was its distinguished name.

With Active Directory, the only object identifier that can never be changed is the object's Globally Unique Identifier (GUID). The GUID is a very large number that is created by the domain controllers. The algorithm used for GUID creation ensures that a GUID can never be created twice.

Using GUIDs also allows objects, such as domains, to be moved in the directory tree or forest.

Therefore, the typical Active Directory dirsync uses the GUID to locate existing shadow users and stores the string representation of the GUID as a correlation field in the KCS recipient store entry.

If multiple shadow users per Active Directory object are needed, you can configure a prefix for the correlation field, by using the registry value *Dirsync**CorrelFormula*. *CorrelFormula* and *UserIdFormula* have the same syntax. For example, two link instances might create separate sets of shadow users, with a link-specific prefix defined in *UserIdFormula* and *CorrelFormula*.

Link Instance	UserIdFormula	CorrelFormula
Link1	Link1-[cn]	Link1-[objectGUID]
Link2	Link2-[cn]	Link2-[objectGUID]

2.2.8 Utility "tcadutil"

Before running Setup, you should decide

- which Active Directory attributes shall be used in the KCS directory entries
  (if the scope is larger than the local domain, these attributes must be part of the Global Catalog)
- from which attributes the KCS user id shall be built
- which attribute holds a per-user template name (optional)

In order to facilitate these decisions, the KCS installs a console application called "tcadutil.exe". This application reads the Active Directory schema and enumerates all possible user attributes.

Additionally, it states whether an attribute is replicated to the global catalog, and whether it is indexed.

If you redirect the program's output to a file, you can create a CSV-file with all possible user attributes, and cut and paste attribute names into the Setup fields.

Called without a command line parameter, "tcadutil.exe" creates a comma-separated output like this:

```
attribute name, exported to GC, indexed
cn,yes,yes
```

Called with a command line parameter that specifies an existing user from the current domain, the output contains an additional column "Attribute value", holding the value for every attribute:

```
attribute name, attribute value, exported to GC, indexed
cn,Administrator,yes,yes
```

For a user within the "Users" container of the current domain, just specify the name of the user, e.g.:

tcadutil Administrator

Special characters: ,=+<>#;\

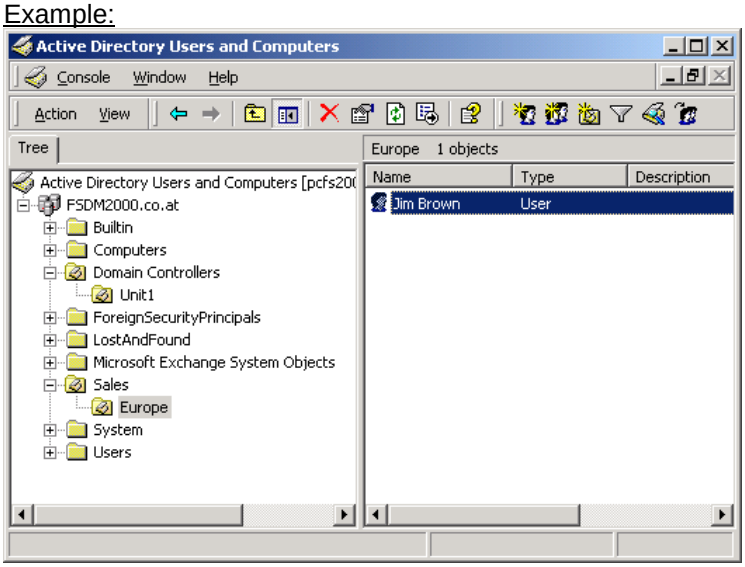
For user names containing one of the special characters, you must put a backslash '\' before the special character, e.g. "\+F" instead of "+F".

For a user that is not in the "Users" container of Windows Active Directory, you have to specify the location of the user within the domain using the following syntax:

CN=*UserName*,OU=*Container1*,OU=*Container2*

UserName and *ContainerX* are placeholders for the real values, the number of containers depends on the real directory structure.

Example:



User Jim Brown is a member of the organizational unit Europe. Organizational unit Europe itself is a member of the Sales organizational unit.

If “tcadutil” shall show the attributes for user Jim Brown, use the following command line:

tcadutil “CN=Jim Brown,OU=Europe,OU=Sales”

The parameter must be surrounded with double quotes, and there must not be any blanks between the components of the path. Use CN to specify the user name and OU to specify organizational units.

Please note that the Windows command prompt does not support all international character sets. If you redirect the output of tcadutil to a text file and open the file with Notepad, international characters will be displayed correctly.

2.2.9 Error Handling

AD dirsync will write events to the application event log for the following problems:

Errors:

- Invalid or missing registry keys
- No domain controller / global catalog server available
- Invalid LDAP filter string
- Missing access permissions to Active Directory
- Other errors (to be defined)

Warnings:

- The target domain controller is not available, dirsync is postponed

A detailed list of event log messages will be part of the final version of this document.

2.2.10 Configuration

AD Dirsync options can be changed via a registry editor. All LDAP dirsync specific options are stored in a subkey *Dirsync* below the registry subkey of the link instance.

Registry Key	Type	Default	Description
ADAllowOtherDC	DWORD	1	0: always use the same domain controller (ADDCName) 1: if access to DC specified in ADDCName fails, dirsync tries to locate another DC
ADBaseDN	SZ		Base node for dirsync (used internally). If the domain naming layout changes,

			you need to set this value to an empty string.
ADDCName	SZ		Fully qualified name of preferred domain controller.
ADDefaultNamingContext	SZ		Default value for defaultNamingContext property (MS ADAM only)
ADDomain	SZ		Fully qualified name of preferred domain
ADInvocationID	SZ		Used internally. If the domain naming layout changes, you need to set this value to an empty string.
ADPageSize	DWORD	100	used internally, do not change
ADPassword	SZ		Password of the user specified in ADUserID
ADPort	DWORD	0	Custom port used for LDAP access to MS ADAM
ADPreviousHighUSN	SZ		Used internally
ADScope	DWORD	0	0: synchronize with local domain 1: synchronize with Global Catalog 2: synchronize with domain tree (uses GC)
ADServers	MULTI_SZ		List of Exchange servers, specified by legacyExchangeDN. Makes only sense for Exchange mailboxes. Only mailboxes from the listed home servers are synchronized.
ADSyncHiddenObjects	DWORD	0	0: objects hidden from Exchange address list are not imported 1: objects hidden from Exchange address list are imported
ADTreeBase	SZ		Domain tree (only valid if Scope is 2), e.g. “DC=us,DC=kofax,DC=com” for subdomain us.kofax.com, “OU=sales,DC=us,DC=kofax,DC=com” for OU sales/us.kofax.com
ADUpgradeFromExch5	DWORD	0	If 1: Enables dirsync to convert existing Exchange 5.5 shadow users to Exchange 2000 shadow users.
ADUserID#	SZ		Specify a Windows user for dirsync, normally not needed format: DOMAIN\USER. But, if it is configured, it must always be in the DOMAIN\USERNAME format. **Note:** The distinguished name (DN) format (for example, “CN=SomeUser,CN=Roles,CN=dirsync,DC=kofax,DC=COM”) is not supported.
CorrelFormula	SZ	[objectGUID]	Formula for creating the shadow user’s correlation (unique ID)
DeletedFilter	SZ		used internally, do not change
ImportIfNameConversionFails	DWORD	1	If 1: objects are imported, even if the name cannot be converted without loss to the KCS character set If 0: objects are only imported if the name can be converted without loss
RecipientFilter	SZ		LDAP filter for Active Directory contacts Default is: (|(mail=*)(proxyAddresses=*)(textEncodedORAddress=*)) (|(&(objectCategory=person)(objectClass=contact)))
UserFilter	SZ		LDAP filter for Active Directory users Default is: (|(mail=*)(proxyAddresses=*)(textEncodedORAddress=*)) (&(objectCategory=person)(objectClass=User)(msExchHomeServerName=*))
UseridFormula	SZ	[cn]	Formula for creating the KCS user ID.
UseSecureConnection	DWORD	0	0: SSL/TLS support is disabled. 1: SSL/TLS support is enabled, configure ADPort accordingly

#: Configured ADUserID must be provided the access rights to the following containers:

- Read permissions for the rootDSE (to read the “dsServiceName” and “defaultNamingContext” properties)
- Read permissions for the “Configuration” Container to open the NTDS Settings container as specified under dsServiceName of the rootDSE (for example, LDAP: //desccm01.corp.hcstarck. com:389/CN=NTDS Settings,CN=DESCC01@ADAM-QS,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration) to check the invocationID
- Read permissions on the container from where the users are synchronized

A sub key *Dirsync\Servers* holds information about all domain controllers contacted during Dirsync. This information allows an incremental update dirsync when connecting to various domain controllers.
There is a sub key for every known domain controller, with the following fields:

Registry Key	Type	Default	Description
USN	SZ	0	Highest committed change number
InvocationID	SZ		Invocation ID (domain dirsync only)

2.2.11 Extending the Active Directory Schema

Extending the Active Directory Schema with new user attributes is possible, but not recommended, as it causes a lot of replication traffic between the domain controllers. It is recommended to use only the standard user attributes for dirsync.

2.3 Prerequisites

Information about supported operating systems and other requirements is available on the Kofax Support Web pages at www.kofax.com.

It must be possible to locate the target domain and at least 1 domain controller via DNS or local HOSTS file.

TCLINK must either run as a domain user, or you must specify the credentials of such a user in the LDAP Dirsync configuration. If configured to dirsync the local domain, this user profile must be a member of the local domain.

The mentioned user must have read access to the Active Directory, including the Deleted Objects folders. With standard settings, only members of the security group “Domain Admins” can read the Deleted Objects folders.

Note:

There is an alternative way of giving the link user access to the deleted items containers. With the DSACLS tool that is part of the Microsoft Remote Server Administration Tools (RSAT) Windows feature, any domain user can be given access to these containers, using the command line tool **dsacls**. For more information, see http://technet.microsoft.com/en-us/library/cc816824(v=ws.10).aspx. Here’s a brief overview of the necessary tasks.

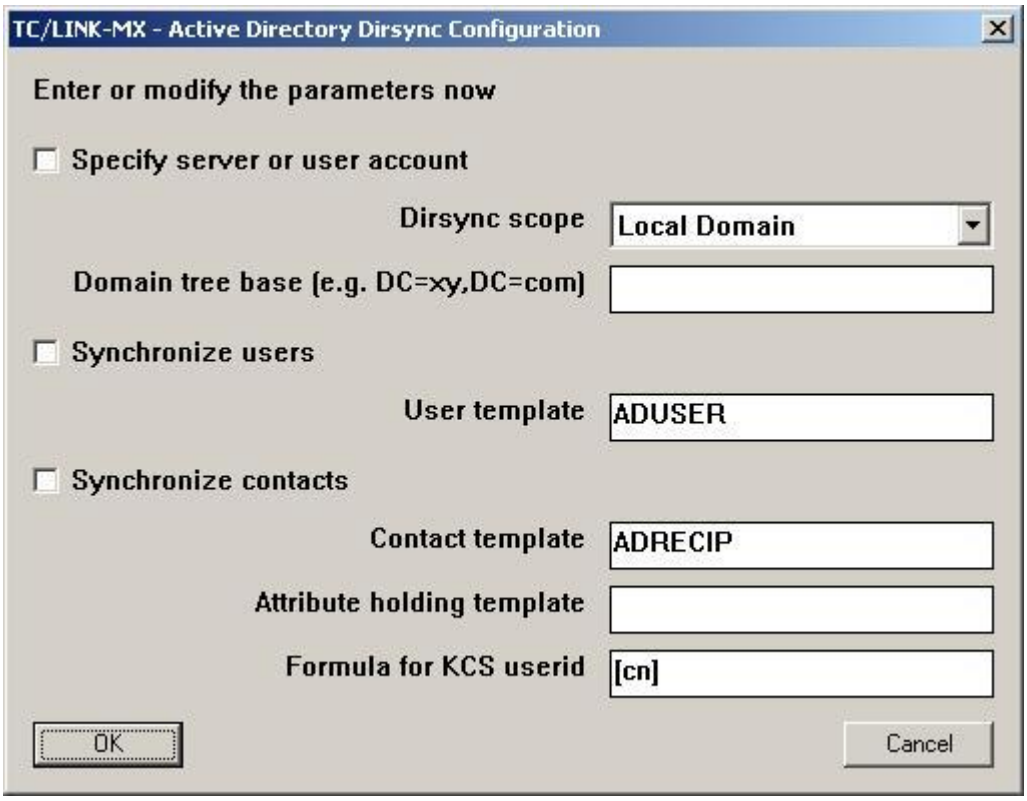
- Install the Windows feature “Remote Server Administration Tools”.
- Log in to the computer as a members of the Administrators group of the AD LDS instance.
- Start a command prompt as an administrator.
- Execute the following two commands (modified as explained below) for every domain in the forest:

```
DSACLS “CN=Deleted Objects,DC=DomainDistinguishedName” /takeownership
DSACLS “CN=Deleted Objects,DC=DomainDistinguishedName” /g DOMAIN\USER:LCRP
```

- Instead of the placeholders DomainDistinguishedName, DOMAIN and USER, use the following:
  DomainDistinguishedName: specify the full domain distinguished name, e.g. DC=kofax,DC=com
  DOMAIN: specify the domain of the link user (as in registry value Domain)
  USER: specify the user id of the link user (as in registry value UserId) or a security group where the user is member.

2.4 Installation

2.4.1 Active Directory Dirsync Configuration



Specify server or user account:
If selected, you will be prompted to enter which domain controller and which Windows domain user shall be used for dirsync.
This option is only needed if if TCLINK runs under a user account that is not a member of the Active Directory forest accessed by Dirsync (e.g. in an ASP environment).

Dirsync scope (registry: Dirsync\ADScope):
Choose the scope of directory synchronization (see section 2.2.2).

Possible values:
- Local Domain
- Global Catalog
- Domain Tree

Domain tree base (registry: Dirsync\ADTreeBase):
Only needed if scope is “Domain Tree”. Setup asks for the domain tree that shall be synchronized.

Synchronize users (registry: Dirsync\UserExport):
Choose if “users” shall be synchronized. See section 2.2.3 for a definition of the term “users”.

User template (registry: Dirsync\UserTemplate):
If users shall be synchronized, you can define here the default dirsync template for users. This default template can be overridden by a user-specific template configured via “attribute holding template”. Dirsync without a dirsync template is not possible. Default: ADUSER (belongs to Exchange)

Synchronize contacts (registry: Dirsync\RecipientExport):
Choose if “contacts” shall be synchronized. See section 2.2.3 for a definition of the term “contacts”.

Contact template (registry: Dirsync\RecipientTemplate):

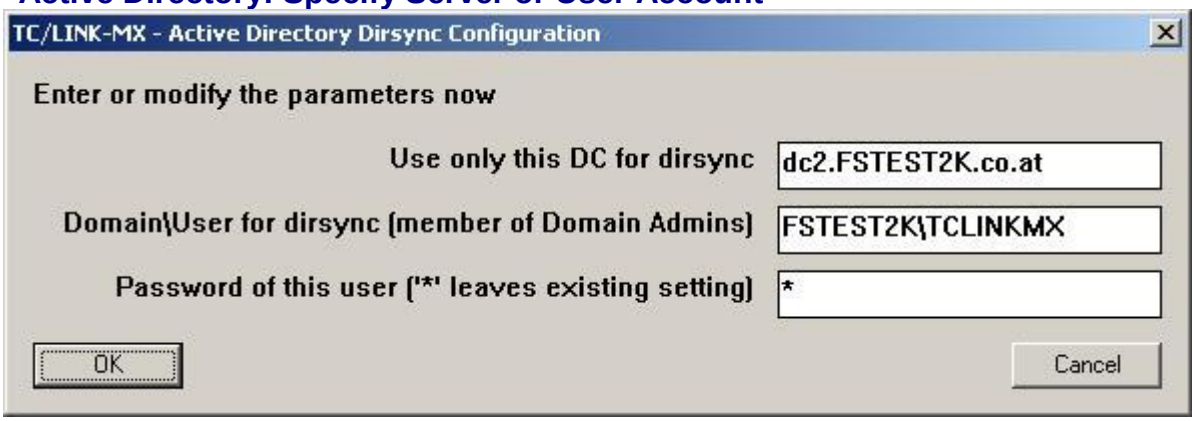
If contacts shall be synchronized, you can define here the default dirsync template for contacts. This default template can be overridden by a contact-specific template configured via “attribute holding template”. Dirsync without a dirsync template is not possible. Default: ADRECIP (belongs to Exchange)

Attribute holding template (registry: Dirsync\TemplateAttribute):
Here you can specify an Active Directory attribute that holds the dirsync template name. If this attribute exists and is not empty for a user (or contact), TC/LINK dirsync will interpret the attribute content as the dirsync template name for this object.
You can find out valid attribute names via the utility “tcadutil” which is part of the KCS (Links group).
Note:
For scopes other than “Local Domain” you can only use attributes that are part of the Global Catalog !
If the template holding attribute is not in the global catalog, dirsync will use the default template.

Formula for KCS userid (registry: Dirsync\UserIDFormula):
This mandatory input option defines how TC/LINK builds the KCS user ID of a shadow user. The user ID can contain various Active Directory user attributes. In this input field, you can specify any combination of fixed text and attribute names in [brackets].
You can find out valid attribute names via the utility “tcadutil”.
Note:
For scopes other than “Local Domain” you can only use attributes that are part of the Global Catalog !

Default:[cn]

2.4.2 Active Directory: Specify Server or User Account



This window appears if you selected “specify server or user account” in the general Active Directory dirsync configuration.

Use only this DC for dirsync (registry: Dirsync\ADDCName):
Specify the name of the domain controller, including the full domain name. Please note that the link computer must be able to find the IP address of this domain controller, either via DNS or via a local hosts file.

If you enter a value into this field, Setup also sets registry key *Dirsync\ADAllowOtherDC* to 0. This means that if this domain controller is unavailable, dirsync will not try to locate another domain controller.

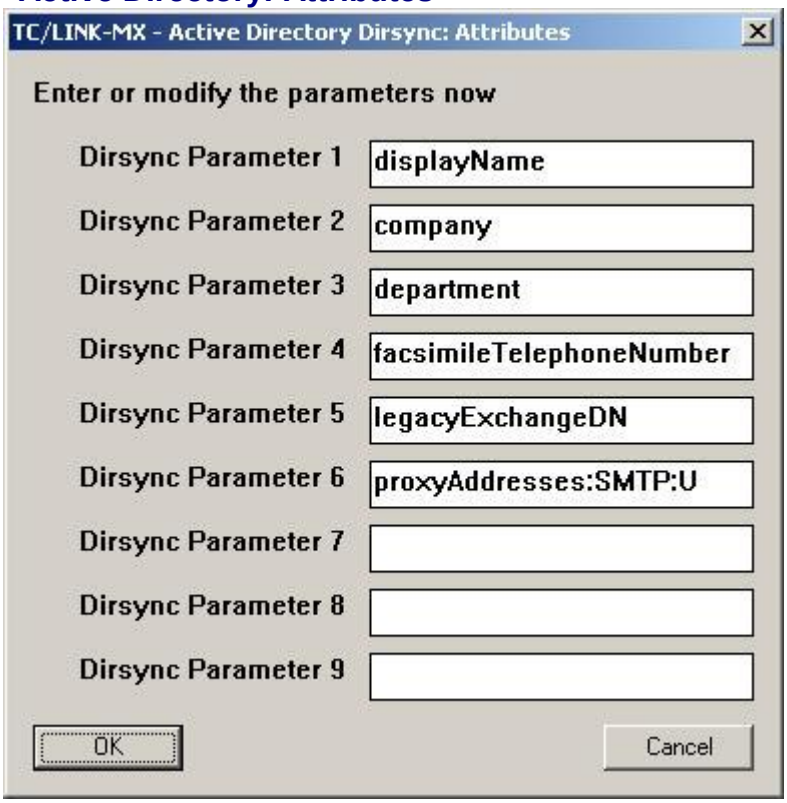
If the dirsync scope is NOT “Local Domain”, the specified domain controller must be a Global Catalog server.

Domain\User for dirsync (member of Domain Admins) (registry: Dirsync\ADUserId):
Enter the domain and user id of an account that has access to the Deleted Objects containers in Active Directory. This user must be in the same forest as the domain controller specified above.

Password of this user (“*” leaves existing setting) (registry: Dirsync\ADPassword):

Enter the password of this user. It will be stored encrypted.

2.4.3 Active Directory: Attributes



Use this setup page to define which Active Directory attributes are needed for dirsync. Setup allows to define up to 18 attributes as dirsync parameters (a second page is available). They are stored in the registry as *Dirsync\List01* to *Dirsync\List18*. If more attributes are needed, they can be entered manually via the registry editor (*Dirsync\List19* etc.).

For scopes other than “Local Domain” you can only use attributes that are part of the Global Catalog !

Please note that some attributes, e.g. legacyExchangeDN and proxyAddresses, do not exist for users without an Exchange mailbox.

Attribute names are case sensitive.

The attribute defining the KCS user name is requested automatically and need not be part of this list.

In the user template, the dirsync parameters can also be referenced via their sequential number, e.g. 1 instead of $displayName $.

Default: If Active Directory dirsync is installed for the first time, Setup configures a set of attributes corresponding to the ADUSER template installed by TC/LINK (see screen shot).

Notes :
If Active Directory dirsync is installed for the first time, TC/LINK installs a dirsync template user “ADUSER”. If this is an upgrade and a dirsync template user already exists, it is not changed.

2.5 Hints

2.5.1 Error After Domain Naming Layout Changes

If you change the domain naming layout in the active directory, you need to manually set the following two registry values to empty strings:

- Dirsync\ADBaseDN
- Dirsync\ADInvocationID

Without these changes, dirsync may fail with the error:

```
error 00000000 accessing property defaultNamingContext
```

2.5.2 Dirsync from Lightweight Directory Services

Active Directory Lightweight Directory Services (AD LDS) is a special mode of the Active Directory service that is designed for directory-enabled applications. The Lightweight Directory Access Protocol (LDAP) directory service runs as a user service, rather than as a system service. AD LDS does not require the deployment of domains or domain controllers. You can run multiple instances of AD LDS concurrently on a single computer, with an independently managed schema for each instance.

This section explains configuration changes for using TCLINK LDAP Dirsync with AD LDS.

Before Windows Server 2008, AD LDS has been called Active Directory Application Mode (ADAM).

Dirsync scope:
Only dirsync scope 0 (= Domain level) is supported, as there is no Global Catalog with AD LDS.

Directory server:
To avoid that dirsync contacts the nearest domain for information, configure the name of the directory server explicitly (registry value *Dirsync\ADDCName*) and disable the use of other directory servers (*Dirsync\ADAllowOtherDC* = 0).

After changing from a different directory server, delete registry value *Dirsync\ADBaseDN*.

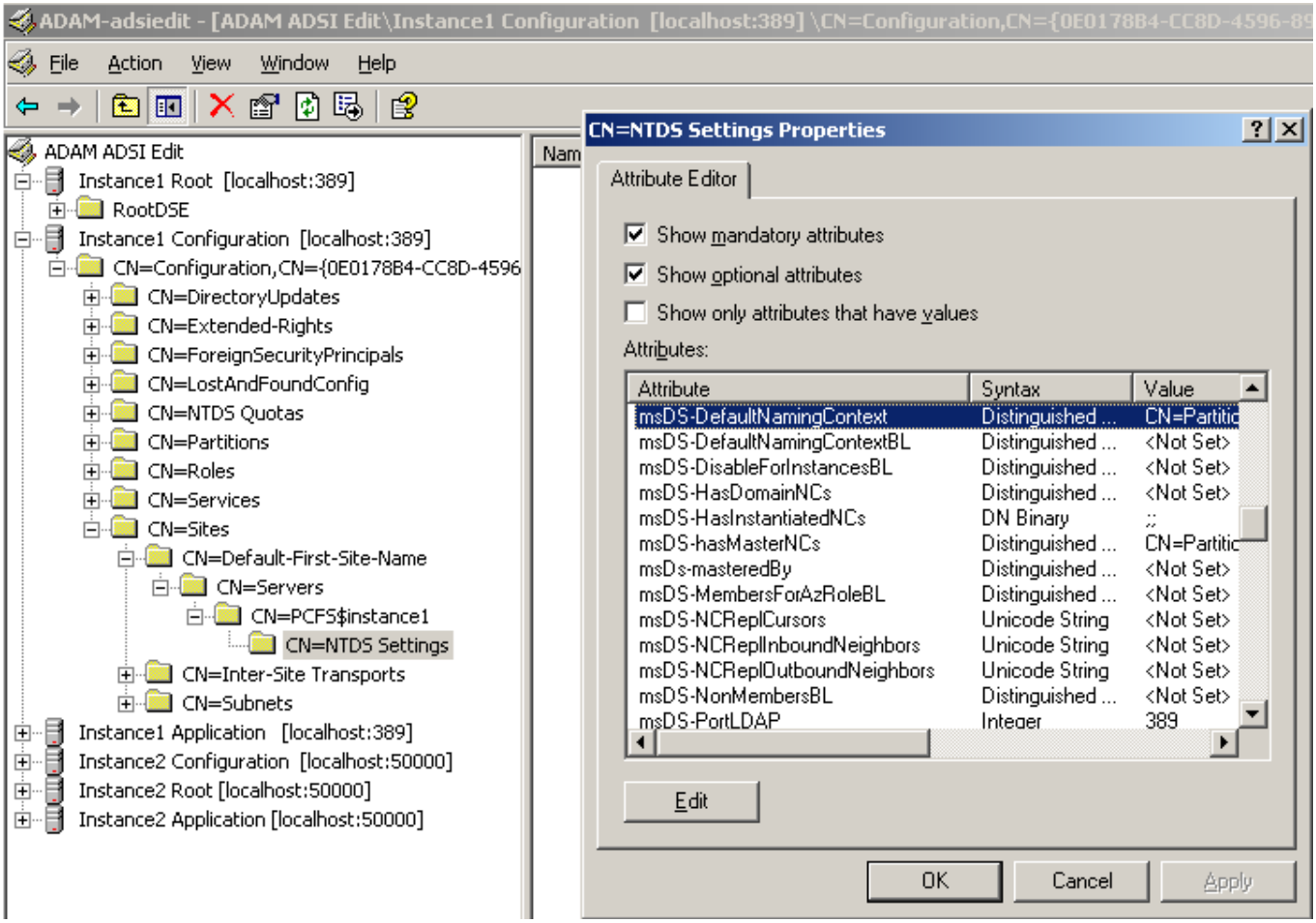
Port number:
AD LDS instances can use non-standard port numbers for LDAP access.
The port number must be configured manually in the new registry value *Dirsync\ADPort*.

Default naming context:
TC/LINK Active Directory Dirsync reads the default naming context property of the LDAP server. In a default AD LDS instance, this property is not defined.

You can define the default naming context in the AD LDS directory or configure a fallback value in the TCLINK registry.

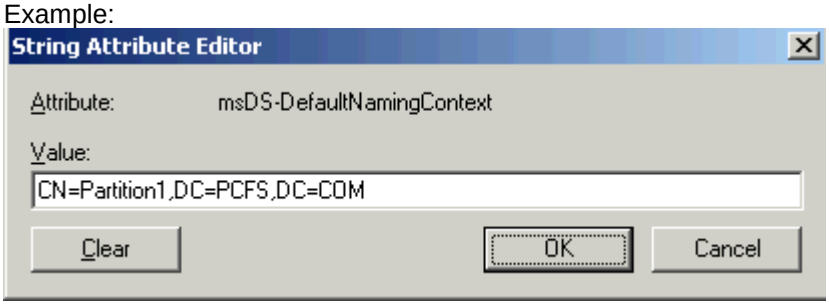
Defining a default naming context in AD LDS:

Using the tool AdsiEdit, edit the attribute "msDS-DefaultNamingContext" of the object "NTDS Settings" of the AD LDS server instance (see screen shot below).



Set this attribute to the distinguished name of the application partition where the users are stored.

Example:



Defining a default naming context in TCLINK configuration:

Use a registry editor to write the distinguished name of the application partition where the users reside into registry value *Dirsync\ADDefaultNamingContext*.

User filter changes:

Change registry value *Dirsync\UserFilter*. Probably, the AD LDS users will not have an Exchange home server and will therefore not be found with the standard dirsync filter.

To get all user objects, set the filter to (&(objectClass=user))

3. LDAP Dirsync Type LDIF Import

3.1 Background

The LDAP Data Interchange Format (LDIF) is a standard plain text data interchange format for representing LDAP directory content and update requests. LDIF version 1 is formally specified in RFC 2849.

The TC/LINK implementation of LDIF Import dirsync can therefore be used for all LDAP directories, provided that a tool for LDIF file creation exists.

LDIF conveys directory content as a set of records, one record for each object (or entry). It represents update requests, such as Add, Modify, Delete, and Rename, as a set of records, one record for each update request.

Note:
TC/LINK LDIF Import can only handle directory content records and Add records. Other update request record types (Modify, Delete, Rename) are NOT supported.

3.2 Functionality

3.2.1 LDIF Files

LDIF import dirsync reads LDIF files. The creation of these LDIF files is out of the scope of this document, and must be configured by the technician or customer. Most LDAP servers provide a tool for LDIF file creation, e.g. “ldifde” for MS Windows Active Directory.

3.2.1.1 LDIF Record Restrictions

Due to general restrictions of the TCLINK directory synchronization algorithm, only a subset of LDIF entries is supported:

- LDIF content
- LDIF change records of type “Add”

All other record types are ignored (e.g.: “Modify”, “Modrdn” and “Delete”).

Change log entries are not allowed in the LDIF file.

3.2.1.2 Character Set

As defined in RFC 2849, the LDIF file must use the UTF-8 character set (UTF-8 encoded Unicode). String attributes can be base64 encoded additionally. Binary attributes must be base64 encoded.

3.2.1.3 Other Restrictions

References to external files are not supported.
Any controls included in the LDIF file are simply ignored.
Language tags are not supported.

3.2.2 Interface Folders

Three different interface folders can be defined. All of them must be accessible by TC/LINK. The TC/LINK process must have permissions to read and delete files in this folder.

Note: The interface folders are NOT created automatically!

Registry Key	Default	Description	Used during
LDIFPath	C:\LDIF\Full*.ldif	Path to LDIF files for full dirsync	Full dirsync
LDIFPathUpdated	C:\LDIF\Updated*.ldif	Path to LDIF files with updated objects	Update dirsync
LDIFPathDeleted	C:\LDIF\Deleted*.ldif	Path to LDIF files with deleted objects	Both dirsync types

LDIF Import dirsync processes all files matching the path. If there are several files, the processing order is undefined. TC/LINK deletes each processed LDIF file.

When using the FullDirsyncDeletes feature, it is recommended to export all users into a single LDIF file.

TC/LINK opens each file for exclusive write access. Thus, the file can only be opened after it has been written completely, and it can only be opened by one process at a time.

3.2.3 Dirsync Types

As for other LDAP dirsync types, TC/LINK can be configured for full or update dirsync.

Depending on the dirsync type, LDIF dirsync polls different interface folders.

Full dirsync:
Full dirsync expects a single LDIF file containing all user entries. This is recommended for installations with a small number of users. With larger systems, full dirsync can last too long.

A simplified update dirsync can be implemented, if the update dirsync LDIF files contain only objects that were changed within a fixed period, e.g. during the previous day. Nevertheless, these LDIF files must contain the same set of attributes as full dirsync LDIF files.

Deletion of unused shadow users can be done in two ways:
After a full dirsync, via the automatic deletion of unused shadow users (FullDirsyncDeletes feature, see section 1.4.8).

In special scenarios, this can be done in an alternative way:

If the user entries on the LDAP server are not really deleted, but instead marked as unused via an attribute value, - or if they are moved to another container (while maintaining their unique user id). Then the deleted entries can also be exported to an LDIF file. For this purpose, KCS Setup lets you define a dedicated LDIF file path for deleted items (*Dirsync\LDIFPathDeleted*).

Ideally, the deleted objects are automatically removed after a time.

All LDIF files found at this place are considered as containing deleted users.

3.2.4 Dirsync Schedule

The time when TC/LINK polls the interface folder is defined by TC/LINK configuration.
Regular creation of LDIF files must be configured separately, e.g. via the Windows Scheduler.

3.2.5 Dirsync Scope and Filtering

TC/LINK LDIF Import handles all content records and “Add” records that can be found in the LDIF file. No additional filtering is done.

Any restrictions of the dirsync scope must therefore be done by the process that creates the LDIF file.

3.2.6 KCS Users and Recipients

TC/Link’s implementation of LDIF Import does not distinguish between user and recipient import. The type of the imported object depends on the dirsync template.

You can use an attribute to define the name of the dirsync template.

3.2.7 Requested Attributes

Make sure that all attributes specified in the TCLINK configuration are exported into the LDIF file!

There are several places in the TCLINK configuration where exported attributes are referred to:

*Dirsync**List01* to *Dirsync**List99:*
Only these attributes can be referenced in the dirsync template via their name or via their number.

*Dirsync**UserIdFormula:*
The user ID resulting from this formula can be referenced as dirsync variable $Name$.

*Dirsync**LDIFCorr*:
The value of this attribute is written into the TS_CORREL_1 field of the resulting TCOSS object. It is used as a unique identifier of this object.

*Dirsync**TemplateAttribute*:
The value of this attribute defines the dirsync template that will be used.

*Dirsync**LDIFBinary*:
This registry value holds a list of binary attributes that shall be converted into hexadecimal strings.

*Usrio**SignatureKey:*
This registry value holds the name of a binary attribute that shall be copied into the signature part of the TCOSS user profile.

*Usrio**MapObject1:*
The binary attribute specified here is copied into a configurable Map object of the TCOSS user profile.

All attribute names configured in the TC/LINK registry are treated in a case-sensitive way.

3.2.7.1 Binary Attributes

From the LDIF file structure, it is not clear which attributes contain binary data. Therefore, any binary attributes that can occur in the LDIF file must be defined in TCLINK configuration. There are three ways of handling binary attributes:

- The binary data can be converted to a hexadecimal string. Example: the objectGUID attribute in Active Directory is a binary unique identifier of an object. Active Directory dirsync converts it to a hexadecimal string and uses it for the corr parameter (stored in TS_CORREL_1 of the resulting TCOSS object). All attributes that shall be handled in this way must be defined in registry value *Dirsync**LDIFBinary*, which holds a comma-separated list of attribute names.

- A binary attribute holding a JPEG file can be converted into the signature of the resulting KCS user. The name of the attribute must be configured in registry value *Usrio**SignatureKey*.

- A binary attribute can be copied into the map object part of the resulting KCS user profile. Example: a public key used for email cryptography. The names of the attribute and of the corresponding TCOSS map object must be configured in registry value *Usrio**MapObject1*.

A single binary attribute can only be handled in one of these three ways.

3.2.7.2 Multi-Valued Attributes

The LDAP directory can contain multi-valued attributes. By default, only the first value becomes part of the dirsync string.

There are two exceptions of this rule:

- Binary map objects defined in the registry value *Usrio\MapObject1* can have multiple values, and each value is exported to a separate map field value.

- Multi-valued string attributes containing well-known prefix strings can be referenced in a special way within the Dirsync\List. An example is the Active Directory attribute proxyAddresses: Each value consists of an address type and an address, separated by a colon character, e.g.: *SMTP:user1@company1.com*

  In such cases, you can add the prefix to the dirsync list value, e.g.:
  Dirsync\List05="proxyAddresses:SMTP:"
  This will be translated into a dirsync string like the following:
  ….,proxyAdddresses:SMTP:=user1@company1.com,….

3.2.8 Synchronizing the KCS Signature Field

LDIF Import dirsync supports the synchronization of binary image data into the signature field of a TCOSS user, as described in section **Error! Reference source not found.**3.3.6.

3.2.9 Synchronizing Binary Data to the KCS Map-Object

LDIF Import dirsync supports the synchronization of binary data into KCS map objects, as described in section **Error! Reference source not found.**3.3.7.

3.2.10 Attribute Holding Unique ID

In order to check if there is already a shadow user for a dirsync item, the algorithm uses the dirsync line parameters Corr and Name: Corr is the mail-system specific unique ID of this user. Setup asks for this attribute when prompting for the "Attribute Holding Unique ID", and stores the attribute name in registry value *Dirsync\LDIFCorr*.

Ideally, this is an attribute that remains intact even if the user is renamed or moved to a different place in the directory.

With MS Windows Active Directory, the objectGUID attribute fulfills this purpose. For LDAP servers that lack a binary unique object ID, choose the dn attribute or leave this configuration item empty.

If item Corr exists, Dirsync searches for a KCS entry with this value (stored in the TS_CORREL_1 field of the address). If there is no Corr parameter or the search yields no results, Dirsync looks for a TCOSS entry with the specified name.

Note:
Section 3.2.3 describes a way of synchronizing deleted users via a separate LDIF file. If you use this option and deleted items are moved to a different container, you cannot use the "dn" attribute as a unique ID (it changes when the user is marked as deleted!).

3.2.11 Configuration

LDIF Import Dirsync options can be changed via a registry editor. LDAP dirsync specific options are stored in a subkey *Dirsync* below the registry subkey of the link instance. The following table holds configuration values specific to LDIF Import Dirsync.

Registry Key	Type	Default	Description
ImportIfNameConversionFails	DWORD	1	If 1: objects are imported, even if the name cannot be converted without loss to the KCS character set If 0: objects are only imported if the name can be converted without

			loss
LDIFPath	SZ	C:\LDIF\Full*.ldif	Path to LDIF files for full dirsync
LDIFPathDeleted	SZ	C:\LDIF\Deleted*.ldif	Path to LDIF files with deleted objects
LDIFPathUpdated	SZ	C:\LDIF\Updated*.ldif	Path to LDIF files with updated objects
LDIFBinary	SZ		Comma-separated list of binary attributes that shall be converted to hexadecimal strings
LDIFCorr	SZ	dn	Attribute holding a unique identifier for the object

The following additional configuration values below registry subkey Usrio are available for LDIF Import:

Registry Key	Type	Default	Description
SignatureKey	SZ		This is the name of the attribute on the Directory Server where the image data for the KCS signature image comes from.
MapObject1	SZ		Semicolon separated value that defines a binary attribute on the directory and the key part of the KCS Map-object: “<dir-attribute>;<tc-mapkey>”

3.2.12 Error Handling

The following error types are written to the application event log:

- Dirsync cannot start (event id 5750)
  The error reason (missing registry value, invalid UserIdFormula) is part of the event log record.
- Error building dirsync record (event id 5751)
  This event log entry is written if a single user cannot be imported, because the user id or the template name is missing. The “dn” attribute of the user is part of the event log record.
- No usable LDIF records in file (event id 5752)
  This event log entry is written if an LDIF file contains no valid LDIF records.

If dirsync cannot start because of a configuration error, all LDIF files remain intact.
If an error occurs while building a dirsync record, the LDIF file is deleted anyhow.

3.3 Installation

3.3.1 Configuring Automatic Creation of LDIF Files

You can use the Windows scheduler for triggering a periodic export of directory entries into an LDIF file.
Most LDAP servers include command line tools for LDIF export.
Example: ldifde for Microsoft Active Directory.

All filtering must be done during LDIF file creation. Typically, the LDIF export tool allows specifying a scope, a filter expression and a list of attributes to export.

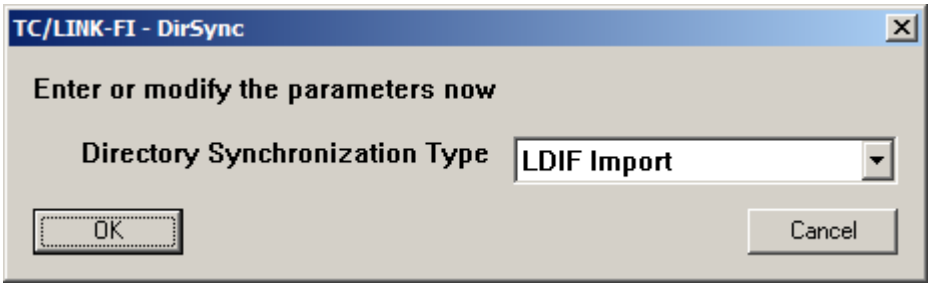
Take care that all needed attributes are exported.

The link process must have full access to the interface folders where LDIF files are stored. It is recommended to use folders on the link server.

3.3.2 KCS Setup

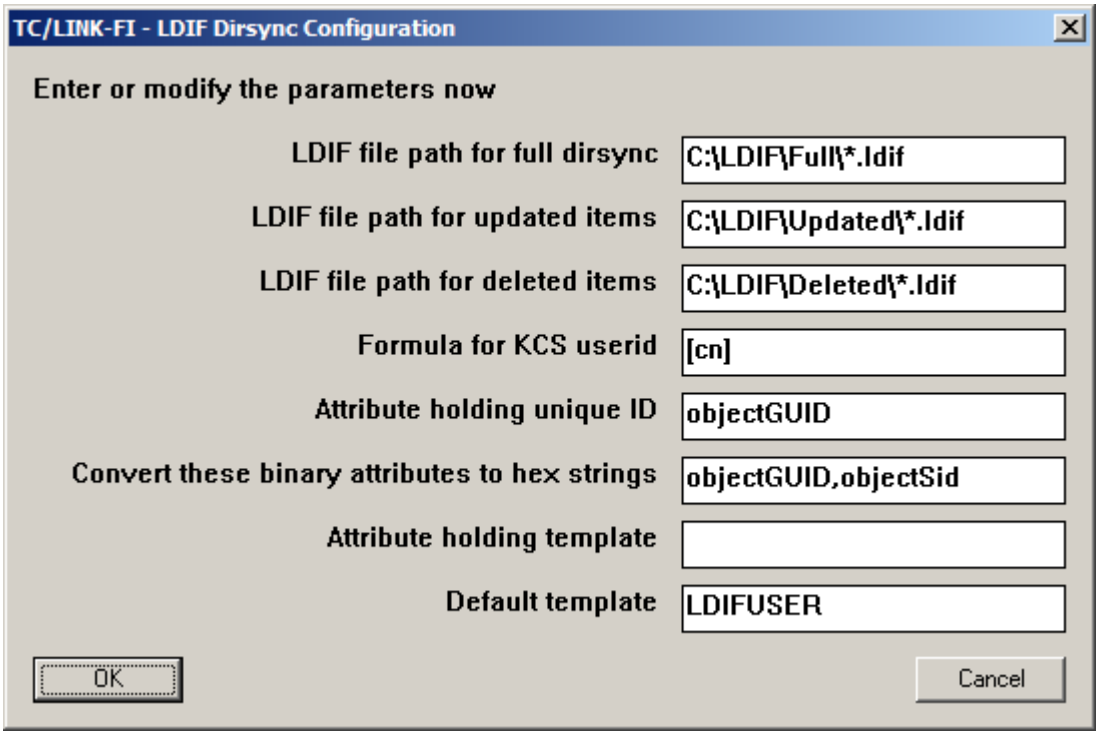
The sample screen shots in this section show a configuration that works with LDIF files from the MS Windows Active Directory.

Run KCS Setup (simple install or advanced install).



When asked for a directory synchronization type, choose “LDIF Import”.

3.3.2.1 LDIF Dirsync Configuration



LDIF file path for full dirsync (registry: Dirsync\LDIFPath):
Enter the full path name of the LDIF files. Wildcard characters ‘*’ and ‘?’ can be used in the file name part. The link process user must have full access to this path.
Default: C:\LDIF\Full*.ldif

LDIF file path for updated items (registry: Dirsync\LDIFPathUpdated):
This optional parameter is only used for the special handling of deleted items as described in section 3.2.3. Enter the full path name of the LDIF files for updated items. Wildcard characters ‘*’ and ‘?’ can be used in the file name part. The link process user must have full access to this path.
Default: C:\LDIF\Updated*.ldif

LDIF file path for deleted items (registry: Dirsync\LDIFPathDeleted):
This optional parameter is only used for the special handling of deleted items as described in section 3.2.3. Enter the full path name of the LDIF files for deleted items. Wildcard characters ‘*’ and ‘?’ can be used in the file name part. The link process user must have full access to this path.
Default: C:\LDIF\Deleted*.ldif

Formula for KCS userid (registry: Dirsync\UserIdFormula):

This mandatory input option defines how TC/LINK builds the KCS userid of a shadow user. In this input field, you can specify any combination of fixed text and attribute names in [brackets].
Default: [cn]

Attribute holding unique ID (registry: Dirsync\LDIFCorr):
Enter the name of an attribute that uniquely identifies an individual user on the LDAP server. If possible, choose an attribute that remains unchanged even when moving the user entry to a different container. With MS Windows Active Directory, the objectGUID attribute fulfills this requirement.

With other LDAP servers, you may have to choose the dn attribute, which has the disadvantage that it changes when moving the user to a different container.
Do not use dn together with LDIFPathDeleted.

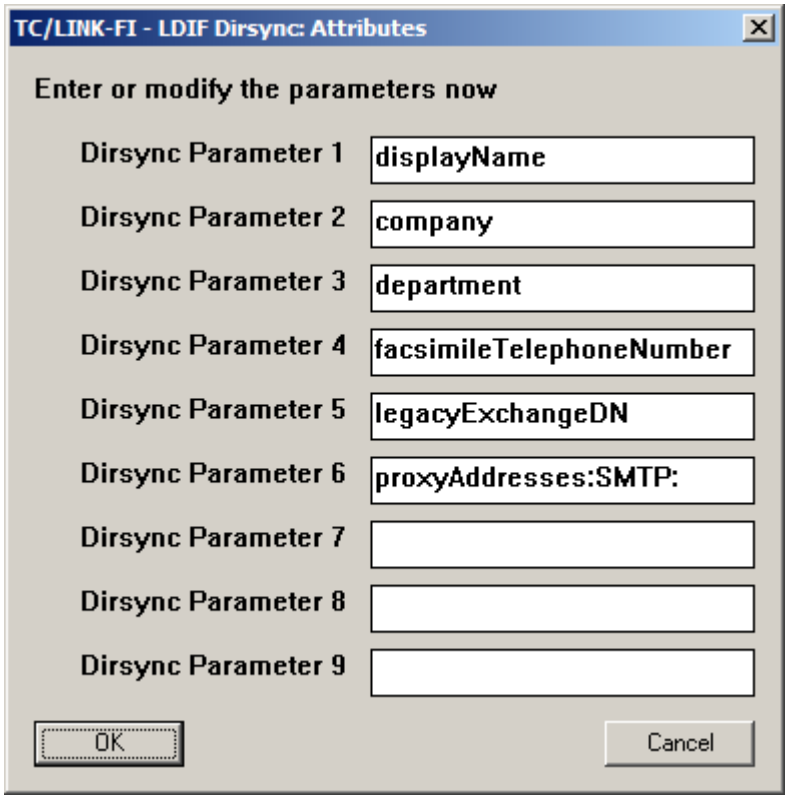
If you leave this field empty, the KCS user id is considered as the only unique ID.

Convert these binary attributes to hex strings (registry: Dirsync\LDIFBinary):
Here you can specify a comma separated list of binary attributes that shall be exported as hexadecimal strings. (This is how the objectGUID parameter is handled in Active Directory dirsync)

Attribute holding template (registry: Dirsync\TemplateAttribute):
Here you can specify an attribute that holds the dirsync template name. If this attribute exists and is not empty for an object, TC/LINK dirsync will interpret the attribute content as the dirsync template name for this object.

Default template (registry: Dirsync\UserTemplate):
This default template is used if there is no template specified via the configured TemplateAttribute. Dirsync without a dirsync template is not possible.

3.3.2.2 LDIF Dirsync Attributes



Use this setup page to define which attributes from the LDIF file are needed for dirsync. Setup allows defining up to 18 attributes as dirsync parameters (a second page is available). They are stored in the registry as Dirsync\List01 to Dirsync\List18. If more attributes are needed, they can be entered manually via the Windows registry editor (Dirsync\List19 to Dirsync\List99).

The attribute defining the KCS user name is requested automatically and need not be part of this list.

In the user template on Kofax Communication Server, the dirsync parameters can also be referenced via their sequential number, e.g. 1 instead of $displayName$.