INTEGRATING DYNAMICS CRM AND SHAREPOINT SECURITY

USING CONNECT BRIDGE

This whitepaper provides an overview of the CB Dynamics CRM - SharePoint Permissions Replicator and explains how it works. It describes the architecture of the solution and the mapping between the security model of Dynamics CRM and SharePoint.

Connecting Software s.r.o. & Co KG Connecting

HQ + Europe office

Handelskai 340

Vienna, 1020, Austria

office-europe@connecting-software.com

+43 (1) 370 72 00

Connecting Software Inc.

North America office

1776 S Jackson St, Suite 602

Denver, CO 80210, United States

office-america@connecting-software.com

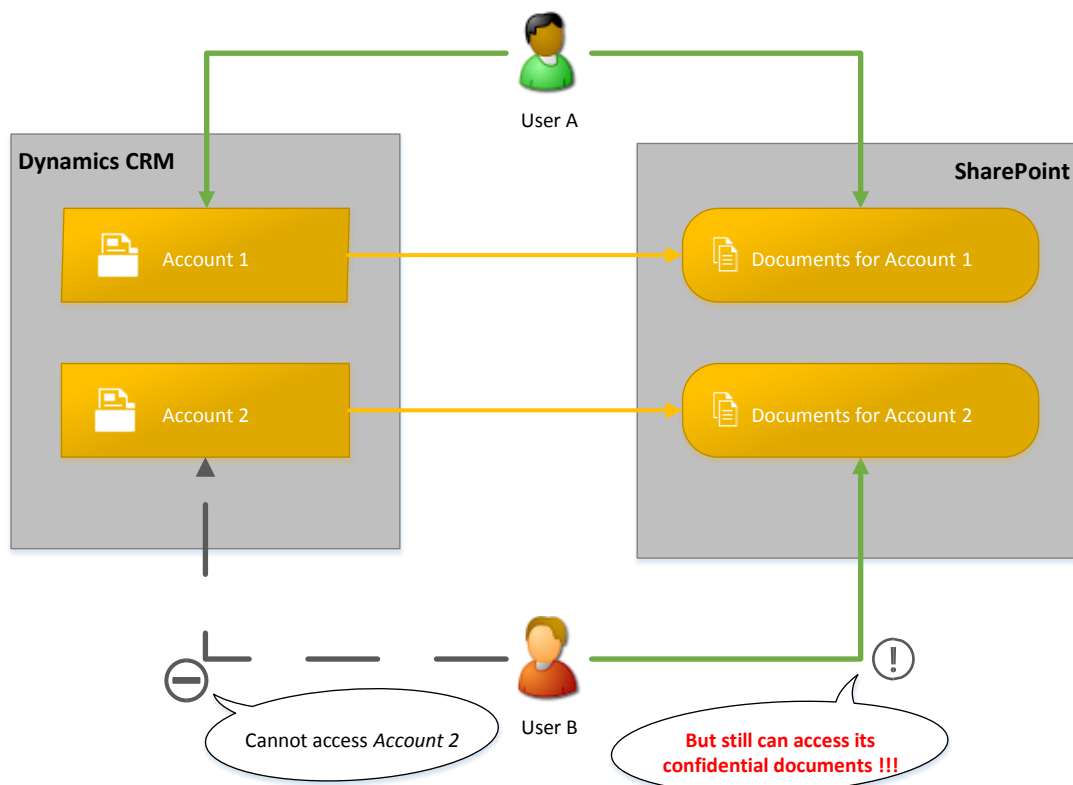+43 (1) 370 72 00 +1 (408) 768 8476

www.connecting-software.com

TABLE OF CONTENTS

INTRODUCTION

The standard out-of-the-box integration between Dynamics CRM and SharePoint is a very powerful feature that enables users to link their SharePoint documents with their CRM records. Moreover, users can manage SharePoint documents and use most of the SharePoint features directly from the CRM user interface. However, there is a limitation: the out-of-the-box solution lacks security integration. And the security models of Dynamics CRM and SharePoint differ significantly. The document capability of SharePoint is integrated into CRM but the security permissions of CRM into SharePoint are not.

User A

Dynamics CRM

Account 1

Account 2

SharePoint

Documents for Account 1

Documents for Account 2

Cannot access *Account 2*

User B

But still can access its confidential documents !!!

Dynamics CRM users can only see records and documents relevant to them. However, even a user with absolutely no rights to see documents for a particular entity in Dynamics CRM can see them in the SharePoint document library. The rights must be integrated in all cases.

Extending the scenario, a user shares a specific document with a colleague who has no rights for that specific record. This must be reflected in SharePoint as well. The standard out-of-the–box solution does not cover the examples above, or rights management at all.

Connecting Software provides a simple solution.

PRODUCT OVERVIEW

The CB Dynamics CRM - SharePoint Permissions Replicator (CB Replicator) covers the entire Dynamics CRM security model. It ensures that the proper user rights are applied to the SharePoint folders (files, libraries, sites, document sets). With this solution, users can be sure that each document in SharePoint will be accessible to exactly those users that have access to the respective record in Dynamics CRM. Any additional modification of the Dynamics CRM privileges for each record will be automatically applied to the permissions in SharePoint.
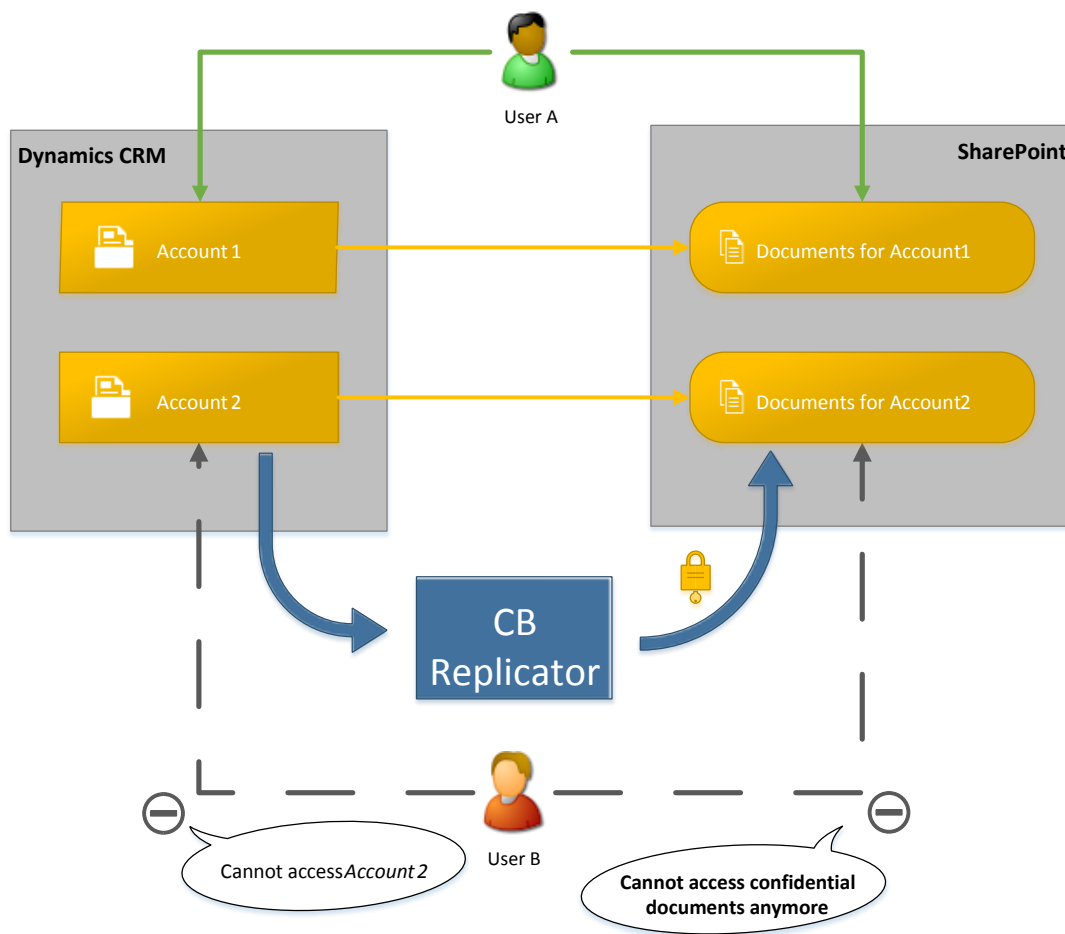
The CB Replicator consists of several components. These components interact together to achieve the desired results. The deployment is rather simple despite multiple components.

1.1 CB Replicator services

The *CB Replicator Core* and *CB Replicator Writer* are standalone services. They handle all the described application logic. The *CB Replicator Core* service opens WCF endpoint where Dynamics CRM can send notifications about the events. The service reads an event and compares the current vs. the expected permissions in SharePoint. If evaluated permissions do not match, it passes this information to the *CB Replicator Writer* service which writes the appropriate permissions into SharePoint.
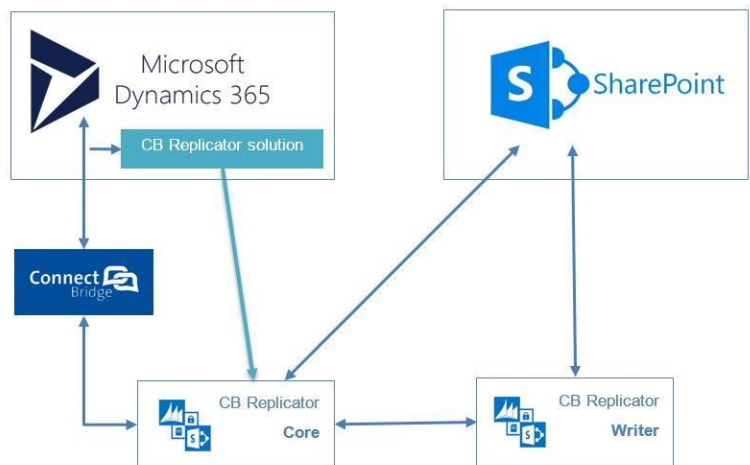
1.2 CB Replicator CRM solution

The purpose of this solution is to collect all the events that occur in Dynamics CRM that can possibly lead to permission replication request(s).

The solution consists of CRM plugin and custom entities to maintain events persistence and necessary configuration information. The managed solution is deployed directly into Dynamics CRM.

1.3 Connect Bridge platform

The CB Replicator uses the Connect Bridge platform to access Dynamics CRM and SharePoint. Connect Bridge has client server architecture and can be installed on the same machine as CB Replicator. For detailed information visit: https://www.connecting-software.com/connect-bridge/.

HOW IT WORKS

The CB Replicator brings everything in one package. It has been designed to cover various client scenarios.

2.1 Fully automated

The CB replicator is fully automated. There are no explicit user actions required to trigger permission replication. Users can concentrate on their work and CB Replicator, working in the background, will ensure confidentiality of their documents.

2.2 Event-based

A small CRM solution is deployed as a part of the CB Replicator. It automatically tracks/checks changes in Dynamics CRM. When a change occurs that requires security attention, it adjusts SharePoint permissions accordingly. The CB replicator supports following list of events:

- SharePoint Document Location
  - Create
  - Update
- User
  - Create
  - Update (manager, position)
  - Disable
  - Add role
  - Remove role
  - Change business unit
- Team (including access team and access team template)
  - Create
  - Delete
  - Add role
  - Remove role
  - Add member
  - Remove member
  - Change business unit
- Role
  - Create
  - Update
  - Delete
  - Add privilege
  - Remove privilege
  - Replace privilege

- Business unit
  - Create
  - Update
  - Delete
  - Disable
  - Change business unit
- Sharing (including cascading and reparent action)
  - Grant (share)
  - Modify
  - Revoke
- Change record owner
- Change status (statecode)
- Organization
  - Update (hierarchy security properties)
- Position
  - Create
  - Update
  - Delete
- Hierarchy security configuration (excluded entities)
- o Create
- o Delete

Enumerated events cover the entire security model of Dynamics CRM. Therefore, whatever the user does, the CB replicator always ensures proper permission mapping to the SharePoint document locations.

2.3 Support of all CRM entities

The CB Replicator works in a generic way with **any document enabled entity** in Dynamics CRM. Thus all the standard entities are supported, e.g. account, contact, opportunity, quote or invoice. Moreover, CB Replicator supports all custom entities.

2.4 Supported versions

Supported versions are Dynamics CRM 2011, 2013, 2015, 2016, Online, Dynamics 365 and SharePoint 2010, 2013, 2016, Online.

2.5 Absolute / relative document locations

The CB Replicator fully supports absolute and relative paths. Users can create document locations how they prefer – the CB Replicator supports both. Moreover, the service can work with SharePoint document location across different SharePoint sites and site collections.

2.6 User mapping

The CB Replicator maps users between CRM and SharePoint automatically based on their login names.

Additionally, it is possible to override or completely disable this behavior, and add custom mapping. Users can configure mapping, from any CRM user to any SharePoint user, or directory group.

2.7 Security model mapping

The CB Replicator breaks security inheritance in SharePoint and transfers the CRM security model as folder (document set), file, library or site level permission on specific items that are referenced by *sharepointdocumentlocation* record in CRM.

Permissions are mapped in one way: from Dynamics CRM to SharePoint.

There are significant differences between the Dynamics CRM and SharePoint security models so the complex permission mapping is required. In Dynamics CRM, we have several entities and actions that must be covered:

- User
- Team
- Access team
- Access team template
- Security role
- Business unit
- Sharing
- Privilege
- Privilege depth
- Hierarchy security (managers, positions)

The SharePoint security model provides only:

- Users
- Groups
- Security roles (Privilege levels)

 The CB Replicator maps target system security objects based on the following rules:

CRM		SharePoint
User (systemuser)	→	User
Manager	→	User
Team	→	Group
Access team	→	Group
Access team template	→	User / Group
Security role	→	Group
Business unit	→	Group (for default team)
Sharing	→	User / Group
Access right	→	Privilege level (configurable)
Position	→	Group

2.8 Access rights mapping

In Dynamics CRM there is a constant list of access rights that are mapped to dedicated SharePoint security roles (permission levels).

CRM access right		SharePoint permission level	SharePoint permissions
ReadAccess	⟶	cbreplicator_crm_ReadAccess	ViewListItems, OpenItems, ViewVersions, ViewFormPages, Open, BrowseDirectories, BrowseUserInfo, UseClientIntegration, UseRemoteAPIs, CreateAlerts
WriteAccess	⟶	cbreplicator_crm_WriteAccess	AddListItems, EditListItems, DeleteListItems, DeleteVersions
CreateAccess	⟶	-	
DeleteAccess	⟶	-	
AppendAccess, AppendToAccess, AssignAccess, ShareAccess	⟶	-	

This mapping is fully configurable so users can create custom mapping between CRM and SharePoint, including custom permission levels.

2.9 Multitenancy

With a single installation of CB Replicator users can configure the replication process for multiple Dynamics CRM instances. The CB Replicator also supports multiple SharePoint site collections for single Dynamics CRM organization.

2.10 Load balancing

Users can connect multiple *Writer service* instances to single CRM organization and create a load-balanced cluster to achieve a higher permission write rate.

2.11 Failover

The failover standby instance(s) can be connected to single CRM organization to fully take over the replication process in case of main instance failure.

SUMMARY

Many companies frequently use the out-of-the-box document integration between Dynamics CRM and SharePoint. Some of them are not aware of the security risk that stems from this integration. For other companies, the lack of this security integration is the reason why they decided not to use this integration.

The CB Replicator solves this missing security integration. It takes the CRM security model and converts it into SharePoint security model. The correct mapping between different models ensures that the same rights are applied to folders and underlying files in SharePoint for the same CRM record.

With the CB Replicator users can elevate the overall power of document integration without fear of possible security leaks and undesirable SharePoint data access.

CONTACTS

Connecting Software s.r.o. & Co KG Connecting

HQ + Europe office

Handelskai 340

Vienna, 1020, Austria

office-europe@connecting-software.com

+43 (1) 370 72 00

Connecting Software Inc.

North America office

1776 S Jackson St, Suite 602

Denver, CO 80210, United States

office-america@connecting-software.com

+43 (1) 370 72 00 +1 (408) 768 8476

www.connecting-software.com