Ensuring Consistency in Security Models:
Lessons learned with Microsoft Dynamics 365 and SharePoint

Whitepaper

Ana Neto
Connecting Software
ana@connecting-software.com

1. Executive Summary

Integrating Microsoft Dynamics 365 and Microsoft SharePoint enhances document management and collaboration. However, their differing security frameworks pose challenges in maintaining consistent user permissions, potentially leading to security risks and compliance issues.

This paper addresses the need to replicate the Dynamics 365 security model to SharePoint, ensuring a cohesive and secure environment. Key insights cover the differences between the security models of Dynamics 365 and SharePoint.

Practical steps for replication are outlined, from assessment and planning to mapping, tool selection, implementation, and validation. The use of both custom scripts and automated solutions like Connecting Software's CB Dynamics 365 to SharePoint Permissions Replicator are discussed.

A case study on Liebherr, a global manufacturer, demonstrates the successful replication of security models, resulting in improved document control, enhanced security, and reduced administrative burdens.

2. Introduction

Security is a critical consideration in managing and maintaining enterprise software solutions such as Microsoft Dynamics 365 and Microsoft SharePoint. Both platforms offer robust security models designed to protect sensitive data and ensure appropriate user access. However, the security frameworks of these systems are separate and distinct, which can create challenges in consistently managing user permissions across both platforms when they are integrated.

Companies frequently integrate Dynamics 365 and SharePoint to store documents in SharePoint, reducing Dynamics 365 storage needs and enhancing collaboration. However, the misalignment of the security models can create risks and compliance challenges.

Replicating the Dynamics 365 security model in SharePoint is crucial for a secure, cohesive environment. This whitepaper examines lessons learned and best practices for effective replication.

3. Understanding Dynamics 365 and SharePoint Security Models

Dynamics 365 Security Model

The security model of Microsoft Dynamics 365 is built around several key components:

- **Privileges**: Specific permissions that dictate the actions users can perform, such as reading, writing, deleting, or sharing records.
- **Roles**: These group together a set of privileges that reflect specific job responsibilities within the organization.

- **Teams**: Groups of users can be assigned roles collectively, which allows for easier permissions management.

SharePoint Security Model

The security model of Microsoft SharePoint comprises the following elements:

- **Permissions**: These are granular permissions that control access to sites, libraries, lists, and documents. Permissions include actions like view, edit, delete, and manage.
- **Permission Levels**: Predefined sets of permissions, such as Full Control, Contribute, and Read, that can be assigned to users or groups.
- **SharePoint Groups**: Collections of users that can be granted permission levels. Groups simplify the assignment of permissions to multiple users.

Comparative Analysis

While both Dynamics 365 and SharePoint offer sophisticated security models, their approaches are fundamentally different.

Dynamics 365 focuses on roles and privileges within the context of CRM records and operations.

In contrast, SharePoint revolves around permissions and permission levels to control access to content.

4. Business Case and Benefits

The integration of Microsoft Dynamics and SharePoint provided by Microsoft does not replicate the Dynamics 365 security model to SharePoint.

Nonetheless, there is a business need for replication, namely in terms of:

- **Enhanced Security**: Aligning security models across both platforms ensures that users have consistent and appropriate access rights, eliminating the risk of unauthorized access.
- **Compliance**: Privacy regulations and policies normally require that the owner of data (or documents containing data) knows exactly who can access that data. This is not the case for companies that only use the out-of-the-box integration by Microsoft.

5. Replication Tools and Technologies

Several tools and technologies are available to aid the replication process:

- **Custom Scripts**: Organizations with a development team and simple permission scenarios may create custom scripts to manage security model replication.
- **Out-of-the-box Solutions**: Solutions such as Connecting Software's CB Dynamics 365 to SharePoint Permissions Replicator automate the replication of security models between Dynamics 365 and SharePoint and can cover complex scenarios.

6. Step-by-Step Process for Replication

The process of replication involves a series of steps:

1. **Assessment and Planning**: Begin by assessing the current security models in Dynamics 365 and SharePoint. Define the requirements for replication.
2. **Tool Selection and Implementation**: Choose appropriate tools or develop scripts.
3. **Mapping Security Constructs**: If not using an automated tool, you must manually map all Dynamics 365 roles and privileges into SharePoint permissions and groups.
4. **Execution**: Perform the replication process, ensuring that security settings are accurately

mirrored in SharePoint. This will have to be repeated when permissions change.

5. **Validation**: If using custom scripts, thoroughly test the new security settings to ensure they match the Dynamics 365 model.

7. Case Study with an Out-of-the-Box Solution

Company Background

Liebherr is a global manufacturer known for high-quality machinery and appliances.

Problem Statement

Liebherr faced challenges managing document access across Dynamics 365 and SharePoint, as they realized all users could access Dynamics documents through SharePoint.

Solution Approach

By implementing Connecting Software's CB Dynamics 365 to SharePoint Permissions Replicator, Liebherr successfully replicated its Dynamics 365 security model to SharePoint.

Outcome and Lessons Learned

The solution ensured consistent access rights and enhanced security. As a result, Liebherr achieved better control over document access and ensured compliance with data protection regulations. The main lesson learned from this implementation is that you should always check access control is enforced after integrating different software.

8. Conclusion

Replicating the Dynamics 365 security model to SharePoint is essential for maintaining secure and compliant enterprise environments. This process addresses critical security concerns, ensuring that users have appropriate access rights while protecting sensitive data.

By following the outlined steps and leveraging appropriate tools, organizations can achieve a streamlined and secure integration, ultimately enhancing their overall security posture. The lessons learned from real-world implementations, such as the Liebherr case study, provide practical guidance for achieving successful replication.

9. References and Resources

Case Study: Improving Document Access at Liebherr

SharePoint Document Management Best Practices

Dynamics CRM Security Documentation

SharePoint Security Documentation

About Connecting Software

Connecting Software is an international company that provides integration, synchronization, and productivity solutions to a global customer base across sectors.

For more information, contact us via email at office@connecting-software.com or visit the page www.connecting-software.com/about-us.

Appendix - Glossary of Terms

Dynamics 365 Privileges: Specific permissions within roles.

Dynamics 365 Teams: Groups of users who work together and can own records and have specific security roles assigned to them.

RBAC: Role-Based Access Control

SharePoint Groups: Collections of SharePoint users with assigned permission levels.

SharePoint Permission Levels: Sets of permissions.