

RESTRICT ACCESS TO SHAREPOINT FILES VIA DOCUMENT EXTRACTOR TEMPORARY PUBLIC LINKS FEATURE

This white paper provides insights on how to restrict access to SharePoint files via Document Extractor Temporary Public Links feature.

**Connecting Software s.r.o. & Co
KG HQ + Europe office**
Handelskai 340 Vienna, 1020,
Austria
office-europe@connecting-
software.com +43 (1) 370 72 00

Connecting Software Inc.
4949 S Syracuse St, Ste 550
Denver, CO 80237
United States
office-america@connecting-software.com
+1 (720) 577-3030



www.connecting-software.com

All rights reserved. No part of the document may be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without the written permission of Connecting Software s.r.o. & Co. KG. Company or product names mentioned in this document may be trademarks or registered trademarks of their respective companies.

TABLE OF CONTENTS

TABLE OF CONTENTS

INTRODUCTION.....	3
HOW DOES IT WORK?.....	3
HOW CAN I BE SURE ONLY THE AUTHORISED USER CAN ACCESS THE FILE?	4
SECURITY CONSIDERATIONS FOR SHAREPOINT.....	4
SUMMARY	6
CONTACTS.....	6

INTRODUCTION

Document Extractor provides functionality called Temporary Public Links, which is intended as an enhanced security measure for providing restricted access to individual files in SharePoint without exposing access to any other files that have been stubbed into SharePoint from Salesforce.

This allows Salesforce users who do not have SharePoint accounts to access the files that they download from Salesforce.

This is also useful when Salesforce permissions are used to control which files different users, profiles or roles have access to. As these Salesforce permissions cannot be applied to SharePoint files, if the user is granted permission to the entire Document Library within SharePoint, then they would be able to see all files that have been stubbed from Salesforce, not just those to which their Salesforce permissions grant them access.

From the Salesforce user's point of view this is transparent. When they download a file from Salesforce they are redirected to that file in SharePoint, and they have the corresponding read or write access to it that they are granted through Salesforce. **The only thing they can NOT do is browse SharePoint to find other files; they must always start from Salesforce so that their permission to view the file can be confirmed by Salesforce before they are granted access to it.**

This grant of access lasts only as long as they have the file open in the SharePoint browser window. Once closed, they must return to Salesforce to download it again, if they require further access. Their Salesforce permissions will be re-checked at this time, in case they have been revoked or altered.

HOW DOES IT WORK?

Within Salesforce, a user will only be able to see files to which they have been granted access. The Salesforce permissions system is highly complex and there could be many reasons why a user may have access to a file. These are outside the scope of this document but remain unchanged by Document Extractor.

If a user has access to a file in Salesforce, they may download it. When this occurs, a request is made from Salesforce to the Document Extractor service. The request is made over https, and secured with credentials stored in a Named Credential within your Salesforce org. For Document Extractor SaaS, the request is made to our secure server hosted in Microsoft Azure. For Document Extractor OnPrem, the request is made to your own self-hosted Document Extractor server, using credentials which you have configured and generated yourself. The request will be made from Salesforce servers, so a firewall can

further be used to restrict incoming requests by IP address. Salesforce documents the IP addresses they may use here: <https://help.salesforce.com/articleView?id=000321501&type=1&mode=1>

Once Document Extractor receives and authenticates this request, it will use the SharePoint API to generate an anonymous public sharing link. **The link will have a short expiration time (5 minutes). This link is not guessable or discoverable and is passed back directly to Salesforce.** Salesforce redirects the user to this address, at which point SharePoint will perform a further redirection to the desired file.

HOW CAN I BE SURE ONLY THE AUTHORISED USER CAN ACCESS THE FILE?

The following are the reasons why only an authorized user can access the file:

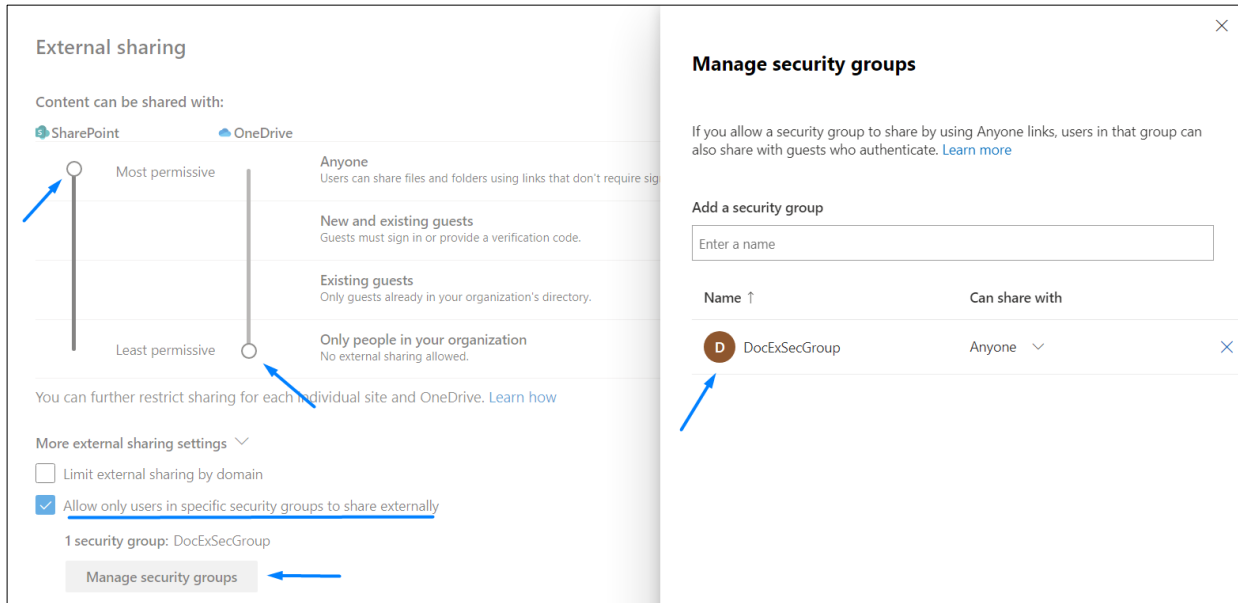
- The user opening the file never sees the anonymous link itself
- The link will expire within 5 minutes, so even if an insider-threat user does obtain the link, they would have only a short window of time to give it to anyone else before it expires.
- The link only provides access to that single file, to which the user already has authorised access via Salesforce. They could equally well download a copy of the file and exfiltrate that.
- Access to shared links is logged by SharePoint, so the IP address and time of any access to the document may be audited.

SECURITY CONSIDERATIONS FOR SHAREPOINT

For Document Extractor to be able to generate these temporary public links, SharePoint must be configured to allow their creation. To do this, there are two configuration settings that may need to be set.

Firstly, external sharing must be allowed at the organization level: <https://docs.microsoft.com/en-us/sharepoint/turn-external-sharing-on-or-off>.

This must be set to allow sharing to “Anyone”, to allow access to users without requiring them to have SharePoint accounts.



External sharing

Content can be shared with:

- ☒ SharePoint
- ☐ OneDrive

Most permissive

Least permissive

Anyone
Users can share files and folders using links that don't require sign-in.

New and existing guests
Guests must sign in or provide a verification code.

Existing guests
Only guests already in your organization's directory.

Only people in your organization
No external sharing allowed.

You can further restrict sharing for each individual site and OneDrive. [Learn how](#)

More external sharing settings

- ☐ Limit external sharing by domain
- ☒ Allow only users in specific security groups to share externally

1 security group: DocExSecGroup

[Manage security groups](#)

Manage security groups

If you allow a security group to share by using Anyone links, users in that group can also share with guests who authenticate. [Learn more](#)

Add a security group

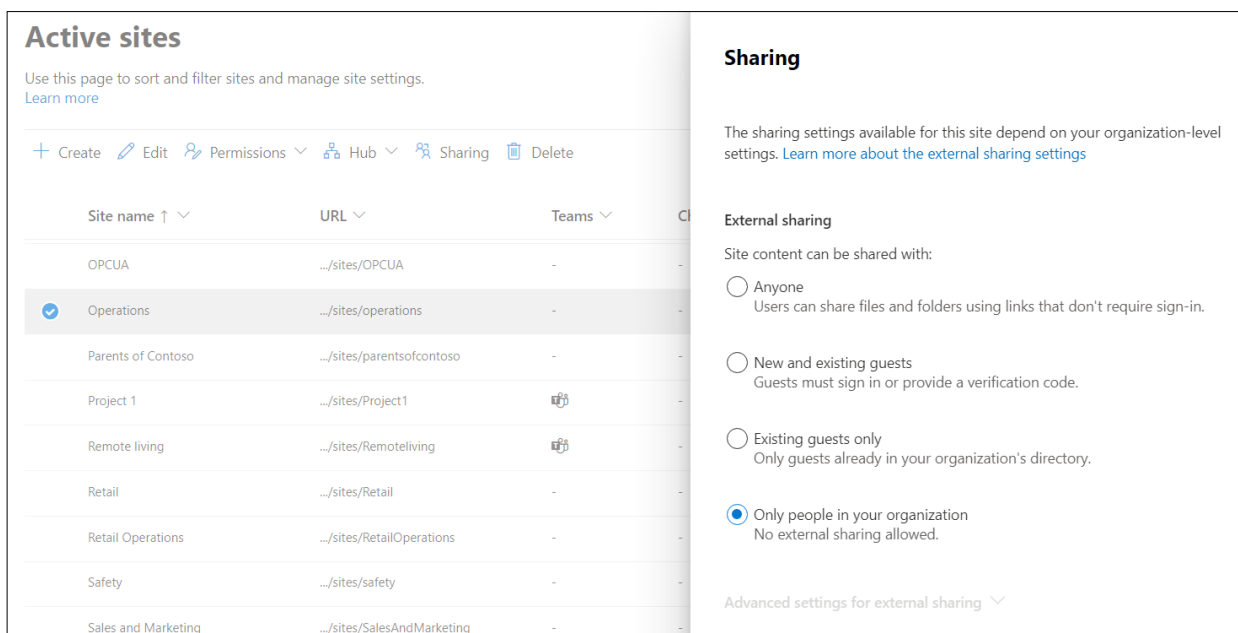
Enter a name

Name	Can share with
DocExSecGroup	Anyone

Please note that even though this organization-level setting represents the maximum allowable sharing, it does NOT mean that all files are shared, or even that all sites allow sharing.

Furthermore, you can restrict the External sharing to only Document Extractor Service user using SharePoint security groups as shown above.

Then, at the site level, you can set the sharing permissions as desired for all sites except the site connected to Document Extractor service.



Active sites

Use this page to sort and filter sites and manage site settings. [Learn more](#)

+ Create Edit Permissions Hub Sharing Delete

Site name	URL	Teams
OPCUA	.../sites/OPCUA	-
Operations	.../sites/operations	-
Parents of Contoso	.../sites/parentsofcontoso	-
Project 1	.../sites/Project1	-
Remote living	.../sites/Remoteliving	-
Retail	.../sites/Retail	-
Retail Operations	.../sites/RetailOperations	-
Safety	.../sites/safety	-
Sales and Marketing	.../sites/SalesAndMarketing	-

Sharing

The sharing settings available for this site depend on your organization-level settings. [Learn more about the external sharing settings](#)

External sharing

Site content can be shared with:

- ☐ Anyone
Users can share files and folders using links that don't require sign-in.
- ☐ New and existing guests
Guests must sign in or provide a verification code.
- ☐ Existing guests only
Only guests already in your organization's directory.
- ☒ Only people in your organization
No external sharing allowed.

Advanced settings for external sharing

Only for the site that Document Extractor uses to store Salesforce files, sharing must be set as allowed to "Anyone": <https://docs.microsoft.com/en-us/sharepoint/change-external-sharing-site>.

SUMMARY

This white paper provided insights on how to restrict access to SharePoint files via Document Extractor Temporary Public Links feature. The white paper also explained how to enable the mentioned feature in a very restrictive way to ensure that only Document Extractor service user can generate those short lived, unguessable and undiscoverable links.

CONTACTS

**Connecting Software s.r.o. & Co
KG HQ + Europe office**
Handelskai 340 Vienna, 1020,
Austria
office-europe@connecting-
software.com +43 (1) 370 72 00

Connecting Software Inc.
4949 S Syracuse St, Ste 550
Denver, CO 80237
United States
office-america@connecting-software.com
+1 (720) 577-3030



www.connecting-software.com