OneDrive for Business Security and Monitoring

What native tools can and can't do, and how to get the enterprise security you need with Quest® solutions

INTRODUCTION

Business users are eager to adopt OneDrive, Microsoft's cloud storage platform, because it makes it simple for them to store and share files. And deploying the platform is a snap. But keeping track of exactly what files are stored there and monitoring how they are used to ensure security is a far greater challenge. IT pros need to be able to quickly answer questions like these:

- What are the OneDrive configuration settings?
- What files are stored in the OneDrive for Business environment?
- Who is accessing those files?
- Which files and folders are being shared and by whom?
- How have file permissions changed?

This white paper explains the native options for configuring, securing and auditing your OneDrive for Business environment, and their limitations. Then it offers a better option: Quest® solutions, including Change Auditor, Enterprise Reporter Suite and Metalogix® ControlPoint, which together provide the enterprise visibility and controls you need to truly ensure OneDrive for Business security.

WHAT IS ONEDRIVE FOR BUSINESS?

From the user's point of view, OneDrive is simply a convenient way to store and share files. Users can have personal OneDrive accounts in addition to their corporate OneDrive for Business accounts, and they can access their files from a web browser, a OneDrive PC client or a OneDrive mobile app. They can even automatically sync their documents to the cloud simply by redirecting the My Documents folder on their devices to OneDrive.

For IT pros, the picture is a bit more complex. The underlying technology for OneDrive is SharePoint, and a user's OneDrive is a document library in SharePoint. You can see this if you go to your Office 365 tenant and view your SharePoint site collections in the SharePoint Admin Center, as illustrated in Figure 1 (in this case, the short name of the Office 365 tenant is "quest"). The data in a SharePoint site collection is stored in SQL Server, which imposes the limit on the number of files you can have in OneDrive, the file name restrictions and so on.

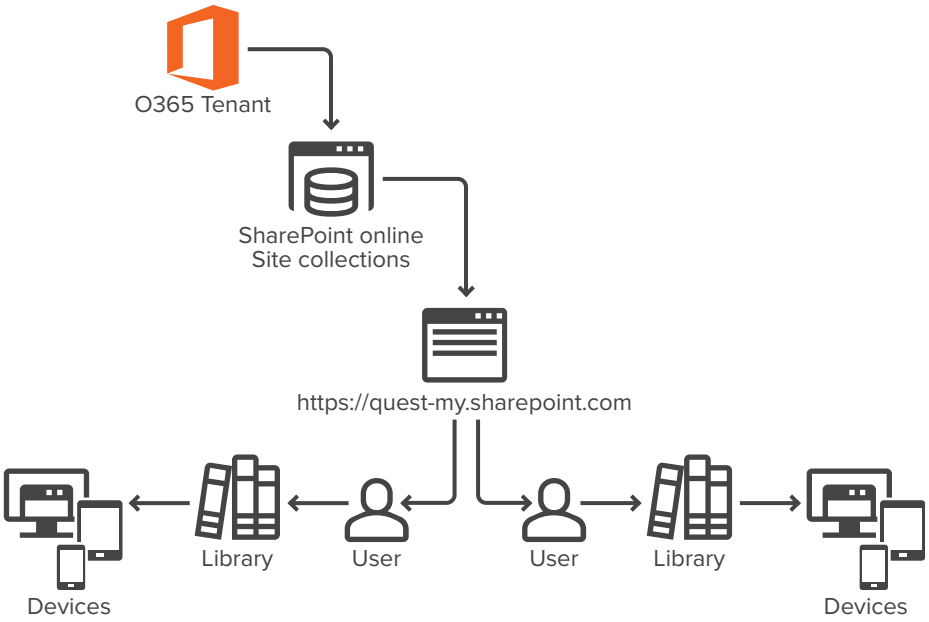


Figure 1. Each user's OneDrive is actually a SharePoint document library, which they can access from a browser, OneDrive PC client or OneDrive mobile app.

The underlying technology for OneDrive is SharePoint, and a user's OneDrive is a document library in SharePoint.

Most organizations also have OneDrive accounts mapped to their SharePoint team sites. For simplicity, this white paper is limited to the OneDrive for Business sites associated with individual users.

MANAGING WHO CAN USE ONEDRIVE

Organizations can control who can administer and use their OneDrive for Business using the SharePoint Admin Center.

Add and remove admins on a OneDrive account

To see and manage all your OneDrive accounts, in the SharePoint Admin Center, go to User profiles / Site collection admins. There you can transfer ownership of a OneDrive account to a different user, or give a user full control over another user's OneDrive. Note that the word "OneDrive" will not appear here because each user's personal OneDrive is hosted under their SharePoint profile.

Disable OneDrive creation for some users

By default, everyone in your organization can create personal SharePoint sites. To limit this ability, in the SharePoint Admin Center, go to User profiles / Manage user permissions. Then change the setting "Everyone except external users" to another group or set of groups. For example, you could create a group in Azure AD called "Approved OneDrive Users," populate it with the appropriate accounts, and then enter that group name here.

ENABLING CONDITIONAL ACCESS

You can use the Office 365 conditional access feature to limit access to OneDrive at the tenant level and at the site-collection level based on factors such as:

- The user's IP address
- The user's identity
- The device and application being used
- The type of data the user is trying to access

For example, you could allow users to access their OneDrive files only from the corporate network or company-owned or company-managed devices. You can also block access from apps that don't use modern authentication.

CONTROLLING SYNCING FROM PCS

Using Group Policy to control OneDrive sync client settings

You can use Group Policy to control whether and how users can sync files to OneDrive from the OneDrive PC client on domain-joined computers. These computer configuration policies can be found under Computer Configuration\Policies\Administrative Templates\OneDrive. In particular, you can prevent users from syncing personal OneDrive accounts, allow or block syncing accounts for other organizations, and manage network usage.

Allow syncing only on computers joined to specific domains

To make sure that users sync files to their OneDrive files only from managed computers, you can configure OneDrive to sync only on PCs that are joined to specific domains. If you enable this setting, users will get an error if they attempt to add an account from an organization not on the list of allowed tenant IDs.

For example, suppose one of your employees does so much work with a particular client that the client has given them a OneDrive account in the client's Office 365 tenant. You can choose whether the PC in your domain is allowed to sync to that external OneDrive account.

Allow syncing only on domain-joined or compliant devices

You can permit the Windows OneDrive client to sync only if it's running on a domain-joined PC. That would, for instance, prohibit users from using their home PC and syncing their personal OneDrive with their OneDrive for Business.

Block syncing of specific file types

You can also block syncing of specific file types, such as all C++ files. Of course, be aware that users can try to get around this restriction by renaming files or putting them in a zip file.

CONTROLLING SYNCING FROM MOBILE DEVICES

You can use the OneDrive Admin Center to create a global policy that manages the OneDrive and SharePoint mobile apps. Note that this policy will apply only to users in your organization who are licensed for Microsoft Intune or Enterprise Mobility + Security. You can use this policy to do things like the following:

- Block downloading files in the apps
- Block copying files and content within files
- Block printing files in the apps
- Require an app passcode
- Block opening OneDrive and SharePoint files in other apps
- Encrypt app data when the device is locked
- Choose how often to verify user access and when to wipe app data when a device is offline

For example, you could allow a user to install the OneDrive app on their iPhone, connect to their OneDrive for Business and view OneDrive files, but prevent them from emailing the files to someone else or uploading them to their personal Dropbox account. You can also require users to re-authenticate to Office 365 every time they open the app, which might be frustrating but improves security if they lose the device.

Some functionality is platform-specific. For instance, you can block users from taking screenshots in the Android apps but not in the iPhone apps.

CONTROLLING ONEDRIVE SHARING

By default, only the user has access to their OneDrive documents (other than the SharePoint site collection admins, of course). However, they can easily share their data with other users by creating one or more sharing links, either on an individual file or at the folder level. For each link, they can specify whether others can edit the item as well as view it, set a password for access, and choose an expiration date for the sharing link.

SharePoint admins can control whether and how users can sync files to OneDrive from their PCs and mobile devices.

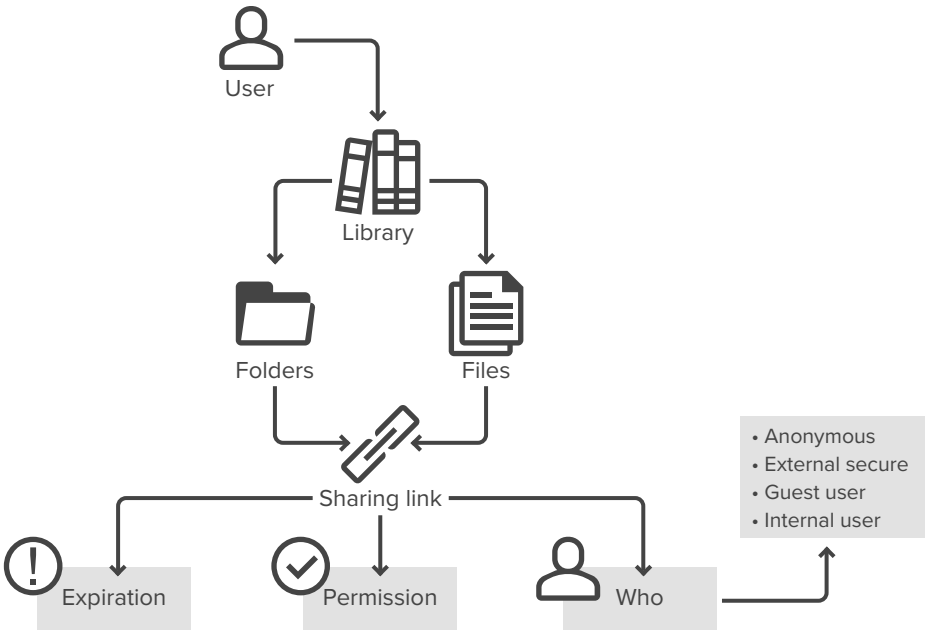


Figure 2. User can share their OneDrive files or folders by creating sharing links.

If a business partner or other external user needs to access a user's OneDrive files on a regular basis, it's wise to create a guest user account for them in Azure AD.

TYPES OF SHARING

There are four types of sharing links, as shown at the right in Figure 2:

- **Internal user —** A particular user who has an Office 365 account in your organization's Azure AD
- **Guest user —** A user, such as a business partner or customer with an Azure AD account in another Office 365 tenant, that an admin has already made a guest B2B or B2C user in your tenant
- **External secure —** A user outside your organization who does not have a guest Azure AD account
- **Anonymous —** Anyone who clicks the sharing link

The security of sharing with internal and guest users is fairly straightforward, since those users are in your AD and have been properly authenticated.

However, if a user wants to share OneDrive data with someone outside the company who is not a guest user, they have two choices. The first is to send the person an anonymous link, perhaps with a note saying, "Please don't share this link with anybody else." This clearly poses a threat to your OneDrive data, since anyone could use the link to access the files.

The other option is for the user to create a secure external link and send it to the external user. In this case, each time the user attempts to access the file or folder, they will receive an email with a time-limited, single-use verification code that they must enter to verify their ownership of the email account. Once they have authenticated, they can access anything that has been shared with their account. But anyone else who might happen to get the link will be unable to access the OneDrive data because they won't know the access code.

Of course, having to provide a verification code each time is very inconvenient for users. Therefore, if a business partner or other external user really needs to access the OneDrive files on a regular basis, it's best to create a guest user account for them in Azure AD.

Setting up sharing policy

By default, users are allowed to share files in OneDrive with anyone using anonymous links. To change that setting for your Office 365 tenant, go to the Sharing tab in the OneDrive Admin Center and adjust the sliders in the External sharing section. You can also define how long links last before they expire, and specify whether the default permissions are view only or view and edit. You can select different options for particular files or folders.

AUDITING AND REPORTING ON ONEDRIVE

Reporting on OneDrive usage

To learn more about how your organization is using OneDrive for Business, go to the SharePoint Admin Center and choose Reports / Usage / OneDrive. There are two reports available:

- **OneDrive for Business activity report —** Shows the number of licensed users who performed file interactions against any OneDrive account, and the trend in the number of active OneDrive users (a user is considered active if they have saved, synced, modified or shared a file within the specified time period)
- **OneDrive for Business usage report —** Shows trends in the number of total and active OneDrive accounts over the last 7, 30, 90 or 180 days; the number of number of total and active files; and the amount of OneDrive storage you're using

You can add or remove columns from the report, filter the report data, drill down into more details about a particular user's OneDrive, and export the report data into an Excel .csv file for further analysis.

These reports will help you evaluate your return for your investment by enabling you to analyze adoption and usage rates and trends. But they don't help much with security or compliance. For that, you need to look to the audit log.

Audit data logged

All access and sharing events in any user's OneDrive creates audit events in the Office 365 audit log. This is not something you need to enable or disable on a OneDrive or folder level; it's all audited automatically.

There are many different types of audit events. Here are four of the most important:

- **File access —** The audit trail records all file access events, such as uploading, viewing, copying, modifying or deleting a file. The events are very specific; for example, you can distinguish between a file being previewed, viewed in a browser or an application, or downloaded.
- **Folder access —** Similarly, the audit trail records when a user creates, copies, modifies, moves, renames or deletes a OneDrive folder.
- **Sync —** File synchronization actions are also audited. For instance, you can review when a user successfully established a sync relationship with a site; when a sync request is denied and a computer is blocked from syncing, when files are downloaded or uploaded and when a full or partial file synchronization takes place.
- **Sharing —** The audit log also records the creation of all four types of sharing links, as well as access attempts made using those links. It's important to know that the sharing link is itself an object that gets a number in the audit log. Therefore, to get the full picture of how a file has been shared, you sometimes need to correlate multiple events in the Office 365 audit log based on that shared link number.

OneDrive for Business provides predefined reports on adoption and usage, as well as a basic search of the audit data.

OneDrive's native reporting and auditing capabilities are quite limited. To ensure security and regulatory compliance, you need flexible enterprise-class solutions.

Viewing the audit log

The Compliance Administration Center enables you to do basic ad hoc searches on the audit data. (There is also an API for those that prefer a programmatic approach.) Keep in mind that the OneDrive activity will be intermingled with activity on the SharePoint document libraries on your team sites.

For example, you can see who accessed the OneDrive files of a certain user. Note that to get complete results, you need to include accessed files, downloaded files and copied files, because all of these actions enable the user to see or share data, but as noted above, they're distinguished from each other in the audit log. You can also audit sharing activities, such as all anonymous links that have been created.

Searches often return a high volume of data, so this functionality is most useful when you're investigating a specific incident and therefore can filter the report by file or folder name, user account, or date range. To strengthen security and prove regulatory compliance, however, you need flexible and powerful enterprise-class solutions.

ENTERPRISE SECURITY FOR ONEDRIVE WITH QUEST SOLUTIONS

Quest solutions streamline governance, enable more effective collaboration and keep your OneDrive for Business environment secure. Quest Enterprise Reporter Suite, Change Auditor and Metalogix ControlPoint provide enterprise visibility into OneDrive for Business access and activity. Moreover, these solutions enable you to correlate that information with the data from other critical systems, including on-premises Active Directory, Azure AD, Exchange, SharePoint, SQL Server and more.

Enterprise Reporter Suite

Enterprise Reporter Suite enables you to see who has access to what across the entire network, as well as understand the configuration of your critical IT assets (see Figure 3). In particular, it gives you clear insight into who has access to the folders and files in your OneDrive for Business environment.

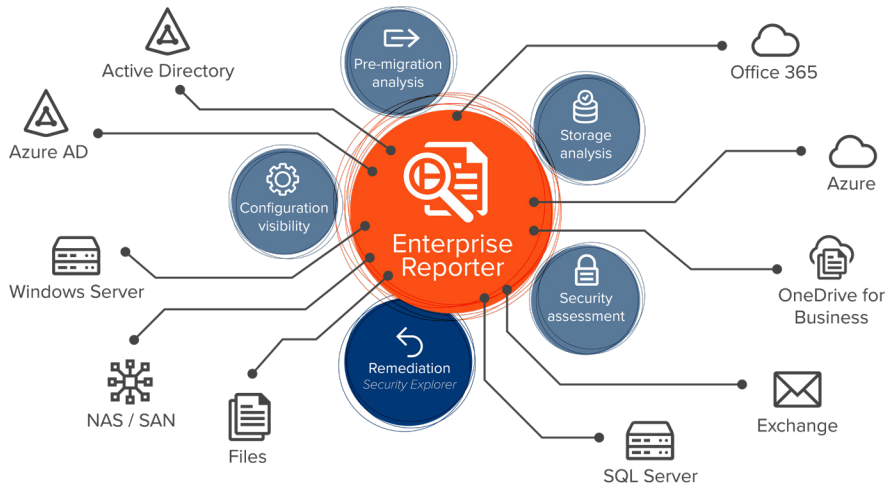


Figure 3. Enterprise Reporter Suite enables you to see who has access to what across the entire network.

Figure 4. Change Auditor provides complete, real-time change auditing, in-depth forensics and comprehensive reporting on all key configuration, user and administrator changes across the enterprise.

Change Auditor

Change Auditor complements Enterprise Reporter by providing complete, real-time change auditing, in-depth forensics and comprehensive reporting on all key configuration, user and administrator changes to critical platforms across the enterprise, including OneDrive for Business, as illustrated in Figure 4.

Metalogix ControlPoint

Metalogix ControlPoint equips SharePoint admins and IT pros with a comprehensive security and governance solution that audits, reports, and governs policy enforcement across their SharePoint, Office 365 and OneDrive for Business environments – all within a single-pane view (see Figure 5). Moreover, the Metalogix Sensitive Content Manager modular component expands the scope of your security by enabling you to scan, detect and classify sensitive data and personally identifiable information (PII).

Quest solutions provide enterprise visibility into OneDrive for Business access and activity — and enable you to correlate that information with data from other key systems like AD and Exchange.

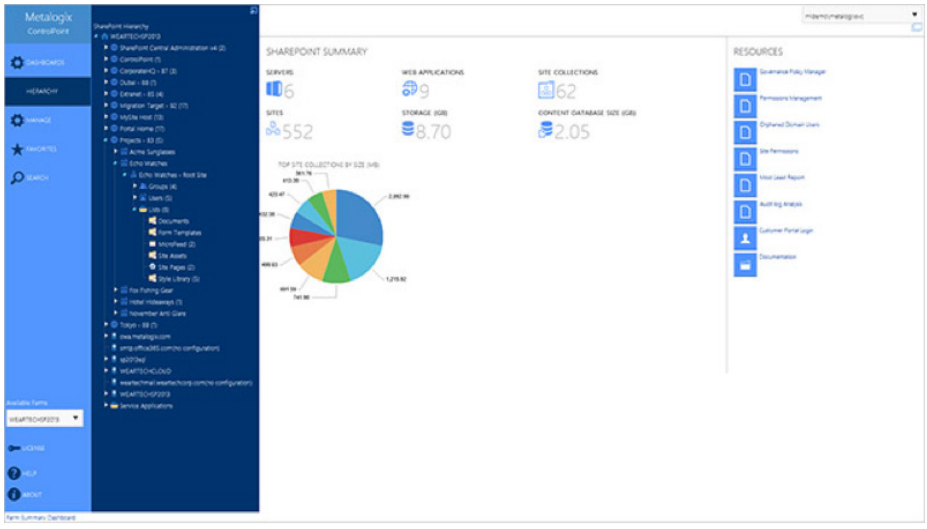
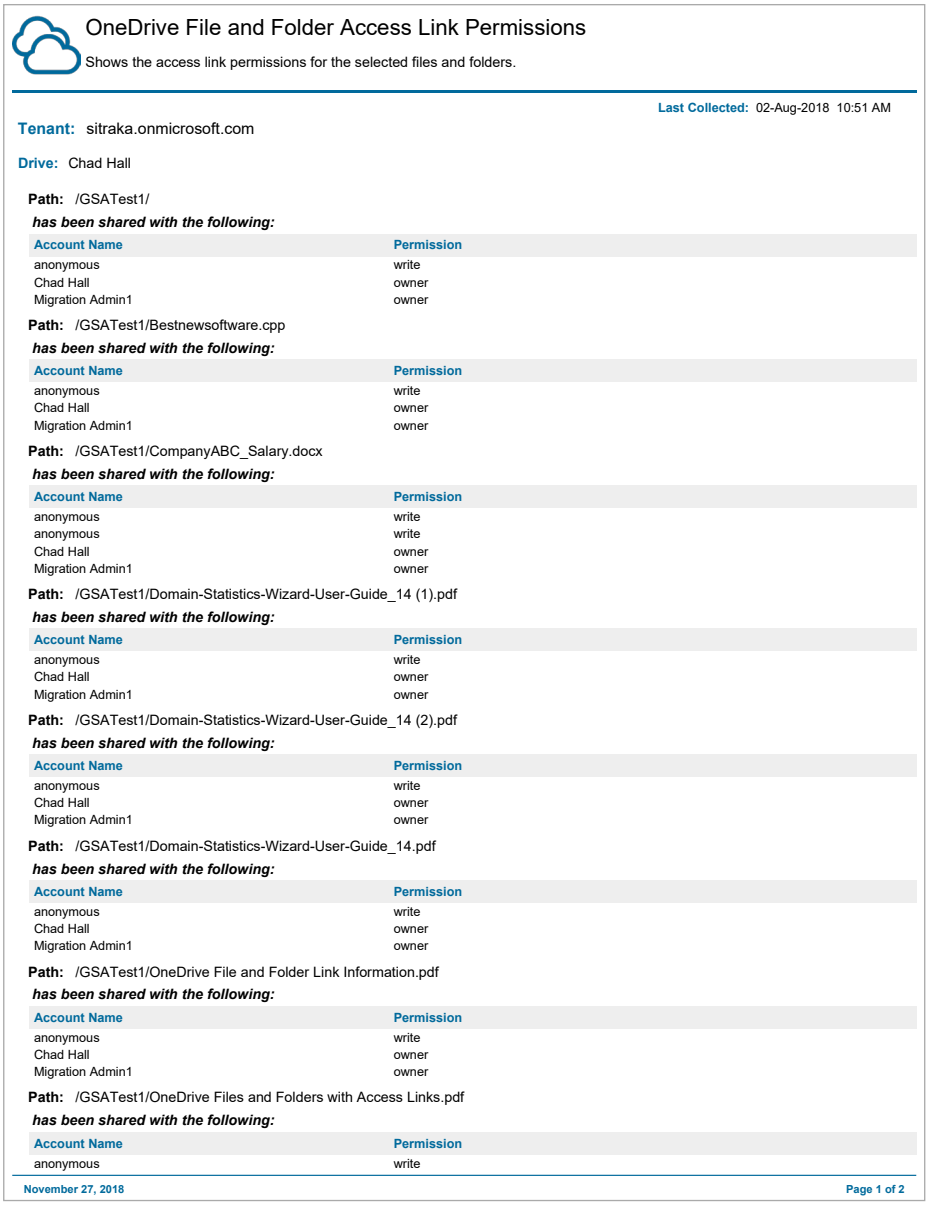


Figure 5. Metalogix ControlPoint enables permissions, auditing, reporting and governance policies for SharePoint, Office 365 and OneDrive for Business.

Quest

Are any of your employees leaking information to outsiders? Enterprise Reporter shows exactly which files have been shared.



OneDrive File and Folder Access Link Permissions

Shows the access link permissions for the selected files and folders.

Last Collected: 02-Aug-2018 10:51 AM

Tenant: sitraka.onmicrosoft.com

Drive: Chad Hall

Path: /GSATest1/

has been shared with the following:

Account Name	Permission
anonymous	write
Chad Hall	owner
Migration Admin1	owner

Path: /GSATest1/Bestnewsoftware.cpp

has been shared with the following:

Account Name	Permission
anonymous	write
Chad Hall	owner
Migration Admin1	owner

Path: /GSATest1/CompanyABC_Salary.docx

has been shared with the following:

Account Name	Permission
anonymous	write
anonymous	write
Chad Hall	owner
Migration Admin1	owner

Path: /GSATest1/Domain-Statistics-Wizard-User-Guide_14 (1).pdf

has been shared with the following:

Account Name	Permission
anonymous	write
Chad Hall	owner
Migration Admin1	owner

Path: /GSATest1/Domain-Statistics-Wizard-User-Guide_14 (2).pdf

has been shared with the following:

Account Name	Permission
anonymous	write
Chad Hall	owner
Migration Admin1	owner

Path: /GSATest1/Domain-Statistics-Wizard-User-Guide_14.pdf

has been shared with the following:

Account Name	Permission
anonymous	write
Chad Hall	owner
Migration Admin1	owner

Path: /GSATest1/OneDrive File and Folder Link Information.pdf

has been shared with the following:

Account Name	Permission
anonymous	write
Chad Hall	owner
Migration Admin1	owner

Path: /GSATest1/OneDrive Files and Folders with Access Links.pdf

has been shared with the following:

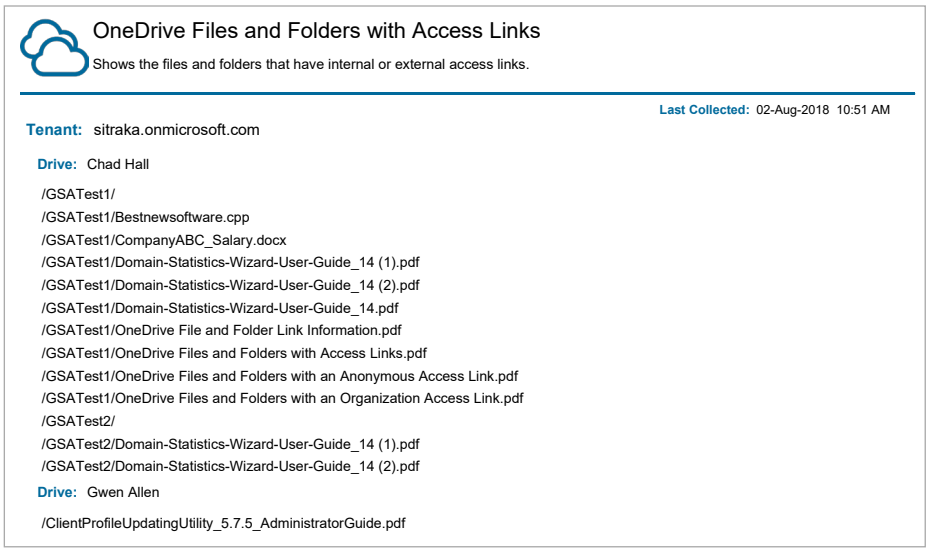
Account Name	Permission
anonymous	write

November 27, 2018 Page 1 of 2

Figure 6. Enterprise Reporter makes it easy to identify which files have been shared outside the organization.

Use case 1: Track down a rogue developer sharing code outside the organization

Suppose your company allows external sharing of OneDrive files and folders, but you suspect that one of your developers might be sharing new software source code with outsiders. With Enterprise Reporter, you can easily identify which files have been shared. The OneDrive File and Folder with Access Links report shows all the files that have been shared outside the organization using an anonymous access link, along with valuable information, such as the URLs to the files and whether the sharing has an expiration date (see Figure 6).


OneDrive Files and Folders with Access Links

Shows the files and folders that have internal or external access links.

Last Collected: 02-Aug-2018 10:51 AM

Tenant: sitraka.onmicrosoft.com

Drive: Chad Hall

/GSATest1/
/GSATest1/Bestnewsoftware.cpp
/GSATest1/CompanyABC_Salary.docx
/GSATest1/Domain-Statistics-Wizard-User-Guide_14 (1).pdf
/GSATest1/Domain-Statistics-Wizard-User-Guide_14 (2).pdf
/GSATest1/Domain-Statistics-Wizard-User-Guide_14.pdf
/GSATest1/OneDrive File and Folder Link Information.pdf
/GSATest1/OneDrive Files and Folders with Access Links.pdf
/GSATest1/OneDrive Files and Folders with an Anonymous Access Link.pdf
/GSATest1/OneDrive Files and Folders with an Organization Access Link.pdf
/GSATest2/
/GSATest2/Domain-Statistics-Wizard-User-Guide_14 (1).pdf
/GSATest2/Domain-Statistics-Wizard-User-Guide_14 (2).pdf

Drive: Gwen Allen

/ClientProfileUpdatingUtility_5.7.5_AdministratorGuide.pdf

Figure 7. Enterprise Reporter makes it easy to identify which files have been shared outside the organization.

Then you can go to the OneDrive File and Folder Access Link Permissions report to determine exactly who has access to the files, both internally and externally, and whether that access is read-only or includes write access as well (see Figure 7).

These sample reports are limited to one particular drive, but you can just as easily create a report that covers multiple drives or even drives in multiple tenants.

Using Change Auditor, we can delve into the activity associated with the files that were shared outside the organization, including who created each anonymous link and the details about each time it was accessed or downloaded. Moreover, this visibility is not limited to OneDrive; you can easily see what else the user who created the anonymous link has been up to in Active Directory, Exchange, SQL Server and other critical systems.

Use case 2: Get alerts on suspicious activity

Change Auditor can also proactively alert you to activity you consider risky. These can be alerts on specific events, such as any sharing of an anonymous link, or threshold-based alerts, like an alert when a user downloads more than 20 OneDrive files within the space of a minute or an hour.

CONCLUSION

OneDrive for Business is a powerful tool for file storage and sharing that facilitates communication and collaboration within an organization and with external parties like partners, service providers and customers. However, left unchecked, use of OneDrive dramatically increases the risk of data loss. Judicious configuration of your OneDrive for Business environment, proper governance and effective monitoring of user activity in the platform is essential to both security and regulatory compliance.

While native tools will help you control who can use OneDrive and how they can share their files, native reporting and auditing capabilities are quite limited. Quest Enterprise Reporter Suite, Change Auditor and Metalogix ControlPoint provide the enterprise visibility into OneDrive for Business activity you need.

To learn more, please visit quest.com/solutions/onedrive-for-business or go to the page for each product:

- Enterprise Reporter Suite
- Change Auditor
- Metalogix ControlPoint

Want an alert if anyone downloads more than 10 OneDrive files in an hour? Change Auditor has you covered.

ABOUT QUEST

Quest provides software solutions for the rapidly-changing world of enterprise IT. We help simplify the challenges caused by data explosion, cloud expansion, hybrid datacenters, security threats and regulatory requirements. We're a global provider to 130,000 companies across 100 countries, including 95% of the Fortune 500 and 90% of the Global 1000. Since 1987, we've built a portfolio of solutions which now includes database management, data protection, identity and access management, Microsoft platform management and unified endpoint management. With Quest, organizations spend less time on IT administration and more time on business innovation. For more information, visit www.quest.com.

© 2018 Quest Software Inc. ALL RIGHTS RESERVED.

This guide contains proprietary information protected by copyright. The software described in this guide is furnished under a software license or nondisclosure agreement. This software may be used or copied only in accordance with the terms of the applicable agreement. No part of this guide may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying and recording for any purpose other than the purchaser's personal use without the written permission of Quest Software Inc.

The information in this document is provided in connection with Quest Software products. No license, express or implied, by estoppel or otherwise, to any intellectual property right is granted by this document or in connection with the sale of Quest Software products. EXCEPT AS SET FORTH IN THE TERMS AND CONDITIONS AS SPECIFIED IN THE LICENSE AGREEMENT FOR THIS PRODUCT, QUEST SOFTWARE ASSUMES NO LIABILITY WHATSOEVER AND DISCLAIMS ANY EXPRESS, IMPLIED OR STATUTORY WARRANTY RELATING TO ITS PRODUCTS INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT. IN NO EVENT SHALL QUEST SOFTWARE BE LIABLE FOR ANY DIRECT, INDIRECT, CONSEQUENTIAL, PUNITIVE, SPECIAL OR INCIDENTAL DAMAGES (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF PROFITS, BUSINESS INTERRUPTION OR LOSS OF INFORMATION) ARISING OUT OF THE USE OR INABILITY TO USE THIS DOCUMENT, EVEN IF QUEST SOFTWARE HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. Quest Software makes no representations or warranties with respect to the accuracy or completeness of the contents of this document and reserves the right to make changes to specifications and product descriptions at any time without notice. Quest Software does not make any commitment to update the information contained in this document.

Patents

Quest Software is proud of our advanced technology. Patents and pending patents may apply to this product. For the most current information about applicable patents for this product, please visit our website at www.quest.com/legal

Trademarks

Quest, the Quest logo, and Metalogix are trademarks and registered trademarks of Quest Software Inc. For a complete list of Quest marks, visit www.quest.com/legal/trademark-information.aspx. All other trademarks are property of their respective owners.

If you have any questions regarding your potential use of this material, contact:

Quest Software Inc.
Attn: LEGAL Dept
4 Polaris Way
Aliso Viejo, CA 92656

Refer to our website (www.quest.com) for regional and international office information.