SPHERE TECHNOLOGY SOLUTIONS

Migration Guide

Managing, Migrating and Minimizing Public Folders in the Cloud

Public Folders and Office365

In terms of raw intellectual capital, there are few information stores in the enterprise that rival the digital assets housed in mailboxes and public folders across the cloud. Think of all the emails sent and received each day. Think of all the assets that move through these systems and the ways individuals and organizations have tried to preserve email for future use, storing them somewhere other than individual mailboxes.

One of the popular methods to preserve email in corporate email systems is by storing email messages in “public folders.” Public folders across Microsoft Exchange allow users to store email, documents, tasks, forms, shared calendars – a slew of information – in a central place which is easily accessible to teams or individuals and easy to integrate with applications. However, all this email has been accumulating for a while now,

and many organizations have started to wonder: Is anyone using all this content? Who does it belong to? Is it locked down correctly? Is it comprising data security?

These questions, however, are not easy to answer using tools native to Exchange, and public folders only continue to grow. Organizations have difficulty enforcing data retention policies, making sure the right people review who has access and monitoring use. There's also that pesky permission issue that can cause users to inadvertently have the ability to see and change data stored in the public folders.

To further complicate matters, migrating to the cloud means that you need to take stock of these assets and answer these questions – you can't simply upgrade public folders from earlier versions of Exchange. At the very least, you'll need to figure out what you have, what you want to migrate and what you want to say goodbye to forever.

Beware of "Default" Access

This is a permission level that exists on every single public folder. Once a user changes the permission level to anything above "None," any new folders created below it will have open access. It is incredibly easy to have serious open access issues due to this one pesky permission level.

Why it Matters

Public folders contain important and sensitive information, with ramifications for both productivity and security. If users rely on them to get their work done, then their availability affects productivity. If they become unavailable, it can affect your organization's mission or its bottom line. On the other hand, if they're not adequately protected and sensitive information is stolen or misused, damage to the organization can be significant in terms of reputation, fiduciary penalties for non-compliance with industry regulations, loss of competitive edge, etc. In addition to concerns related to productivity and security, costs to store and manage this growing data set continue to rise.

3 Steps for Mitigating Risk

STEP 1: SCOPE IT OUT

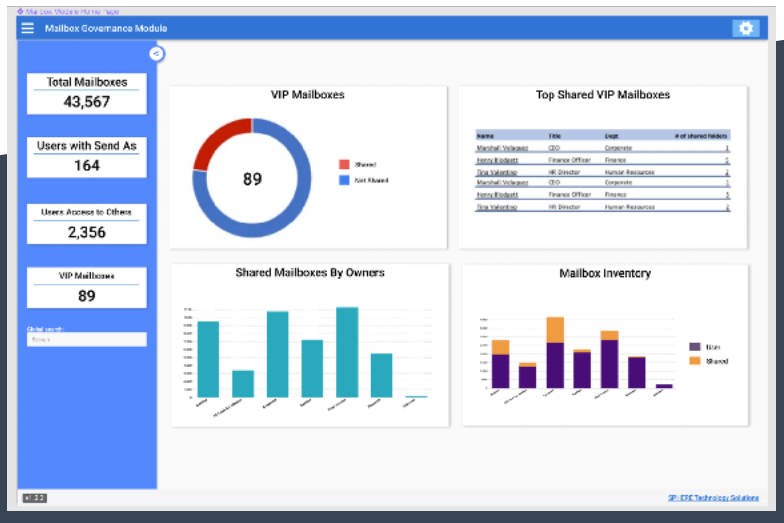
The first step on the path to managing, migrating and minimizing public folders on the cloud is to analyze the current public folder hierarchy and develop a scope of what needs to be moved, what needs to be cleaned up and who needs to be involved. To scope out your public folders, you'll first need to define use case and determine which folders are active or stale.

Public folders can be stale in two ways. First, people can stop sending emails to them, or creating content inside them. Second, people can stop reading their contents. The last time someone sent an email to a public folder can be determined by the time stamps on the emails themselves. To determine whether anyone is still making use of the contents, you'll need technology beyond what's provided in Exchange to manage, migrate and secure public folder usage.

These data points will help you to identify "owners" for public folders. Owners are critical to the migration and to review access – without an owner you'll be stuck making a guess as to how important each folder is, whether it contains anything sensitive, whether it should be migrated or not, and who should have access to it.

Identifying data owners is critical for almost any project that relates to data, however, it is not always clear who should take on that role. It can be helpful to decide at what layer within an organization ownership should be assigned. This will avoid having a pool of people that is too large and difficult to coordinate or conversely having too few owners to respond to inquiries quickly. Too few owners may struggle to manage large numbers of data collections. These owners must have adequate context and authority to make meaningful decisions about the data for which they are responsible.

You'll also need a system to track owners and make sure it stays updated over time so you don't need to do this all over again next time round. Once you have owners assigned and tracked, work with them to review who has access. It's helpful to provide owners with metadata, such as Last Modification Date for stale folders. It's possible to create a permissions report manually by listing the users and groups on the public folder's access control list and then cross-referencing the group members in Active Directory, or a technology platform can create these for you automatically.



STEP 2: CLEAN IT UP

Once you've defined your scope, it's time to start taking action – archive or delete what you've identified as stale or unneeded, and then start getting what's left into better shape. Step 2 is the most involved, so we've broken it into 7 stages:

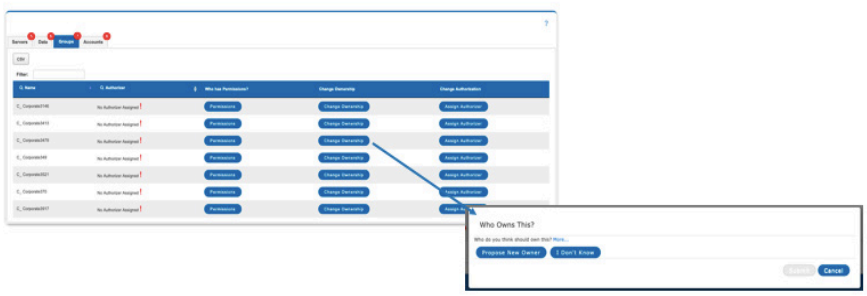
1. Categorize First, systematically categorize data as "Potentially Stale," "Potentially Active," and "Unknown." You can look at modification and access timestamps, access activity and whether there are any valid permissions. It's important to have an "Unknown" category, because sometimes it's not possible to draw a line in the sand, and there will be times when something needs to be looked at more closely over time.

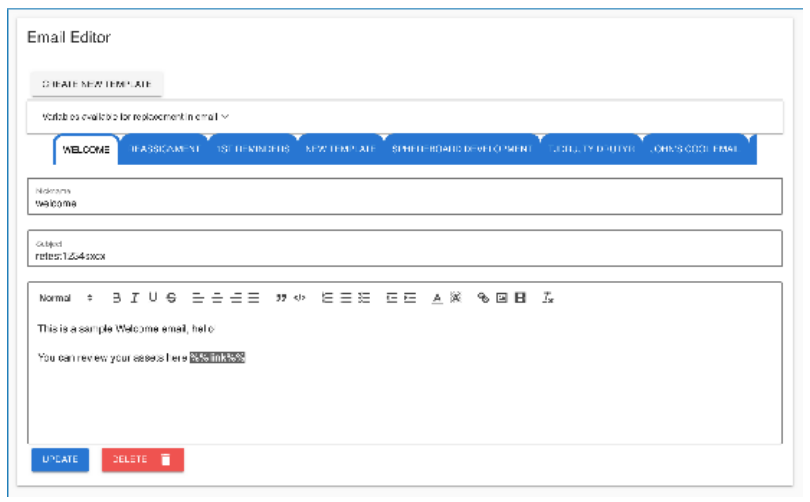
2. Review Unknowns Next, send an automated email to likely owners of "Unknown" data and utilize their responses to categorize this data as either "Stale" or "Active." Email responses are the simplest way to get input on this data set, and identify who is most knowledgeable about it, we can begin to work with them to determine if it is needed or can be deleted, and who needs access to it.

3. Delete Stale Data – in stages For all "Stale" data, implement a staged deletion and/or archival process. Multiple stages act as fail-safes and minimize potential business disruption – you never just want to hit "delete," of course. Stages make it seem like the data is gone when it isn't. Rename a folder or file by adding the words "To be deleted" to the name. This will warn users that it's going to be deleted and they will call support staff if they think it needs to be kept. For data that no one calls about, first remove permissions, then a week or so later, move it. Then, finally, delete or archive it.

The appropriate number of stages and the amount of time in between them can vary between organizations; the important thing is to avoid business disruption. Also, communication and response needs to be quick and easy. For example, before making any changes, the Help Desk should be notified of the potential outages so they know where to look for all the stages and affected repositories and revert a change quickly.

4. Analyze Active Data and Assign Owners Analyze "Active" data to determine how the data is being used and whether it belongs in public folders, or if it would be better in another platform (e.g. SharePoint). This is an opportunity to classify data, develop a taxonomy and proactively identify what data is sensitive, confidential, etc. All "Active" data should have an assigned owner that is required to regularly review and validate that its permissions are correct. Understanding ownership and access can also assist in classification and taxonomy. For example, if you focus on folders owned by Legal and HR, you can work with them to add classifications (or tags) to information they are currently accessing, changing and adding.





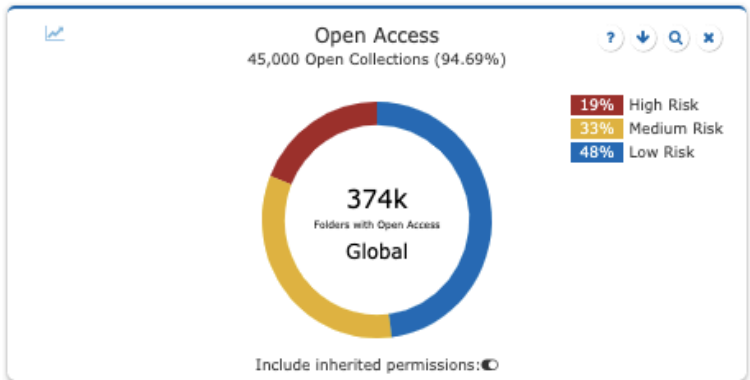
5. Migrate Active Data That's in the Wrong Place Migrate "Active" data that is being stored in an inappropriate repository. Whether you're moving sensitive data to a more controlled system or simply removing Exchange Public Folders from the environment, active data needs to go somewhere where it can be managed and accessed. For instance, a team using Public Folders for sharing documents should move the documents to SharePoint or a file share, instead of migrating data to a mailbox. It's important not to migrate until you've done the previous steps, as you don't want to migrate stale or inappropriate data.

6. Restrict Access If you've found public folders that are too open or permissive, restrict them to only those people that need access. You'll need to work with the data owner to determine who those people are.

7. Entitlement Reviews The last piece of the clean-up process is to implement regular reports that help keep things clean. Data owners should be able to review which of their public folders are active and stale, who is using them, and who has access to them. Finding the right frequency is important – if you run reports too infrequently clean-up efforts will be more substantial; if you run them too frequently data owners will observe few changes between reports and they may be tempted to start ignoring them. A quarterly review is appropriate for many organizations.

Name	Excessive Count	Total Count	Excessive Owner Count
Banking	8,447	9,500	3,761
CEO and Administration	1,388	3,348	1,091
Corporate	4,505	10,700	2,341
Equities	260	7,202	254
Fixed Income	380	11,268	366
Research	176	5,467	150
Unknown	12	41	0
Global	**15,168**	**47,526**	**7,963**

Hide



Include inherited permissions:

Name	High Risk Folders	Medium Risk Folders	Low Risk Folders	Total Open Collections	Open Owner Count
Banking	14,773	25,769	36,466	9,030	4,127
CEO and Administration	5,151	8,974	12,740	3,158	1,763
Corporate	15,704	27,614	40,003	10,139	3,635
Equities	10,553	18,645	26,912	6,800	2,547
Fixed Income	16,601	28,794	42,393	10,663	3,408
Research	8,053	14,069	20,837	5,182	1,490
Unknown	35	74	127	28	0
Global	**70,870**	**123,939**	**179,478**	**45,000**	**16,970**

Hide

STEP 3: MOVE IT OVER

Now that you've identified what you want to move to the cloud and gotten it into shape, it's time to get it where it needs to go. Here are some tips to make that process go smoothly:

•Identify logical groupings collections of public folders that share the same permissions. Then, map these to public folder mailboxes, making sure that none of the new cloud thresholds are exceeded.

•Work with the data owners you identified in Step 2 to verify that your proposed destination makes sense – that collections are grouped coherently and permissions are correct.

•Migrate data using technology and processes appropriate to their desired destination.

Conclusion

Following the steps described above will ensure that you have identified and remediated all potential issues, minimizing your public folders in preparation for cloud migration.

If you're like most organizations, your current public folders are most likely in disarray. Cloud migration is the perfect opportunity to gain a deep understanding of what public folders you have, who owns and is permissioned to them and which assets are stale/empty vs. active. By utilizing the right tools and the right processes you can create a clean, secure and compliant environment in preparation for your next upgrade or migration to the cloud.

About SPHERE

SPHERE Technology Solutions is an award-winning, woman-owned cybersecurity business focusing on improving security and enhancing compliance. SPHERE puts the controls in place to secure your most sensitive data, create the right governance processes for your systems and assets, and make sure companies are compliant with the alphabet soup of regulations surrounding their respective industries. For more information, please visit www.sphereco.com.

CONTACT US

50 Harrison St
Suite 308
Hoboken, NJ 07030

+1 (201) 659-6204

sales@sphereco.com

www.sphereco.com