SECURITY IN AND WITH OFFICE 365

USING SECURE SCORE

URL: www.jethroseghers.com

Email: jseghers@skysync.com

Twitter: @jseghers

LinkedIn: https://www.linkedin.com/in/jseghers/

Security in and with Office 365

Table of Contents

1. The Purpose of this Document

Security is important; security matters. If we are honest, most of us will admit that we were more conscious about security when our workloads were still on-premises. When we are fully responsible for our workloads, from hardware to software to configuration, we tend to be more focused on the overall picture. When our workloads were on-premises, we protected all the different layers. We had UPS, server redundancy, and high-available hardware clusters in our datacenters. Password policies, reverse proxies, and firewalls made the user access more secure. To protect the data itself, we implemented backup policies, making sure that if something happened, we had a backup on disk or tape. This is just subset of protective measures we implemented to guarantee that nobody could access data they were not supposed to. We went to great lengths to make sure we did as well as we could around uptime and security.

However, with Office 365, Microsoft takes on the biggest burden when it comes to uptime and security. Today, we think that an uptime of 99.9X is the industry standard. Microsoft and other cloud services have spoiled us when it comes to uptime. If you want to see the progress of Office 365 uptime, use this link (https://products.office.com/en-us/business/office-365-trust-center-operations). This report will show you that Office 365 has been very close to an impressive, consistent 99.99X.

But when it comes to security, Microsoft can only do so much.

Let's look at the next image.

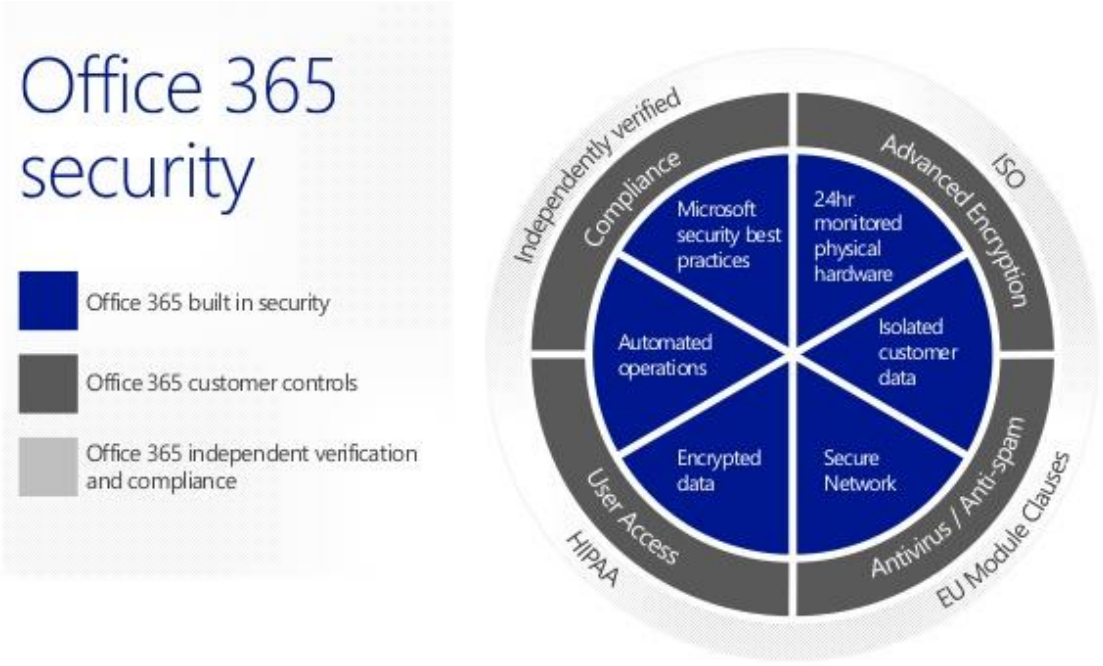

Figure 1. Office 365 security wheel

The blue is built-in Office 365, guarded by Microsoft and completely their responsibility. The gray is what you can do as a customer, and that is the focus of this document.

In this document we are going to use the Secure Score portal to guide you in the security world of Office 365. If you are already familiar with Secure Score you will recognize a lot of the guidelines of Microsoft. If you are not, this is going to help you guide through the Secure Score and why certain parts are important to you. Secure Score are guidelines that help you increase the security in your tenant based on best practices and principles defined by Microsoft. We will add in some of them our opinion potentially deviating from the official Microsoft point of view. It is up to the reader of this document to decide which security measures to implement. The Secure Score should be treated as a guideline and not as an absolute truth. Some measure will make more sense to you than others, if a security measure does not apply to your organization, you should not implement it. Implementation of security is not a matter of being right, it is finding a balance between what your organization needs and how it feels around security.

2. Accessing Your Existing Security Using Security Score

In this document, we are going to use the Secure Score of Microsoft to guide us on the journey to improve our security; you will consciously decide if you want to implement a certain security measure or not. First, we will focus on the security tips that will not require that you invest in additional licenses. Since there are several license combinations in Office 365, we will add as much context as possible if there is a difference in the behavior of the security feature based on the licensing model.

Let's start by retrieving our Secure Score. Log in to https://securescore.office.com/ with a global administrator. This will show you your tenant's security score.

Figure 2. Secure Score number

It will also provide you with a comparison between your score and the average score in your tenant size.

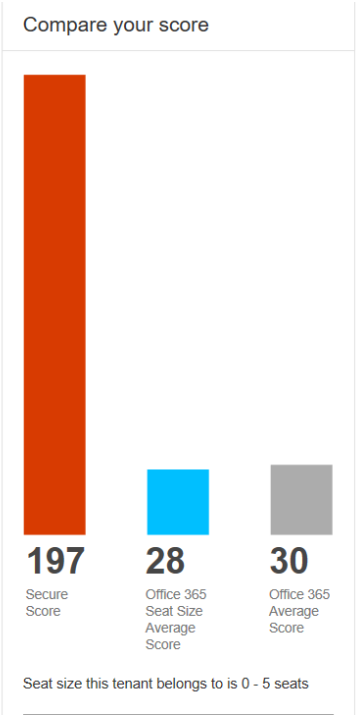

Figure 3. Comparison of your score vs. average score of equal sizing vs. average score

There is a second tab that we want to look at: The Score Analyzer. We will use this information to improve our security score. You will see a breakdown of your score in three categories: Account, Data, and Device.

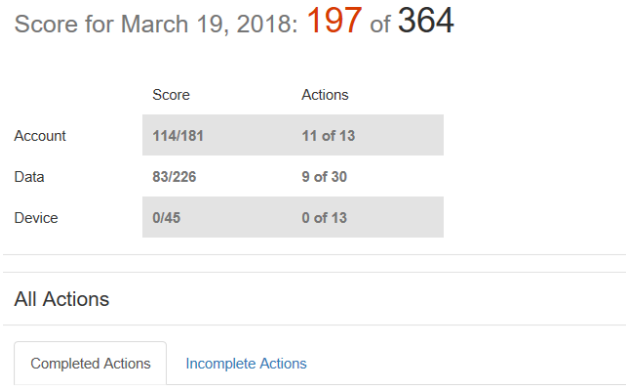

Figure 4. Secure Score breakdown

You can see that we are doing a great job for Account, but Data and Device need some work. You can get into more detail using the Completed Actions and the Incomplete Actions tabs. You can filter the actions you want to implement with several pre-built filters.

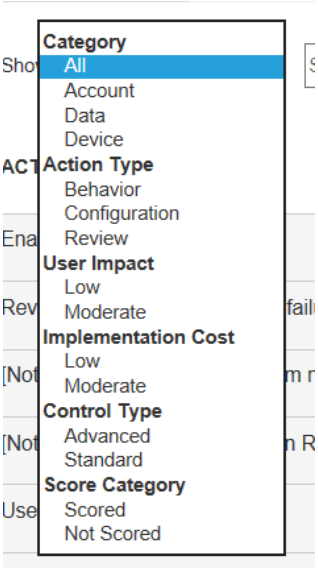

Figure 5. Overview filters

You can use this filter to start with the security actions that solve your immediate needs, work with the lowest user impact. When you choose to implement a new security measure, do it with respect and consideration for your users; no matter how small the implementation is, there is always a need for good communication and change management.

Note: If you are focused on improving your security score, do as much as possible from your Secure Score portal. Some reports will only be taken into consideration when you retrieve them from the Secure Score portal, and not if you go directly to the report. However, the Secure Score should only be an indication, not a goal.

3. Analyzing Your Security Score

3.1. Authentication and Identity

3.1.1. Multi-factor Authentication (MFA)

Let's start with why MFA is something you should investigate. When we look at the current use of authentication, we see that most systems use the combination of username and password as the primary form of authentication. This is based on the security system "*S*omething you know". All approaches for human authentication rely on at least one of the following:

- Something you know (e.g., a password).
- Something you have (e.g., a smart card or mobile phone)
- Something you are (e.g., a fingerprint or eye scan)

We implement at least two of these principles in a multi-factor authentication process. The benefits of implementing more than one principle is twofold. First, it increases security. If one method is compromised, the second can act as a backup. Second, and potentially more importantly, when we are talking about user behavior and adoption, is that the implementation of two factors in your authentication process allows you to be more lenient with the strictness and complexity of the authentication parts. Here is an example: When you rely solely on the combination of a username and password, you feel forced to increase the complexity to make it more secure; if a password is too easy, the chances of somebody guessing it are just too high. That complexity causes people to act insecurely with their password. They write it down on a Post-It Note, and instantly undermine that security level you were trying to achieve. However, when you include the use of a smart card, mobile phone, or fingerprint, the password complexity can be reduced significantly, since whoever is trying to get into your system still needs something you have or are. When you look in the Secure Score of Office 365, you will find the following rules, which will increase your security score related to this topic:

- Enable MFA for all global admins -> +50 points
- Enable MFA for all users -> +10 points/user
- Do not expire passwords -> +10 points

Since all your users need alternate contacts like cell phone number, you get another point for:

- User alternate contact information is completed for all users

If you don't want MFA to be an on/off switch, but rather have it based on certain conditions, like the domain join status of a device or the location of authentication, this is possible with Azure Active Directory Premium – Conditional Access. Read more here: https://docs.microsoft.com/en-us/azure/active-directory/active-directory-conditional-access-azure-portal. Be aware that Azure Active Directory Premium comes with an additional cost.

3.1.2. Do Not Expire Passwords

While this is not the most intuitive recommendation, research has found that when periodic password resets are enforced, passwords become weaker as users tend to pick something weaker and use a pattern of it for rotation. If a user creates a strong password (long, complex, and without any pragmatic words present), it should remain just as strong in 60 days as it is today. Implementing this rule will increase your Secure Score with +10 points.

3.1.3. Administrators

Within Office 365 admin there are multiple roles available that you can assign to your users. The King of the Castle is the Global Administrator. This user has management access to each service and can grant himself permissions to all the content in your Office 365 tenant. Due to the extreme nature of this admin role, lots of security attention goes into making sure that we balance the need for administrators with the need for security. There are some basic rules to the use of administrators and administrator roles that are very easy to implement, thus reducing some of the complexity:

- **Nobody should have administrator rights attached to their user account**. If you have users who need administrative access, they should receive a separate account with a clear identification that they are using their administrator account and not their personal account. This way you prevent people from accidentally using their administrator account. This will grant you +1 points in your Secure Score.
- **Have more than one global administrator account**. This is a measure to make sure you still have a global administrator in case you lose access to your first one. However, there is no need to create many administrator accounts, which would, of course, defeat the purpose of a global administrator. The usage of your global administrator should be a last resort. If you keep it under 5, Secure Score will grant you another +1 points. If you have more than one, you get +2 points.
- **Use the Principle of Least Privilege.** The Principle of Least Privilege (POLP), an important concept in computer security, is the practice of limiting access rights for users to the bare minimum permissions they need in order to perform their work. Under POLP, users are granted permission to read, write, or execute only the files or resources they need to do their jobs; in other words, the least amount of privilege necessary. This principle applies to admin users as well. If your admin is an Exchange admin, there is no need to assign SharePoint admin rights. In Office 365, you can assign the custom administrator role, which allows you to granularly define what admin rights are required.

3.1.4. User Permissions Based on Role

Unfortunately, this rule is not scored in the Secure Score. Nevertheless, it is an important one, allowing you to the reduce the complexity of rights and permissions pollution. The issue here is assigning permissions to users instead of to their role in the company. For example, imagine that in Exchange we have a shared mailbox called “Financial Questions” and a part of the official intranet is dedicated to the financial team, allowing members of that team to publish documents and procedures. In many organizations this is done by individually adding the members of the team to the shared mailbox and to the intranet section.

A far better approach is to create Security Groups, in this case “Financial Team”, add all the members and assign the permissions of the shared mailbox and the intranet site to that Security Group. All members of that security group will have access to the resources they need. When a new person starts on the financial team, you need to add him/her to the security group, and all permissions are automatically set. The same is true when a person leaves the team or organization. If you assign permissions individually, it is difficult to keep track of who has access to what, and that leads to security breaches of content they should not have access to. The important question now becomes *How far do you take this?* It is a choice that each organization needs to make for themselves, but again you must find a balance between security and end-user improvement. For content that is required to be secure, we advise that you absolutely implement this. You can create a security group “Chief Financial Offer” with just one user in it, or two if that person has an assistant. When for some reason the assistant need to be changed, or the CFO moves on to a new organization, his/her replacement simply needs to be added to the security group to get the same permissions.

3.1.5. Disable Accounts That are Not Being Used.

One of the biggest security risks is unused accounts. Unused accounts aren't monitored by a person, and a breach of such an account could go unnoticed for days or even weeks. Most of us would know if somebody used their account to log in from a location where they shouldn't be logged in or identify changes made that they didn't make. With Secure Score, you can add another +1 points if you disable accounts that haven't been used within 30 days. To do so, you can use the built-in report you find here: https://portal.office.com/AdminPortal/Home#/reportsUsage/LicenseActivity. This will provide you with all the information you need. Export it and perform some custom actions, but it should be done as part of a documented process. If you are using the synchronization between your local Active Directory and Office 365, you might want to do this on your local AD and let AADConnect pick it up and sync it back to Office 365.

3.2. Content

3.2.1. Store User Documents in OneDrive for Business

This is measure that is a no-brainer. OneDrive for Business is a better way to store documents than storing them on your local device. A local device can be stolen, a hard drive can be removed, and you lose that data. Your data is safer with OneDrive for Business.

But what happens if you sync your OneDrive for Business data to a local device to have it available offline? This is where device management can help you. If you are using OneDrive for Business as a data availability tool, you are set, but if you want to use it as a security tool then there are some things you need to think about. There are number of synchronization settings that can apply in the OneDrive for Business admin console.

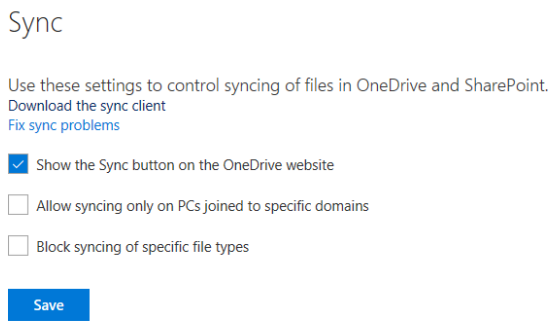

Figure 6. Sync options for OneDrive for Business

3.2.2. Configure Expiration Time for External Sharing Links

You should restrict the length of time that anonymous access links are valid. An attacker can compromise a user account for a short period of time, send anonymous sharing links to an external account, then take his time accessing the data. The attacker can also compromise external accounts and steal the anonymous sharing links sent to those external entities well after the data has been shared. By using a default expiration time for your shared links, you can reduce the time-based vulnerability. If you set an expiration time, your score will go up +2 points. To configure this expiration time, go to the **Office 365 Admin > SharePoint Online Admin > Sharing > Sharing outside your organization**.

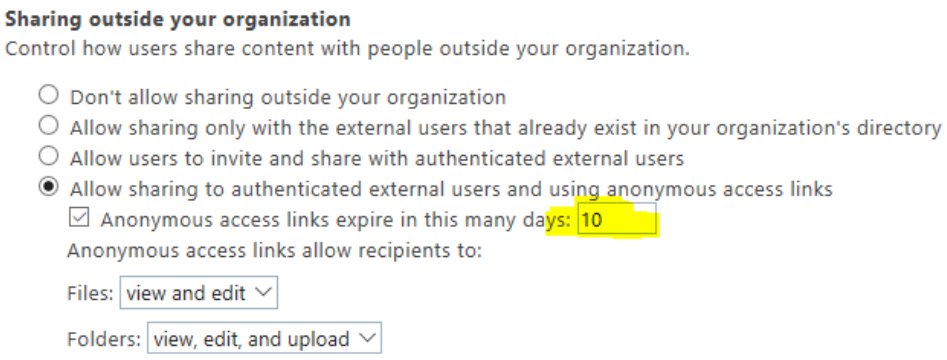

Figure 7. Configure expiration time for external links

3.2.3. Allow Anonymous Guest Sharing Links for Sites and Docs

You should allow your users to use anonymous guest sharing links for SharePoint Online sites and documents. While there are inherent risks in sharing documents anonymously, Microsoft has found that when anonymous sharing is disabled, users often use more risky methods of sharing sites and documents, like email. One proactive approach is to enable anonymous sharing links for customers while also educating users on the pitfalls of sharing anonymously and monitoring links shared for signs of exfiltration by an attacker. If you allow anonymous guest sharing links, your score will go up +1 points. To configure this setting, go the **Office 365 Admin > SharePoint Online Admin > Sharing > Sharing outside your organization**.

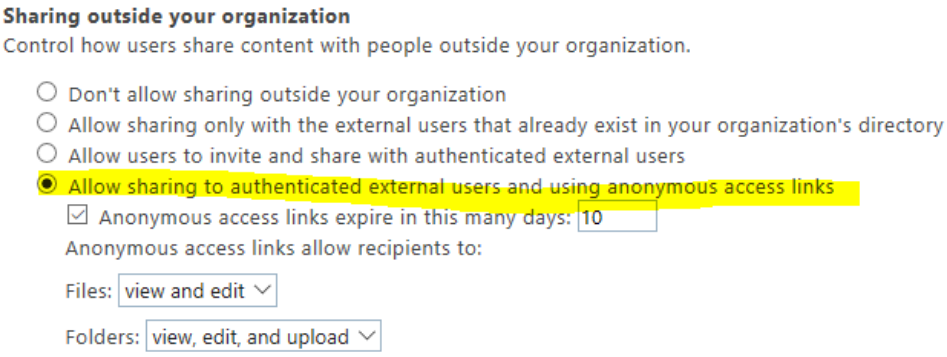

Figure 8. Configure anonymous links

3.2.4. Client Rules Forwarding Blocks

Client-created rules, that auto-forward emails from users' mailboxes to an external email address, are becoming an increasingly common and fruitful data exfiltration method used by bad actors today, and that is no different in Office 365.

There are legitimate reasons for using rules that externally auto-forward email, such as mergers and acquisitions. However, they represent a risk that needs careful and vigilant management by the admins of your tenant to ensure they are not being misused.

These rules can be created through several interfaces: a desktop client, Outlook Web Access, and an admin can even use PowerShell to implement these rules. Users themselves are often unaware of the rules they have in place, so it is very easy to miss them, either accidentally created rules that auto-forward externally, or intentionally created rules created by a bad actor after compromising an end-user's account or breaching a high-privileged account such as the tenant admin.

Even though there are multiple ways to counteract forwarding rules, only the check on transport rules increases your Secure Score. For educational purposes, we will add the other options as well. Implementing this rule increases your score with +20 points.

- **Remote domains**: Per domain, you can define if auto-forwarding is enabled.

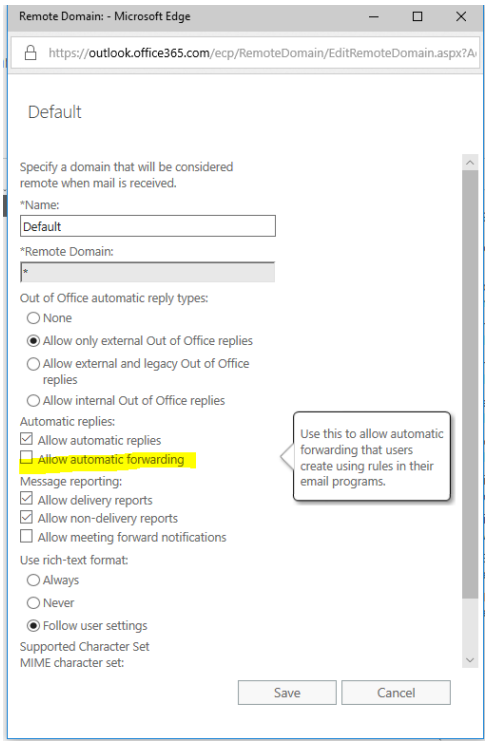

Figure 9. Settings Remote Domain - Allow Automatic Forwarding

- **Review Client Auto Forwarding Rules**: With a simple PowerShell script, you can retrieve and export all client rules and see if any are of the auto-forwarding type. If your PowerShell skills are limited, you can use this prebuilt script DumpDelegatesandForwardingRules.ps1, available on https://github.com/OfficeDev/O365-InvestigationTooling. Make sure to go through the documentation for the overall setup. And note that credit for the project goes to GitHub (https://github.com/OfficeDev/O365-InvestigationTooling/graphs/contributors).
- **Role-Based Access Control**: You can use RBAC to limit the impact as well, by adding a new management role based on the MyBaseOptions, and restricting the parameters DeliverToMailboxAndForward, ForwardingAddress, ForwardingSmtpAddress.
- **Transport Rules**: You can use the Secure Score to implement these rules. This Security Control will create a transport rule that will stop external messages from leaving your tenant, that are of the type AutoForward, mitigating the use of Client-created external mail forwarding rules and malicious Remote Domain entries as a data exfiltration vector.
    - If the sender is located "Inside the organization"
    - If the recipient is located "Outside the organization"
    - If the message type is "Auto-Forward"
    - Reject the message with the explanation "External Mail Forwarding via Client Rules is not permitted"

3.2.5. Do Not Use Mail Forwarding Rules to External Domains

This rule is closely attached to Client Rules Forwarding Blocks but is defined on a forwarding rule level on the mailbox. Go into the Exchange Admin Center, where you can review the forwarding rules and remove rules which forward mail to domains not registered in your tenancy. Removing these rules will reduce the ability of attackers from siphoning out data. This is currently not scored yet. But once the scoring is activated, this will increase your Secure Score with +1 points. To configure this setting, go the **Office 365 Admin > Exchange Online Admin > Recipients> <Select the mailbox> > Mailbox Features > Mail flow > Delivery options**

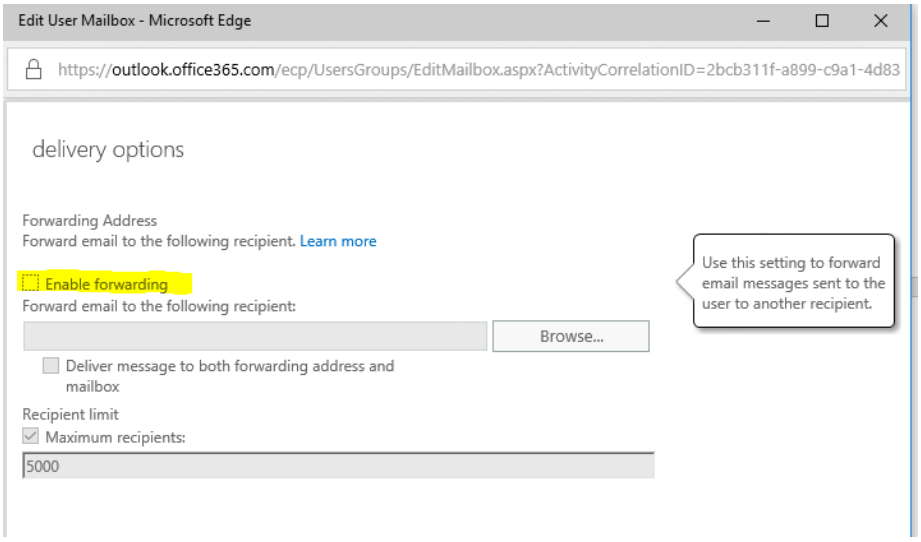

Figure 10. Configure forwarding on mailbox

3.2.6. Do Not Use Transport Rule to External Domains

This rule is closely attached to Client Rules Forwarding Blocks but defined on a transport rule level. Go into the Exchange Admin Center, where you can review the existing mail transport rules and remove rules which forward mail to domains not registered in your tenancy. To set Exchange Online mail transport rules, navigate to M**ail flow > Rules** in the Exchange admin center. Removing these rules will reduce the ability of attackers from siphoning out data from your tenancy. This is currently not scored yet. But once the scoring is activated this will increase your Secure Score with +5 points. To configure this setting, go the **Office 365 Admin > Exchange Online Admin > Mail flow > Rules**.

3.2.7. Do Not Use Transport Rules to Whitelist Domains

In Exchange Online, you can use transport rules to whitelist a specific domain or bypass spam filtering. This is something you should do very carefully; whitelisting a domain can potentially open a very wide door for attackers using that domain to deliver spam or malware. By whitelisting a domain, you are bypassing regular malware and phishing scanning, which can enable an attacker to launch attacks against your users from a haven domain.

If you choose to whitelist domains, make sure you do it in the spam filter policy and not in the transport rules. This is currently not scored yet. But once the scoring is activated this will increase your Secure Score with +5 points. To configure this setting, go the **Office 365 Admin > Exchange Online Admin > Mail flow > Rules**. The rules that you are looking for have the following setup:

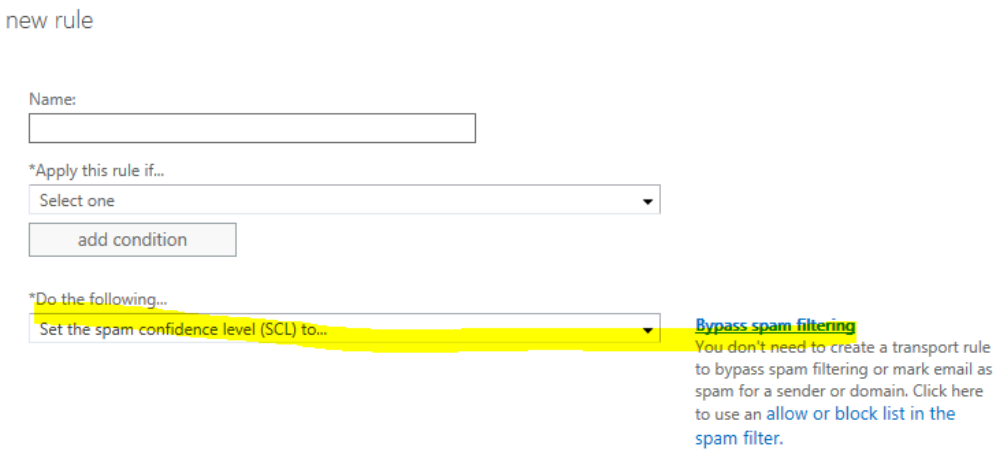

Figure 11. Transport rule to bypass the spam filtering

3.2.8. Do Not Allow Mailbox Delegation

Although there are many legitimate reasons to allow delegation, be aware that providing access to someone's mailbox does have security risks. Before we provide access, we need to be aware of the consequences and see if there is any other way of providing the same functionality by a different mechanism or feature. We could argue that if people need access to each other's mailboxes, the option of a shared mailbox should be investigated for the content that needs to be shared. To configure this setting, go the **Office 365 Admin > Exchange Online Admin > Recipients> <Select the mailbox> > Mailbox Features > Mailbox delegation.**

3.2.9. Enable Versioning on all SharePoint Online Document Libraries

While versioning does not necessarily influence security, it does provide benefits for your end-users. Allowing versioning on your SharePoint Online document libraries will be a life saver in many instances. Fortunately, this setting is activated by default. Using versioning increases your Secure Score with +2 points. Consider this a freebie.

3.2.10. IRM Protections Applied to Documents

You should enable and use Information Rights Management protections on document data. This will help prevent accidental or malicious exposure of your data outside of your organizational boundaries. Attackers targeting specific, high-value data assets will be prevented from opening them without a user credential in your tenancy. Implementing IRM on your SharePoint Online document libraries will improve your score with +5 points. To configure this feature, go **to Office 365 Admin > SharePoint Online Admin > Settings > Use the IRM service specified in your configuration**. Once that setting is activated, you can use IRM on your documents in SharePoint Online.

3.2.11. Set Outbound Spam Notifications

Outbound spam filtering is always enabled if you use the service for sending outbound email, thereby protecting organizations using the service and their intended recipients. Like inbound filtering, outbound spam filtering is comprised of connection filtering and content filtering, although the outbound filter settings are not configurable. If an outbound message is determined to be spam, it is routed through the higher-risk delivery pool, which reduces the probability of the normal outbound IP pool being added to a block list. If a customer continues to send outbound spam through the service, they will be blocked from sending messages. Although outbound spam filtering cannot be disabled or changed, you can configure several company-wide outbound spam settings via the default outbound spam policy. You should set your Exchange Online Outbound Spam notifications to copy and notify someone when a sender in your tenant has been blocked for sending excessive or spam emails. A blocked account is a good indication that the account in question has been breached and that an attacker is using it to send spam emails to other people. This is currently not scored. Secure score allows you to set the notification from within the secure portal. You can set your notification directly through the secure portal or you can go into the **Office 365 Admin > Exchange Online Admin > Protection > Outbound Spam > Outbound Spam Preferences**.

3.2.12. Enable and Implement SPF/DKIM/DMARC

Spam mail messages have been a plague since the Internet opened and spam kept growing as the number of devices and people connected grew. Despite the numerous attempts at creation of anti-spam tools, there's still a huge number of unwanted messages sent every day.

Luckily, it seems that lately something is changing with the adoption of three (relatively) new tools which are starting to be widely used: SPF, DKIM and DMARC. Let's take a quick look at each of these tools and what they achieve.

SPF (Sender Policy Framework) is a DNS text entry which shows a list of servers that send mail for a specific domain. Incidentally, the fact that SPF is a DNS entry can also be considered a way to enforce the fact that the list is authoritative for the domain, since the owners/administrators are the only people allowed to add/change that main domain zone.

DKIM (Domain Keys Identified Mail) is a method to verify that the messages' contents are trustworthy, meaning that they weren't changed from the moment the message left the initial mail server. This additional layer of trust is achieved by an implementation of the standard public/private key signing process. Once again, the owners of the domain add a DNS entry with the public DKIM key, which will be used by receivers to verify that the message DKIM signature is correct, while on the sender side, the server will sign the entitled mail messages with the corresponding private key.

Domain-based Message Authentication, Reporting, and Conformance (DMARC) works with Sender Policy Framework (SPF) and Domain Keys Identified Mail (DKIM) to authenticate mail senders and ensure that destination email systems can trust messages sent from your domain. Implementing DMARC with SPF and DKIM provides additional protection against spoofing and phishing email. DMARC helps receiving mail systems determine what to do with messages sent from your domain that fail SPF or DKIM checks.

Implementing these three methods can be done by adding the right DNS record to your system. Get more detailed information on DKIM here and DMARC here. These methods will become even more important in avoiding your emails to be tagged as spam or phishing.

3.2.13. SharePoint Online Sites Have Classification Policies

You should set up and use SharePoint Online data classification policies on data stored in your SharePoint Online sites. This will help categorize your most important data so that you can effectively protect it from illicit access and will help make it easier to investigate discovered breaches. This only applies to modern team sites that are attached to a group. More information can be found here. It is currently not scored yet, but when it is, it will improve your score with +10 points.

3.2.14. Do Not Allow Anonymous Calendar Details Sharing

You should not allow anonymous calendar sharing. This feature allows your users to share the full details of their calendars with external, unauthenticated users. Attackers will spend time learning about your organization (performing reconnaissance) before launching an attack. Publicly available calendars can help attackers understand organizational relationships and determine when specific users may be more vulnerable to an attack, such as when they are traveling. This is currently not scored yet, but when it is, it will improve your score with +10 points. A lot of people use this to provide their availability to people they work with externally. This was a preferred way in the past, but there are better tools available now that make sharing your availability easier and more secure for you. A replacement based on your needs could be **FindTime**. Read more about here.

Secure score has an additional rule for Do not allow calendar details sharing which is identical to this one. You can change the setting in **Office 365 Admin > Services & add-ins > Calendar**. Change them to deactivate all if you want to implement this rule.

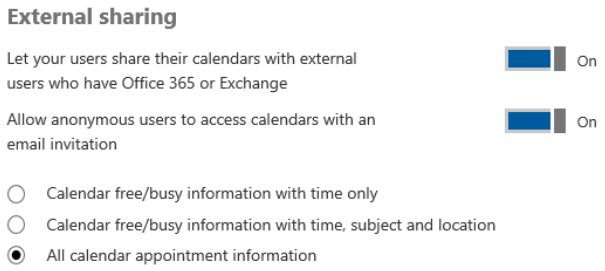

Figure 12. Calendar external sharing options wide open

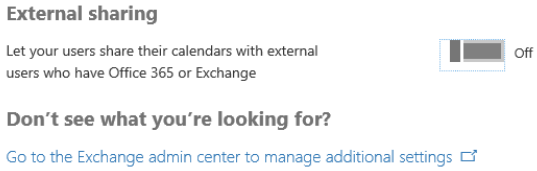

Figure 13. Calendar external sharing options closed down

3.2.15. Do Not Allow External Domain Skype Communication

You should not allow your users to communicate with Skype users outside your organization. While there are legitimate, productivity-improving scenarios for this, it also represents a potential security threat in that those external users will now be able to interact with your users over Skype for Business. Attackers may be able to pretend to be someone your user knows, and then send malicious links or attachments, resulting in an account breach, or leaked information. This is currently not scored yet, but when it is it will improve your score with +5 points. We are not a huge fan of this rule. We work daily with people outside of our organization and it is easy to just jump on Skype for Business and see if they are available for a quick IM, chat, etc. As with most of these rules, you need to find a balance between security and productivity. We do not allow just any domain to be able to reach out to us; it needs to be on our approved domain list.

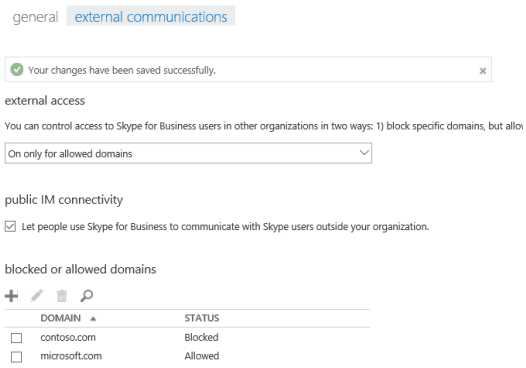

Figure 14. External communication settings in Skype for Business

3.2.16. IRM Protections Applied to Email

You should enable and use Information Rights Management protections on email and document data to help prevent accidental or malicious exposure of your data outside of your organizational boundaries. Attackers targeting specific, high-value data assets will be prevented from opening them without a user credential in your tenancy. Information Rights Management (IRM) allows you to specify access permissions to email messages. IRM helps prevent sensitive information from being read, printed, forwarded, or copied by unauthorized people. After permission for a message is restricted by using IRM, the access and usage restrictions are enforced regardless of where the message goes, because the permissions to access an email message are stored in the message file itself. IRM helps you restrict the transmission of personal or private information. IRM also helps organizations enforce corporate policy governing the control and dissemination of confidential or proprietary information, both within the organization and with customers and partners. This is currently not scored yet. Once the scoring is activated, this will increase your Secure Score with +5 points.

3.2.17. Tag Documents in SharePoint, Tag Emails in Exchange Online

You can create classification labels that the users in your organization can apply to emails, documents, or sites. If you use document classification tags, you will be able to implement specific retention and deletion policies in data loss protection (DLP) that leverage those tags. Read more about those labels here. If you need to comply with certain data regulations where you need to preserve data, emails and documents for amount of time based on content, this is the way to go. This is currently not scored yet. Once the scoring is activated, this will increase your Secure Score with +2 points.

3.3. Reporting and Follow-up

In this section, we will discuss the reporting and follow-up reports. While the Secure Score has a few requests around follow-ups, it is important to know that with the activation of audits on your content you need a plan for follow-ups. What are you looking for? How do you determine the severity when you encounter an action that was not supposed to happen? Within Office 365 Security and Compliance you can of course search the audit log (in some cases you need to activate the audit first), but you must ask yourself if searching is enough. Office 365 can also create alerts when a certain action is triggered under a specific condition.

3.3.1. Use Audit Data

Consuming your audit log data will make your score go up with +5 points. Make sure you enable this in case this hasn't happened yet.

Use the Security & Compliance Center to turn on audit log search. In the **Security & Compliance Center**, go to **Search & Investigation > Audit log search.** Click Start recording user and admin activities. If this button is not available, that means audit log is active. Just click on Search to test. In our test tenant we did not have to activate it even though that the documentation on support.office.com said we had to. Reference: click here.

Audit Log Search: https://protection.office.com/#/unifiedauditlog

Audit Log Alerts: https://protection.office.com/#/managealerts

3.3.2. Review the Signs-ins After Multiple Failures Report Weekly

Most of security is monitoring and keeping up with potential threats within your Office 365 tenant. Early detection of a breach can reduce its impact. When we look at the activity log just before a breach, what we see is that there are number of login attempts, followed by a successful login. Of course, there could be a legitimate reason for that, for example, somebody changed his password yesterday and today he had to be reminded by an incorrect login attempt, force of habit. However, when this is really somebody gaining access to your system, you will be able to identify:

- User: The name of the user that was used during the sign-in operation
- IP: The IP address of the device that was used to connect to Azure Active Directory

- Location: The location used to connect to Azure Active Directory
- Sign-in time: The time when the sign-in was performed
- Status: The status of the sign-in

A best practice is to examine these risky sign-ins at least once a week. If you see false positives, you can report them as false positives, allowing the risky sign-in engine to learn and do a better job of identifying risky behavior.

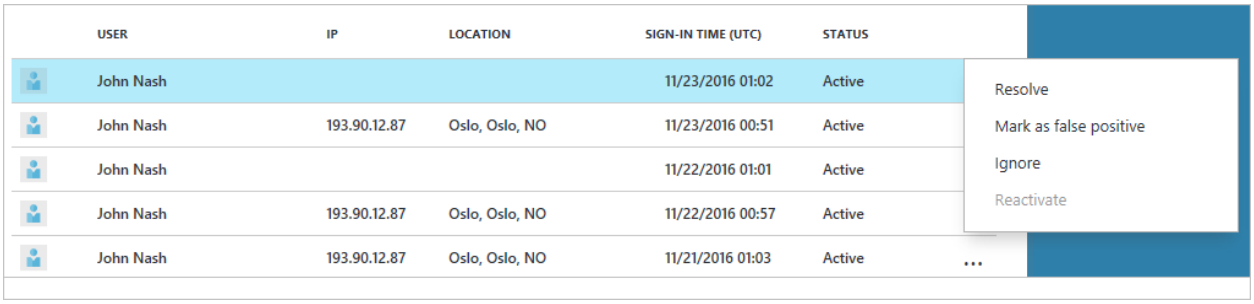

Figure 15. Risky Sign-ins - Credit: docs.microsoft.com

If you want more than just reporting, start looking into to Azure Active Directory Premium, either P1 or P2. These more advanced licenses give you access to more than reporting. It allows you to enable Azure AD Identity Protection. The advanced properties allow you to create more detailed reporting, policies, and much more, based on risky behavior. Read more here: https://docs.microsoft.com/en-us/azure/active-directory/active-directory-identityprotection

Reviewing this on a weekly basis will increase your Secure Score with +45 points.

3.3.3. Review Role Changes Weekly

When you follow the guidance within Secure Score, you will be directed toward the Active Users page (https://portal.office.com/AdminPortal/Home#/users), however it is difficult to identify the changes in role by looking at memberships. Luckily, in audit log search, you can search for two triggers: Added member to Role, Removed a user from a director role.

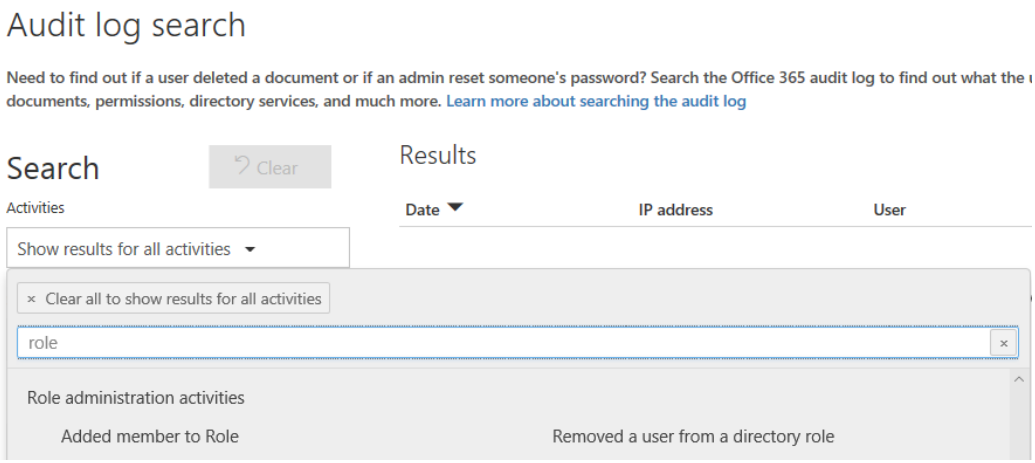

Figure 16. Audit Log Search - Role Changes

3.3.4. Review the Mailbox Forwarding Rules Weekly

You should review mailbox forwarding rules to external domains at least every week. There are several ways you can do this, including simply reviewing the list of mail forwarding rules to external domains on all your mailboxes using a PowerShell script, or by reviewing mail forwarding rule creation activity in the last week from the Audit Log Search. If you review this report, your score will go up +5 points. This is the follow-up of Client Rules Forwarding Blocks.

3.3.5. Review the Mailbox Access by Non-Owners Report Bi-weekly

You should review the Mailbox Access by Non-Owners report at least every other week. This report shows which mailboxes have been accessed by someone other than the mailbox owner. While there are many legitimate uses of delegate permissions, regularly reviewing that access can help prevent an external attacker from gaining access and can help discover malicious insider activity sooner. If you review this report, your score will go up +5 points. This is the follow-up of Do not allow mailbox delegation.

To access the report, log in to your **Exchange Online Admin dashboard > Compliance management > auditing > Run a non-owner mailbox access report.**

3.3.6. Review the Malware Detections Report Weekly

You should review the Malware Detections report at least weekly. This report shows specific instances of Microsoft blocking a malware attachment from reaching your users. While this report isn't strictly actionable, reviewing it will give you a sense of the overall volume of malware being targeted at your users, which may prompt you to adopt more aggressive malware mitigations. If you review this report, your score will go up +5 points. The report can be found in **Office 365 Admin > Security and Compliance > Reports**.

3.3.7. Review the Account Provisioning Activity Report Weekly

You should review your account provisioning activity report at least weekly. This report includes a history of attempts to provision accounts to external applications. If you don't usually use a third-party provider to manage accounts, any entry on the list is likely illicit. But, if you do use a third-party provider, this is a great way to monitor transaction volumes, and look for new or unusual third-party applications that are managing users. If you see something unusual, contact the provider to determine if the action is legitimate. If you review it, your score will go up +5 points.

To get the report, go to https://portal.azure.com. Select **Azure Active Directory > Audit logs** and look for the category Account Provisioning.

3.3.8. Review the Non-Global Administrator Weekly

What do you look for? Look for new or unusual names. While these non-global administrator roles are less powerful than a global admin, they do grant special privileges that can be used illicitly. If you see something unusual, contact the user to confirm that there is a legitimate need. You can use the audit log for this as well. We like the methodology described in Review role changes weekly.

3.3.9. Enable Auditing on the Mailbox

By default, all non-owner access is audited, but you must enable auditing on the mailbox for owner access to also be audited. This will allow you to discover illicit access of Exchange Online activity if a user's account has been breached. Setting the auditing can be done through PowerShell. You can find a PowerShell script on GitHub or click here.

3.3.10. Enable Advanced Security Management Console

If you don’t find any documentation about this, it is because Microsoft changed this name to Cloud Apps Security. As an Office 365 user, you have access to the functionality in Office 365. At the time of this writing, there were default 11 policies that Cloud Apps Security would check against, going from Unusual file share activity (by user) to Impossible travel. The functionality is limited in comparison to the full-blown version you have available when you have a Cloud Apps Security license, but that comes at an additional cost. You do get those 11 policies and the alerts triggered against them. So it's worth using it.

3.4. Devices

Mobile phones are important. People use them all the time; they have become an extension of our corporate environment. While devices are personal property (unless the phone is owned by the company), we still need to think about additional security for mobile phones since they generally contain corporate information and data. You should use a mobile device management service such as Office 365 Mobile Device Management or Microsoft Intune. Devices, especially mobile devices, are vulnerable to attacks, such as malware, that can lead to account and data breaches. Rolling your devices in MDM will increase your security score with +20 points.

First, you will need to activate MDM in Office 365, or you can choose to use Microsoft Intune. Microsoft Intune will come with an additional cost but allows you to configure more. In this document we will focus on the MDM built-in Office 365.

The first thing we need to do is to enroll our devices in MDM. If you have Windows 10 and you have connected your Office 365 to the device when you go **to Office 365 > Admin > Security and Compliance > Data Loss Prevention > Device management** might already see your Windows 10 device.

To add your mobile phone, we need to make sure we have everything we need. Your domain needs to be set up to deal with MDM. When you added your domain, there were two DNS records you needed to add specifically for MDM.

Mobile Device Management for Office 365

Type	Priority	Host name	Points to address or value	TTL
CNAME	-	enterpriseregistration	enterpriseregistration.windows.net	1 Hour
CNAME	-	enterpriseenrollment	enterpriseenrollment.manage.microsoft.com	1 Hour

Figure 17. DNS settings for MDM

If you are using iOS, you need to get an APNs Certificate for iOS device. Click on manage settings and go through the setup for the certificate. The process is very straightforward. Finally, we need to enroll our device in MDM. Before we do this, we must create a device security policy that will define the settings for our mobile phone. We can start by defining the organization wide settings. These settings cover two topics: what do we do with unsupported devices, and what are the Security Groups that excluded from the MDM. Then we can create a more specific policy.

A device security policy is attached to a security group or groups. Furthermore, it contains all the settings for the mobile device. These settings contain, but are not limited to:

- Require a Password (+5 points)
    - Prevent Simple Passwords (+2 points)
    - Require an alphanumeric password (+1 point)
    - Minimum password length
    - Number of sign-in failures before device is wiped (+1 point)
    - Lock devices if they are inactive for this many minutes (+1 point)
    - Password expiration (+1 point -- is not set yet)
    - Remember password history and prevent reuse (+1 point)

- Require data encryption on devices (+1 point)
- Prevent jail-broken or rooted devices from connecting (+1 point)
- Require managing email profile (required for selective wipe on iOS) (+5 points)
- If a device doesn't meet the requirements, then
    - Allow access and report violation
    - Block access and report violation (+5 points)

Based on the membership of the group, people will receive an enrollment email they need to follow for the enrollment procedure. However, sometimes those emails do not make it to the owner of the device. Your end-users can enroll by themselves by installing the Microsoft Intune Company Portal. The portal will guide them through the enrollment procedure. If all goes well, you should see the mobile phones appear in the device list.

4. Advanced

4.1. Enable the Advanced Threat Protection Safe Attachments Policy

The Advanced Threat Protection is an advanced feature in Exchange Online Protection. You are required to have a more advanced license or buy it as an extension to your existing license SKU. If you want to add additional security when it comes to your attachments, you should enable the Office 365 Advanced Threat Protection Safe Attachments feature. This will extend the malware protections in the service to include routing all messages and attachments that don't have a known virus/malware signature to a special hypervisor environment where a behavior analysis is performed using a variety of machine learning and analysis techniques to detect malicious intent. Using this policy comes with a delay in message delivery, since the message is rerouted to a separate environment where more advanced analysis is being performed. If the message comes clean, it will be delivered to your mailbox; if not, it depends on the settings within the Safe Password Policy to determine how the message and the attachment will behave. If you enable Safe Attachments, your score will go up +15 points. Click here to learn more about it.

4.2. Enable Advanced Threat Protection Safe Links Policy Data

If you want to add additional security for your emails and hyperlinks in the content, you should enable the Office 365 Advanced Threat Protection Safe Links feature. This will extend the phishing protection in the service to include redirecting all email hyperlinks through a forwarding service, which will block malicious ones even after it has been delivered to the end user. If you enable Safe Links, your score will go up +15 points. Click here to learn more about it.

4.3. Enable Customer Lockbox Feature Data

As an Office 365 admin, Customer Lockbox Request allows you to control how a Microsoft support engineer accesses your data. Sometimes if you run into an issue, you might need a Microsoft support engineer to help you fix it. In some cases, the support engineer will require access to your Office 365 content to troubleshoot and fix the issue. Customer lockbox requests allows you to control whether to give the support engineer access to your data. There's also an expiration time on the request and content access is removed after the support engineer has fixed the issue. Customer lockbox is included in the Office 365 E5 plan. If you don't have an Office 365 E5 plan, you can buy a separate customer lockbox subscription with any Office 365 Enterprise plan. Enabling the button below will enable the Customer Lockbox feature so that Microsoft engineers do not get access to your content without your explicit approval. When you get the request for access, you can scrutinize the request and either approve or reject it. Implementing this feature will increase your score with +5 points.

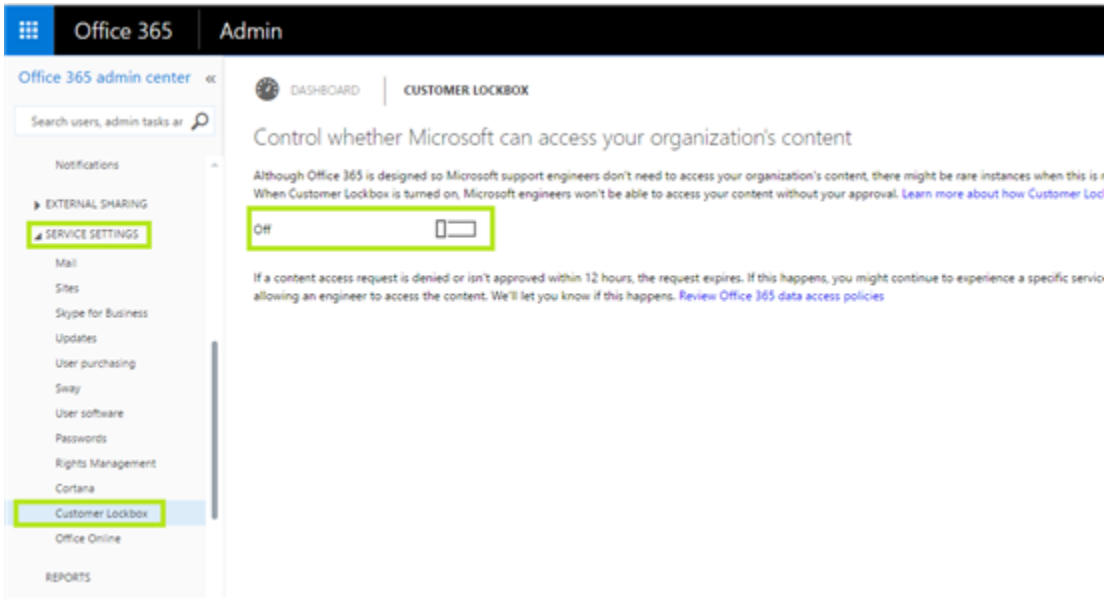

Figure 18. Customer Lockbox

4.4. Do Not Allow Third-party Integrated Applications

You should not allow third-party integrated applications to connect to your services unless there is a very clear value and you have robust security controls in place. While there are legitimate uses, attackers can grant access from breached accounts to third-party applications to exfiltrate data from your tenancy without having to maintain the breached account. Blocking third-party integrations will increase your score with +10 points.

4.5. Enable Data Loss Prevention

Not all data loss is caused by malicious outsiders trying to access your systems by hacking their way into it. Sometimes it is just an honest mistake, people accidentally shared information or emailed sensitive information out of their environment to somebody who was not supposed to have access to that information. That is why we have Data Loss Prevention (DLP); to prevent people from making mistakes by implementing rules and guidelines. With DLP we are going to focus on sensitive information, and sensitive information can be whatever the organization defines it to be. When you ask people *What is sensitive information?* in most cases they will say Personally Identifiable and financial information like bank accounts, social security numbers, etc., because that is what we know best.

Try to think about in the terms of an organization or company. The CEO of a company of course wouldn't want his financial information to be accidentally shared, and he wouldn't want his contracts or employee files accidentally shared, either. That is exactly what DLP does; it helps people identify risks in sending and sharing information while trying to avoid data leakage from occurring. Implementing Data Loss Prevention will increase your Secure Score with +20 points.

4.6. Azure Active Directory Premium

While the basic Azure Active Directory is enough for most security purposes, Azure Active Directory Premium gives you access to several features that allow you to customize the end-user experience. While this takes us technically outside of the scope of this document, we will give you an example how attached Azure Services like AAD can help you increase the security of your Office 365. This is not covered in the Secure Score, but we think it should be because it helps your end-user detect phishing attacks. The feature is called Company Branding. You won't find it in Office 365, but you will when you go to the Azure Portal and go to Azure Active Directory. If you have a license for Office 365 or Azure Active Directive Basic or higher, you should have access to this.

Phishing attacks will lead you to a fake login page, where they will ask for a username and password, hoping that the end-user will not see the difference between the real login page and the fake page. With Azure Active Directory, you can change the login page for Office 365, so it contains your logo, a tagline, and some basic company information. Phishing attackers in most cases won't go to the trouble of building a custom login page. If your end-user sees that the login page is not your custom-designed login page, they will know it is a fake one. Once you have your customized your company branding, your login experience could look like this:

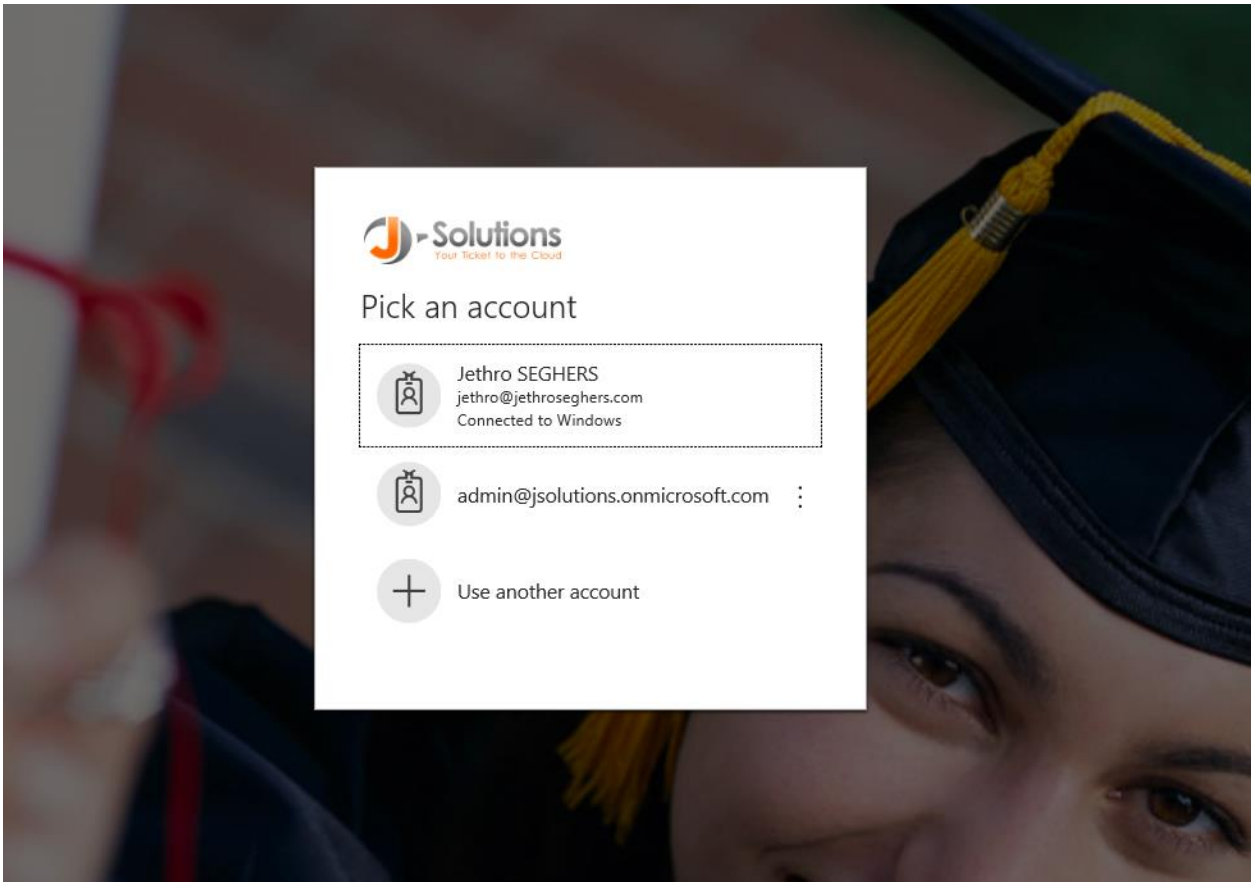

Figure 19. Custom login Experience - Company branding

This is the checklist we use when we start implementing a security plan in Office 365. You will see two lists. The first one is crucial and has such a huge ROI that it is a no-brainer. The second one is for when you want to take your security to the next level.

	Security measure	Explanation
Type: Account		
	Enable Multi-factor authentication	More Info
	Separation of Administrator accounts and user accounts	More Info
	Assign the minimal permissions required to do their job	More Info
	More than one global administrator, less than five	More Info
	Permissions based on role rather than on name	More Info
	Disable unused accounts	More Info
	Do not expire their passwords	More Info
	Provide alternate contact information for all your users	More Info
Type: Content		
	Enable mailbox auditing for all users	More Info
	Enable Client Rules Forwarding Block	More Info
	Store user documents in OneDrive for Business	More Info

	Use audit data	More Info
	Enable versioning on all SharePoint online document libraries	More Info
	Configure expiration time for external sharing links	More Info
	Do not use mail forwarding rules to external domains	More Info
	Do not use transport rule to external domains	More Info
	Do not use transport rule to whitelist domains	More Info
	Set outbound spam notifications	More Info
Type: Device		
	Enable mobile device management services	More Info
	Require mobile devices to use a password	More Info
	Require mobile devices to block access and report policy violations	More Info
	Require mobile devices to manage email profile	More Info
	Do not allow simple passwords on mobile devices	More Info
	Require mobile devices to lock on inactivity	More Info
	Require mobile devices to have minimum password length	More Info
	Do not allow jail broken or rooted mobile devices to connect	More Info
	Do not allow mobile device password re-use	More Info
Type: Reporting		
	Create alerts for important events in your audit log	More Info
	Review the signs-ins after multiple failures report weekly	More Info
	Review role changes weekly	More Info
	Review the malware detections report weekly	More Info
	Review the account provisioning activity report weekly	More Info
	Review the non-global administrators weekly	More Info
	Review mailbox forwarding rules weekly	More Info
	Review the mailbox access by non-owners report bi-weekly	More Info

Checklist 2

	Security measure	**Implemented**
Type: Account		
	Enable Advanced Security Management Console	More Info
Type: Content		
	Do not allow third-party integrated applications	More Info
	IRM protections applied to documents	More Info
	Do not allow mailbox delegation	More Info
	Enable Data Loss Prevention policies	More Info
	SharePoint Online Sites have classification policies	More Info
	Do not allow anonymous calendar sharing	More Info
	Do not allow external domain skype communications	More Info
	Do not allow calendar details sharing	More Info
	IRM protections applied to email	More Info
	Tag documents in SharePoint	More Info

	Allow anonymous guest sharing links for sites and docs	More Info
	Enable customer lockbox feature	More Info
Type: Device		
	Require mobile devices to use alphanumeric password	More Info
	Require mobile devices to use encryption	More Info
	Require mobile devices to lock on inactivity	More Info
	Require mobile devices to wipe on multiple sign-in failures	More Info
	Require mobile devices to never expire password	More Info

5. Conclusion

After reading this document, we hope you are inspired to think about security very seriously. Start thinking about what you can do to increase your security. Security matters. It is not something to be taken lightly. And if we are honest, most Office 365 customers do take security far too lightly. The average Secure Score of all the tenants says it all. The average score is 30. If you implement basic security settings, you should rate much higher than that. Let's get that number up, one tenant at the time.

6. Contact Information

If there is anything I can help you with, feel free to reach out to me on any of these contract addresses:

Jethro Seghers

URL: www.jethroseghers.com

Email: jseghers@skysync.com

Twitter: @jseghers

LinkedIn: https://www.linkedin.com/in/jseghers/