MICROSOFT 365 ENTERPRISE

SECURITY ASSESSMENT PLAYBOOK

A field guide and toolkit for assessing the security quality of Microsoft 365 Enterprise deployments and operations

SEPTEMBER 2020

riskrecon
mastercard

A playbook by RIskRecon, Inc. | WWW.RISKRECON.COM

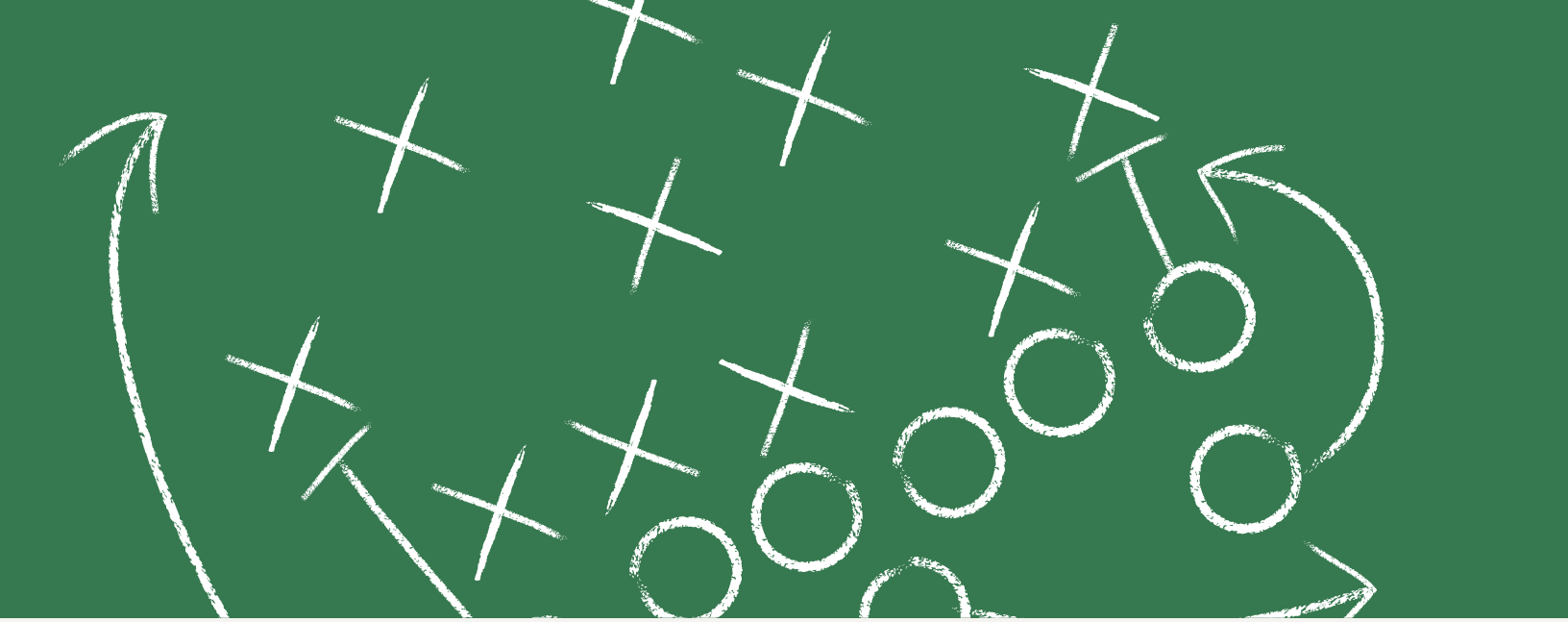
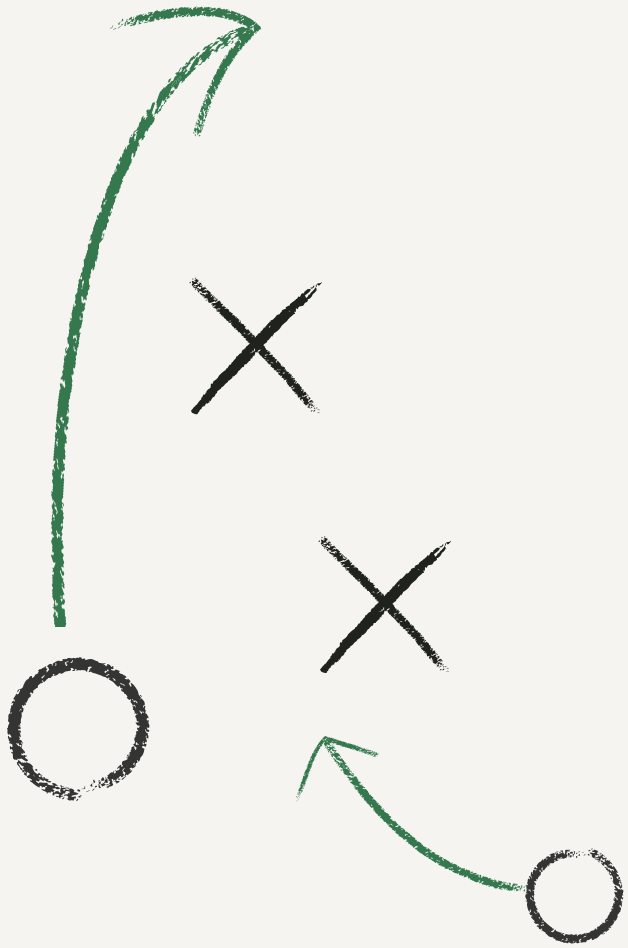


TABLE OF CONTENTS

INTRODUCTION



Like many cloud services, the Microsoft 365 Enterprise (formerly Office 365) core value proposition is also the security challenge. “Office 365 and Microsoft 365 Apps enables you to create, share, and collaborate from anywhere on any device with a cloud-based suite of productivity apps and services.” [1] Extending the challenge further, all of the related data is centrally stored in OneDrive, which Microsoft describes as providing the ability to “access files from any device, at any time.” [1]

Even if your enterprise is not operating on Microsoft 365, no doubt a large percentage of your vendors are. Correct security configuration and operation of Microsoft 365 by you and your third parties is critical to protecting your risk interests.

To aid you in assessing the security of Microsoft 365 deployments in your own organization and by your third-party providers, RiskRecon has developed the Microsoft 365 Enterprise Assessment Playbook. This Playbook provides a step-by-step methodology for assessing the quality of the essential security configurations of any Microsoft 365 Enterprise deployment.

Here you will find essential Microsoft 365 security assessment security criteria, explanations of the importance of each criteria, how to gather related evidence, and what proper configuration looks like. RiskRecon’s Microsoft 365 Security Assessment Questionnaire accompanies this Playbook, providing you tools to assess the security of third-party deployment.

Third-party security assessments founded on objective evidence are the most effective way to achieve good risk outcomes. This Microsoft 365 Third-Party Assessment Playbook and the accompanying Questionnaire do just that - they help you achieve better risk outcomes by providing you the knowledge and tools for objectively assessing the security quality of any Microsoft 365 deployment.

ACKNOWLEDGEMENTS

The Microsoft 365 Assessment Playbook was developed by experts in the fields of cloud security and third-party cybersecurity assessment from RiskRecon and Stratum Security. The project was led by Jonathan Ehret, a widely known third-party risk expert and RiskRecon’s Vice President of Strategy and Risk. RiskRecon provides automated risk assessment and workflow technology that make it easy to understand and act on your own enterprise and your third-party cybersecurity risk.

Stratum Security provided additional subject matter expertise, developing the draft security assessment criteria. STRATUM SECURITY is a Washington D.C.-based security consulting firm that specializes in web application and cloud security assessments.

1. Retrieved from https://www.microsoft.com/en-us/microsoft-365/enterprise/compare-office-365-plans on 8/31/2020

THE MICROSOFT 365 SECURITY CRITERIA

While Microsoft 365 provides an expansive set of capabilities, the core security controls boil down to a pretty short set of essential controls. This is achieved through Microsoft's unified identity and access management architecture. While the control list is short, getting the configurations right is critically important. Microsoft 365's default configuration is pretty promiscuous. These default settings include allowing non-privileged users to invite guest users to the organization's Azure AD and default file sharing settings.

THE ASSESSMENT CRITERIA

The Microsoft 365 Security Criteria covers three security domains. Each domain contains one or more security criterion. Each criterion is presented as follows:

- ID - The unique criterion identifier. This maps to the associated questionnaire.
- Criterion - The assessment criterion, phrased as a question.
- Why this is important - An explanation of why the criterion is important for securing the Microsoft 365 deployment.
- Validation steps - A description of how to collect the evidence necessary to assess compliance with the criterion.
- Acceptable responses - A listing of the configuration states that meet the criterion requirements.
- Failure responses - A listing of the configuration states that do not meet the criterion requirements.
- More info - A hyperlink to additional information related to the criterion.

THE QUESTIONNAIRE

We've instantiated this Criteria in a security questionnaire. Please feel free to use the questionnaire to assess the security of your vendor's Microsoft 365 deployments. Send it over to your vendors to fill out, or ask the questions over the phone. As you do this, you will get much greater transparency into an important component of their security program. You will also get greater accountability to securing the environment right, because generic responses like "Yes, we do Identity and Access Management stuff" isn't going to fly.

AUTHENTICATION

WHAT

Identity and Access Management is centered around Azure AD and is arguably the most sensitive component within the Microsoft 365 ecosystem. Azure AD also allows organizations to synchronize their on-prem Active Directory with Azure AD, allowing authentication with other external services.

WHY

Azure AD is a feature-rich identity and access management system that can be complex, depending on the organization's configuration. Additionally, if the organization synchronizes their on-prem Active Directory to Azure AD, it is possible to expose internal domain objects to external threats. As such, a well-planned and properly secured Azure AD configuration is critical.

ID: o365 - 1: Are users configured with multi-factor authentication?

WHY IS THIS IMPORTANT?

Multi-factor authentication is a critical security control that protects organizations from password attacks such as password guessing and credential theft. If a Microsoft 365 user account is compromised, an attacker may gain access to the user's emails, files, chat history, and other sensitive data.

BACKGROUND

Microsoft 365 provides organizations multi-factor authentication through two different features:

- Azure MFA for Microsoft 365 – Basic but effective multi-factor authentication available in all Microsoft 365 subscriptions
- Microsoft Azure Conditional Access – Feature-rich and granular multi-factor authentication enforcement available

Azure MFA for Microsoft 365 provides basic multi-factor authentication and is implemented via the Microsoft 365 user management interface. There are three multi-factor authentication settings that can be applied to each user:

- Disabled – The user is not allowed to self-enroll or use multi-factor authentication
- Enabled – The user may enroll in and use multi-factor authentication
- Enforced – The user must enroll in and use multi-factor authentication

Microsoft Azure Conditional Access is an Azure AD Premium P1/P2 feature that allows organizations to define granular user access policies, including which users need to use multi-factor to be granted access to Microsoft 365 resources.

VALIDATION STEPS

Access the Multifactor Authentication screen by:

1. Navigate to HTTPS://ADMIN.MICROSOFT.COM/
2. Access the "Users" menu, then select "Active users"
3. Click the "Multi-factor authentication" menu item
4. Inspect the value in the "Multi-factor Auth Status" column for each user.
5. Confirm whether each user is configured with the "Enforced" value.

For Azure MFA for Microsoft 365, the following URL and screenshot can help validate the response:

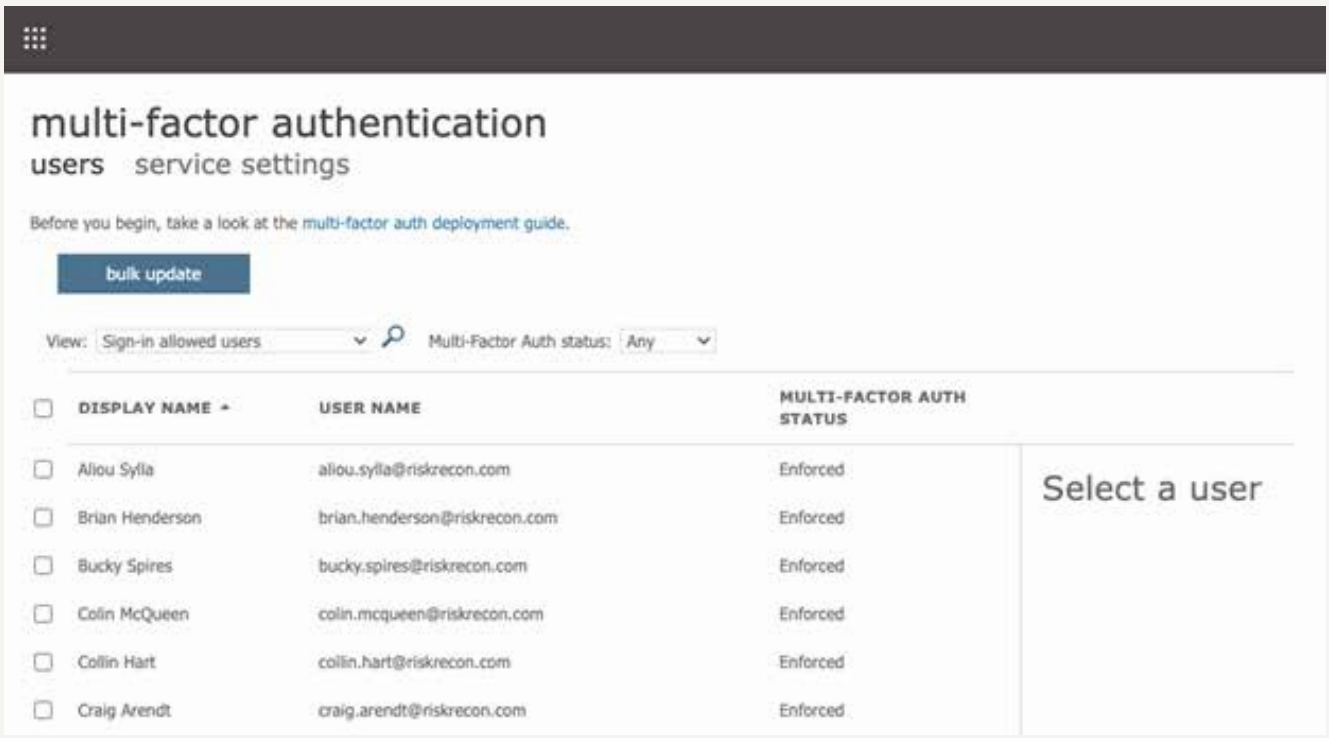


Figure 1: *Screenshot showing the users within the organization are configured with a multi-factor status of "Enforced"*

ACCEPTABLE RESPONSE(S)

- All users are configured with a multi-factor status of "Enforced".

FAILURE RESPONSE(S)

- Multiple users are configured with a multi-factor status of Disabled.
- Multiple users are configured with a multi-factor status of Enabled.

MICROSOFT AZURE CONDITIONAL ACCESS

VALIDATION STEPS

From the Azure Portal, access the Azure Active Directory interface. Then, access the Security menu, and then Conditional Access Policies screen and view the tenant's Conditional Access policies. Identify if a policy is enabled (State column should show "On") that requires multi-factor authentication for all users within the organization. The screenshot below shows a Conditional Access Policy named Enforce MFA that is assigned to a group called Company Employees.

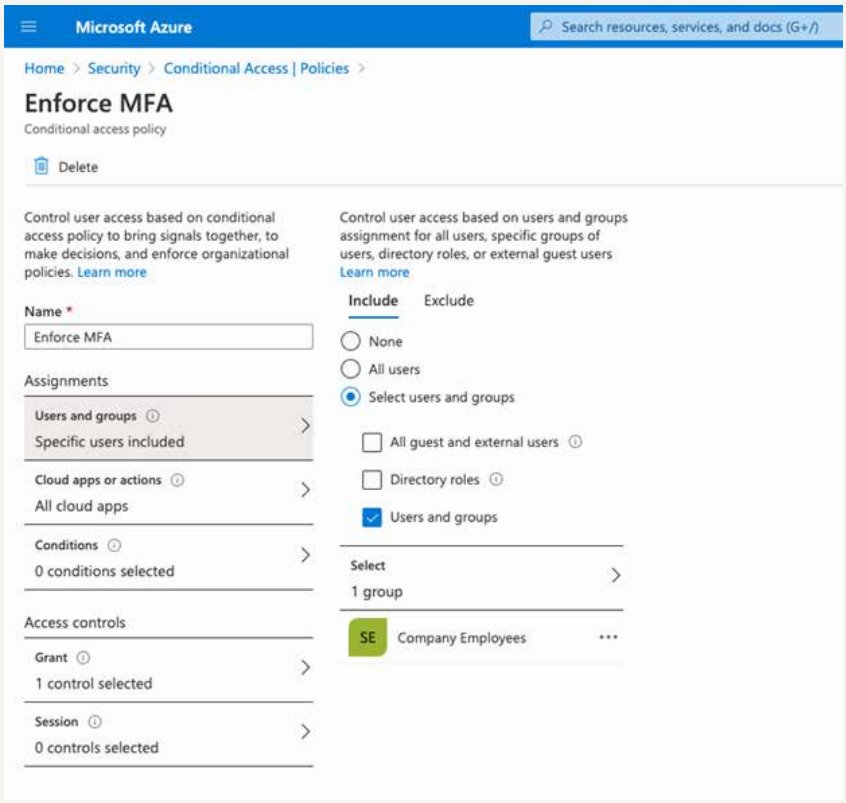


Figure 2: *Screenshot of a Conditional Access rule (Enforce MFA) that requires that all users within the "Company Employees" group is required to use multi-factor authentication*

For Azure MFA for Microsoft 365, the following URL and screenshot can help validate the response:

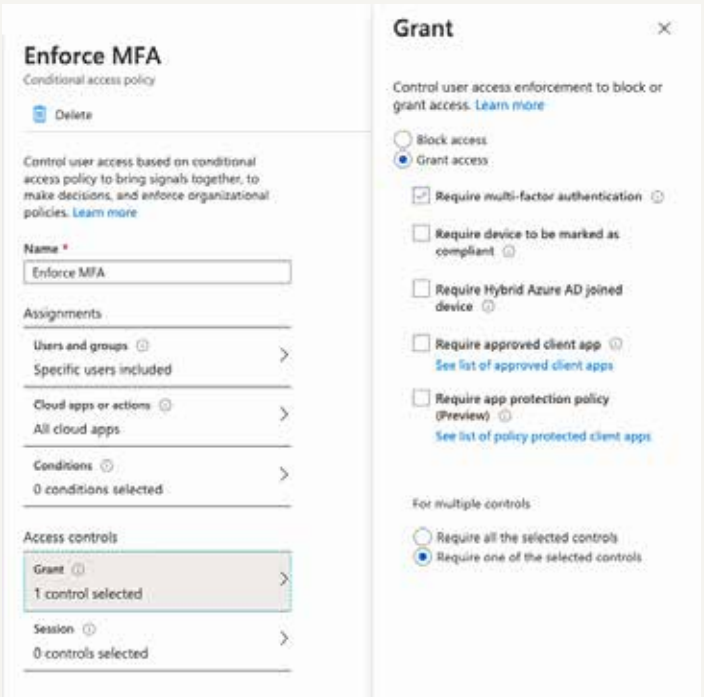


Figure 3: *Screenshot of a Conditional Access rule that requires that all users within the "Company Employees" group is required to use multi-factor authentication.*

ACCEPTABLE RESPONSE(S)

- A Conditional Access rule for all employees is configured and enforced that only grants access to Microsoft 365 via multi-factor authentication. (Note: some service or non-user accounts may not have multi-factor authentication configured).

FAILURE RESPONSE(S)

- The policy is not enabled
- Not all users are assigned to the Conditional Access policy
- The policy does not require multi-factor authentication to access to Microsoft 365

FURTHER INFORMATION:

- How it works: Azure Multi-Factor Authentication

  HTTPS://DOCS.MICROSOFT.COM/EN-US/AZURE/ACTIVE-DIRECTORY/AUTHENTICATION/CONCEPT-MFA-HOWITWORKS

- What is Conditional Access?

  HTTPS://DOCS.MICROSOFT.COM/EN-US/AZURE/ACTIVE-DIRECTORY/CONDITIONAL-ACCESS/OVERVIEW

ID: o365 - 2: If the organization's on-prem Active Directory is synchronized with Azure Active Directory, are only necessary objects synchronized?

WHY IS THIS IMPORTANT?

If an organization is synchronizing their on-prem Active Directory with Azure Active Directory (Azure AD), it is a good indicator that the organization's IT environment is complex enough to justify cloud authentication. Organizations will commonly synchronize their on-prem AD with Azure AD to allow users to authenticate via public cloud SaaS applications and to ease the administrative burden of managing users across a portfolio of cloud services. However, it is a best security practice to only sync those AD objects that require use within Azure AD (e.g. on-prem service accounts that only access on-prem resources should not be synchronized, whereas user accounts should be synchronized). As such, examine the objects within Azure AD to determine if the organization is synchronizing the appropriate objects.

VALIDATION STEPS

View all users within the Azure AD Users screen and identify on-prem resources:

1. Navigate to https://portal.azure.com and select Azure AD.
2. From the "Manage" menu on the left, select "Users"
3. Identify any user accounts that appear to be on-prem users.
4. Hint: Look for usernames containing words that indicate the account is for internal / on-premise purposes only, such as: backup, firewall, duo, nessus, audit, IWAM_*, IUSR_*.

ACCEPTABLE RESPONSE(S)

- Evidence that indicates that not all on-prem AD users have been syncronized to Azure AD.

FAILURE RESPONSE(S)

- Evidence that all on-prem user accounts have been syncronized to Azure AD.

ACCOUNT MANAGEMENT

WHAT

Some of the services, features, and components within Microsoft 365 are an extension or complete replacement of an organization's traditional on-prem infrastructure and services.

WHY

Attention to detail within an organization's Microsoft 365 account is critical. On-prem environments benefit from compensating security controls such as firewalls and VPNs. Microsoft 365 is a cloud service and by design is exposed to the Internet. It is critical that organizations take care when administering their Microsoft 365 environments.

ID: o365 - 3: Is the number of users configured as administrators in Microsoft 365 appropriate for the size of the organization?

WHY IS THIS IMPORTANT?

Having more than one administrator in Microsoft 365 ensures that if one administrator is unavailable, another user can make changes to the tenant. However, users who do not have a valid justification to have administrative access to Microsoft 365 may expose the organization to risk. Microsoft recommends that in most cases there should be no more than five Global Admins.

VALIDATION STEPS

View all admin users by accessing the Microsoft 365 Admin portal's Active users screen:

1. Navigate to HTTPS://ADMIN.MICROSOFT.COM/
2. Access the "Users" menu, then select "Active users"
3. Click the filter icon on the right side of the screen:
4. Select "Global Admins"
5. View the users that have the Global Administrator role

For Azure MFA for Microsoft 365, the following URL and screenshot can help validate the response:

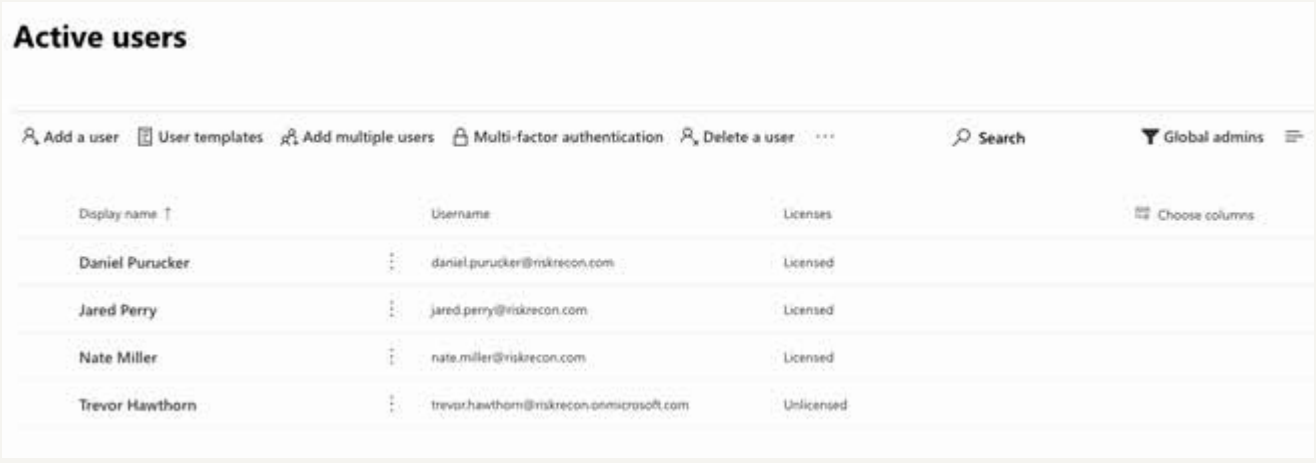


Figure 4: *Screenshot of the "Active Users" screen with a filter for "Global admins" applied*

ACCEPTABLE RESPONSE(S)

- Ensure that at least two users are configured with the Global Administrator role
- If more than two users are Global Admins, identify the justification for the additional privileged users

FAILURE RESPONSE(S)

- Only one Global Admin is listed
- More than two Global Admins are listed, however there is no justification for the additional administrators

ID: o365 - 4: Are dedicated administrative accounts used?

WHY IS THIS IMPORTANT?

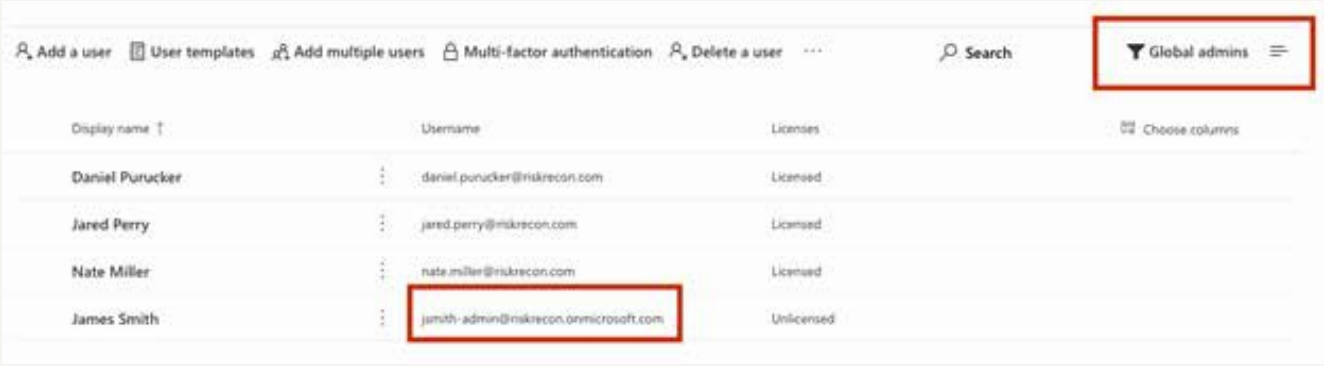
Given that it is the path of least resistance, attackers will target users with privileged access to the Microsoft 365 tenant. Using a privileged account for day-to-day use increases the likelihood that an attacker will gain privileged access to the environment if they are successfully exploited. As such, administrative personnel should use their privileged accounts only when it is required.

VALIDATION STEPS

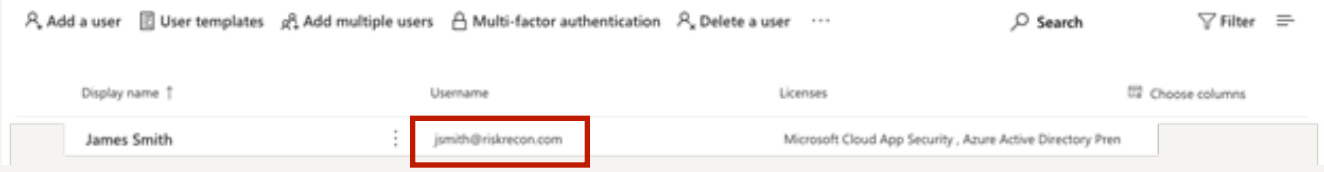
View all admin users by accessing the Microsoft 365 Admin portal's Active users screen:

1. Navigate to https://admin.microsoft.com/
2. Access the "Users" menu, then select "Active users"
3. Click the filter icon on the right side of the screen:
4. Select "Global Admins"
5. View an example user (e.g. jsmith-admin) with the Global Administrator role
6. Click the filter icon on the right side of the screen, and select "Clear Filter":
7. View an example user (e.g. jsmith) without the Global Administrator role

The screenshot below shows an example of a user with the Global Administrator role, with an obvious username:



The screenshot below shows an example of a non-admin user:



ID: o365 - 5: Are tenant Global administrators configured with working email addresses?

WHY IS THIS IMPORTANT?

Microsoft 365 Global Admins receive a variety of important email notifications that include service status, security events, and other information. When an organization first signs up for Microsoft 365, users are provisioned with a default username and email address in the username@organizationame.onmicrosoft.com format. For example, a new Global Admin, Larry Washington, at RiskRecon might have the following username: larry.washington@riskrecon.onmicrosoft.com. Since Larry is a Global Admin, Larry receives administrative notifications at his riskrecon.onmicrosoft.com email address. However if the organization doesn't use Microsoft 365 Outlook for email, Larry might not receive tenant administrative notification emails. Another scenario is Larry's Microsoft 365 username is larry.washington-admin@riskrecon.com. While this may be Larry's username on Microsoft 365, that may not be a valid email address. As such, it is important that organizations ensure that global admins use an email address that is configured to a working address.

VALIDATION STEPS

1. Navigate to https://portal.azure.com and select Azure AD
2. From the Manage menu on the left, select "Users"
3. Identify a Global Administrator from the list of users
4. Within the "Contact info" area, verify that the user's email is a working email address:

Figure 7: *Screenshot within the "Contact info" section showing a valid email address*

ACCEPTABLE RESPONSE(S)

- A working email address is configured for the Global Administrators

FAILURE RESPONSE(S)

- The email address field is blank or an invalid email address is configured for the user

SERVICE CONFIGURATION

WHAT

By default, Microsoft 365 is configured with settings that encourage sharing, collaboration, and ease of use. These default settings include allowing non-privileged users to invite guest users to the organization's Azure AD and default file sharing settings.

WHY

Depending on the organization's risk profile, the default settings may be overly permissive, resulting in leak of sensitive information and compromise of the integrity of the environment.

ID: o365 - 6: Are Azure AD User Settings configured from non-default settings?

WHY IS THIS IMPORTANT?

By default, non-administrative users may access the Azure AD administrative portal and perform several different actions including:

- Register custom-developed applications for use within Azure AD
- Access the Azure AD administrative portal
- Allow user to connect their Azure AD accounts with their LinkedIn account
- Invite external guest users
- Invited guest users can invite additional guest users

Each of these setting may have a security impact, depending on how the organization. If the target organization has not configured these default settings to be more restrictive, it is a tell-tale sign that the organization lacks Microsoft 365 security maturity.

VALIDATION STEPS

There are two screens to inspect to determine how the settings are configured. First, view the Azure AD User settings:

1. Navigate to HTTPS://PORTAL.AZURE.COM and select Azure AD
2. From the Manage menu on the left, select "User settings"
3. Inspect the three toggle settings:

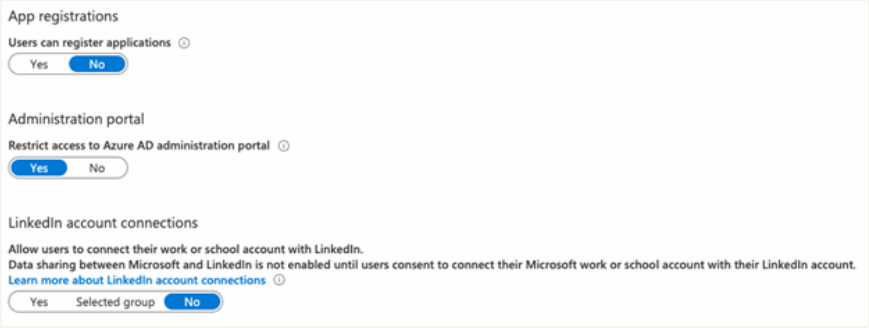


Figure 5: *Screenshot showing the most restrictive and secure settings*

4. Determine if the settings are appropriate for the organization

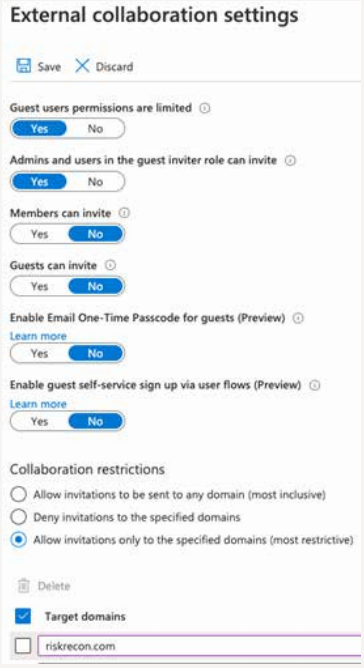


Figure 6: *Screenshot showing the most restrictive external collaboration settings*

ACCEPTABLE RESPONSE(S)

- Settings have been changed from the default

FAILURE RESPONSE(S)

- Settings are configured with the default settings

ID: o365 - 7: Are users restricted from creating auto-forwarding rules within Outlook?

WHY IS THIS IMPORTANT?

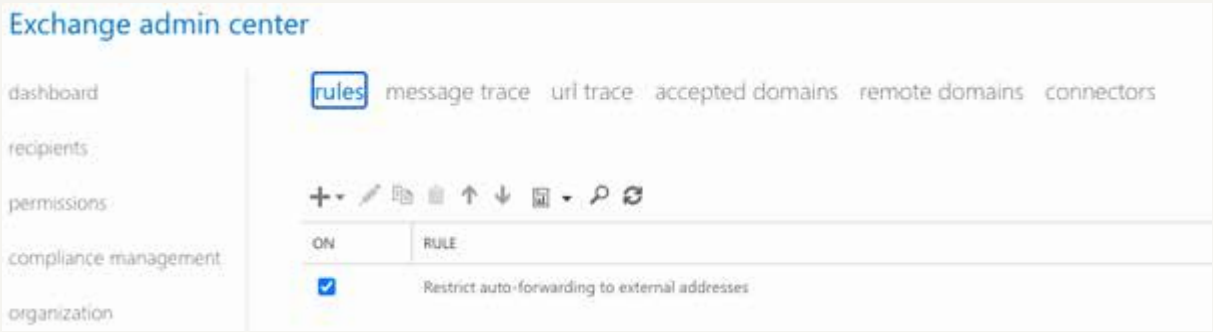
When a user creates an auto-forwarding rule, emails sent to the account are automatically forwarded without user notification to an email box that the organization does not control. This may expose the organization to risk of loss of sensitive data.

A techinique employed by hackers is to auto-forward email of compromised accounts to a private account, enabling them to monitor emails for sensitive information and to understand organizational controls and operations. They leverage this information to compromise other systems and execute fraudlent transactions, such as wire transfers and payroll modifications.

VALIDATION STEPS

1. Navigate to the Exchange Admin Center
2. Under the “mail flow” section, click “rules”:

3. Within the “rules” interface, identify a rule that prevents auto-forwarding to external addresses:



4. Inspect the rule to ensure it prevents auto-forwarding from internal users to external users:

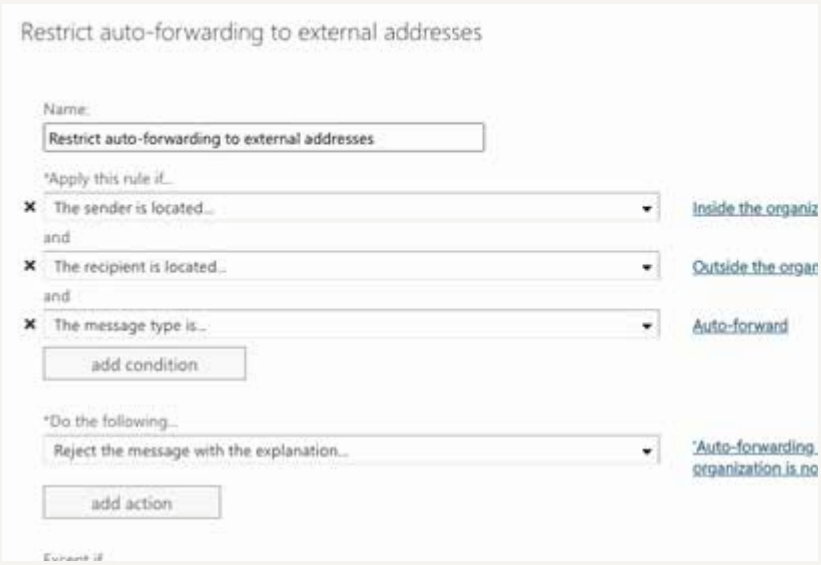


Figure 8: *Screenshot showing a rule that prevents internal users from auto-forwarding messages to external users*

Further information: HTTPS://SUPPORT.MICROSOFT.COM/EN-US/OFFICE/STOP-AUTO-FORWARDING-EMAILS-IN-MICROSOFT-365-F9D693BA-5C78-47C0-B156-8E461E062AA7

ACCEPTABLE RESPONSE(S)

- A rule is present thats restricts the forwarding of emails to external users

FAILURE RESPONSE(S)

- No rule is present that restricts the forwarding of emails to external users.

ID: o365 - 8: Are OneDrive links configured so that the default link type is “Shareable: Anyone with the link”?

WHY IS THIS IMPORTANT?

When a user creates a sharable OneDrive link, by default the link type is set to “Shareable: Anyone with the link”. The risk here is that if the link is forwarded in email or otherwise shared outside of the organization, anyone with the link will be able to access the OneDrive file. As such, it is more secure to configure the default OneDrive sharing setting to “Internal: Only people in your organization”. If a user needs to share the file with an external user, they may configure the link to “Shareable” – but the by default links will be internal-only.

VALIDATION STEPS

1. Navigate to the One Drive Admin screen
2. Under the menu on the left, click “Sharing”
3. Inspect the “Links” section and identify the default link type:

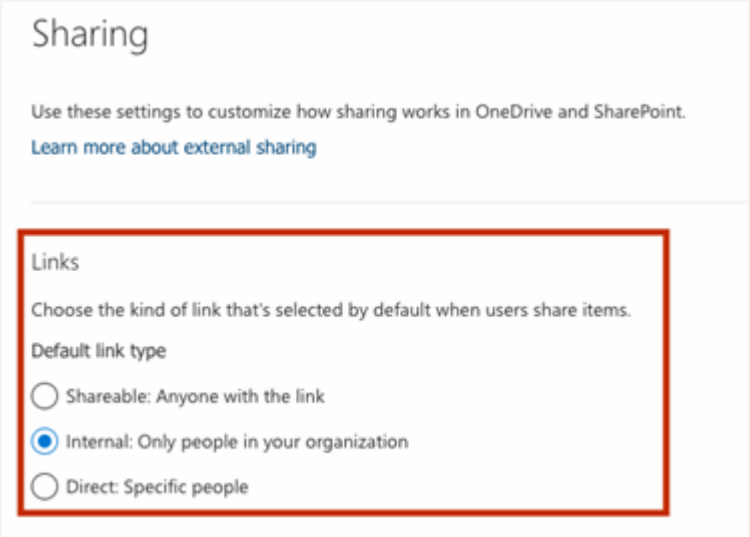


Figure 9: *Screenshot showing that Links are set to “Internal” by default*

ACCEPTABLE RESPONSE(S)

- The Links configuration is set to “Internal” or “Direct”

FAILURE RESPONSE(S)

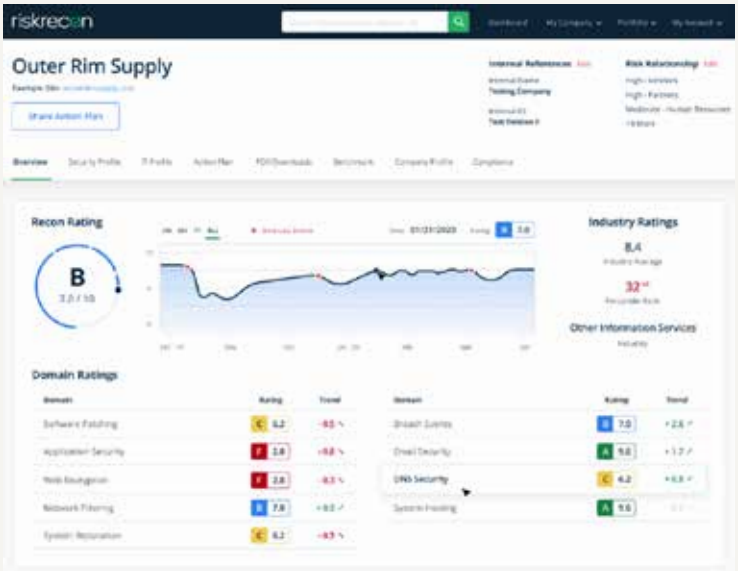
- The Links configuration is set to the default “Shareable”

ABOUT RISKRECON

RiskRecon is a leading global provider of Security Ratings Services that enable enterprises to easily understand and act on their cybersecurity risks. Customers use RiskRecon ratings and assessments to better manage risk across a wide range of contexts and use cases.

- Third-party risk teams use RiskRecon to make better vendor selection decisions and to hold existing vendors accountable to managing cybersecurity risks well.
- M&A teams use RiskRecon to assess acquisition targets for latent cybersecurity liabilities.
- Internal security analysts use RiskRecon to maintain a wholisitc understanding of their internet attack surface and related exposures, with particular focus on managing shadow IT and forgotten IT risk.
- CISOs and boards use ratings to benchmark their cybersecurity performance against peers and competitors.

In Q4 2018, Forrester named RiskRecon a leader in their Cybersecurity Risk Rating Solutions report. “RiskRecon stands out with its focus on contextualized, action-oriented cyber-risk ratings. Its Risk Priority matrix tool helps customers narrow down, prioritize, and take action on their top third-party cyber risks based on their unique business assets and security posture.” HTTPS://WWW.RISKRECON.COM/FORRESTER-REPORT



COPYRIGHT

LEGAL DISCLAIMER

RiskRecon, a Mastercard Company, makes no representations or warranties of any kind, express or implied, with respect to the contents of this document and the associated security questionnaire. Without limitation, RiskRecon specifically disclaims all representations and warranties, including but not limited to any and all implied warranties of merchantability, fitness or suitability for any purpose. Any action taken using the information in this document or the associated security questionnaire is strictly at the user's own risk.