Microsoft Security Report

FAQ

Logicom Cloud Business Unit
cloud@logicom.net

What is the Microsoft Security Report?

It is new intuitive report now available on Logicom Cloud Marketplace that provides detailed information on the MFA status for your customers' Azure Active Directory Tenants.

Where can I find the report?

The report is available under **LCMP -> Reporting -> Sales -> Microsoft Security Report**

How does the report help me?

The Microsoft Security Report helps you to:

- Objectively measure your Customers' Privileged accounts status in terms of MFA enablement.
- Plan MFA improvements for Privileged users
- Review the success of your improvements

How does the report work?

Microsoft Security Report collects the data available from **Azure AD Identity Secure Score** regarding the "**Require MFA for administrative roles**" improvement action **only** for Tenants that are using **Azure Plan** in Logicom Cloud Marketplace.
All data in the report can also be found under **Azure AD Identity Secure Score** service of each Tenant.

How often is the report updated?

At least three (3) times a week, Monday, Wednesday and Friday at 0:00.

Why is MFA important for Administrative roles?

Requiring multi-factor authentication (MFA) for all administrative roles makes it harder for attackers to access accounts.
Administrative roles have higher permissions than typical users. If any of those accounts are compromised, critical devices and data is open to attack.

Which administrative roles qualify as Privileged in the "Microsoft Security Report"?

At a **minimum**, the following roles need to be MFA secured:

- Security administrator
- Exchange service administrator
- Global administrator
- Conditional Access administrator
- SharePoint administrator
- Helpdesk administrator
- Billing administrator
- User administrator
- Authentication administrator

How is MFA scored?

You get a "**Privileged Account MFA %"** score of 100% if you have MFA configured based on Microsoft recommendations.
If you only have a subset of the total Privileged number of Privileged users protected, you would be given a partial score.
Also below are some additional elements of the report:

- **SecureScoreAdminMFAin%** - Average percentage of MFA configured on privileged accounts across all tenants.
- **FLOP Customers by MFA Score%** - Customers with lowest MFA percentage.
- **UserQty** - Total number of Privileged accounts in the tenant reported by Microsoft.
- **IsCompliant** -Tenant MFA compliance status.

What is "ISCompliant" status?

IsCompliant status measures the status of the tenant in terms of **Privileged Account MFA** configuration based on Microsoft recommendations.
It is calculated taking into count BRAKE GLASS account recommendation from Microsoft. Maximum 2 accounts could be without MFA, 1 for Partner, other for End customer. So if 6/8 have MFA configured it is considered **compliant**.

What does [Null] mean on "Customers with Null access"?

It means that no detailed information was returned during the report generation.
This can most likely occur either because it was not processed successfully or there is no DAP granted or there is a Conditional Access policy in place preventing access to that tenant.
Please note that there are cases where "Security Defaults" has been enabled and is reflected in the report for accounts where access status is NULL.

How can I improve the "Privileged Account MFA %" score?

If you are using **Azure Active Directory Free** versions with Office 365 or other SAAS/Web applications integrated with Azure Active Directory, then we suggest you enable "security defaults"

1. "Security defaults" achieves multiple objectives:
2. Requiring all users to register for Azure AD Multi-Factor Authentication.
3. Requiring administrators to do multi-factor authentication.
4. Blocking legacy authentication protocols.
5. Requiring users to do multi-factor authentication when necessary.
6. Protecting privileged activities like access to the Azure portal.

If you have invested in Azure Active Directory Premium P1 or P2 you can enable Conditional Access policies to enable custom policy enforcement for selected users or applications, under specific conditions.
Set up Azure Multi-Factor Authentication policies to protect devices and data that are accessible by your users with administrative roles: In the Azure AD Conditional Access portal

1. Select + New Policy
2. Go to Assignments > Users and groups > Include > choose Select users and groups > check Directory roles
3. At a minimum, select the following roles:
    - Security administrator
    - Exchange service administrator
    - Global administrator
    - Conditional Access administrator
    - SharePoint administrator
    - Helpdesk administrator
    - Billing administrator
    - User administrator
    - Authentication administrator
4. Go to Cloud apps or actions > Cloud apps > Include > select All cloud apps (and don't exclude any apps)
5. Under Access controls > Grant > select Grant access > check Require multi-factor authentication (and nothing else)
6. Enable policy > On
7. Create

NOTE: Classic Conditional Access policies are not scored. Use the recommended steps to receive credit.
NOTE: Security defaults and Conditional Access cannot be used side by side.

Emergency Access Accounts: If your organization has set up additional global admin accounts for **"break-glass"** scenarios which are not protected by MFA, it is recommended that you set this control's status to **"Risk accepted".**

Does the Privileged Account MFA% and the Average Microsoft Secure Score% measure my risk of getting breached?

In short, no. They do not express an absolute measure of how likely you are to get breached.
They express the extent to which you have adopted features that can offset the risk of being breached.
No service can guarantee that you will not be breached, and the scores should not be interpreted as a guarantee in any way.