



MFA fatigue attacks ?

An MFA fatigue attack occurs when a threat actor runs a script that **attempts to log in repeatedly with stolen credentials, resulting in an endless stream of MFA push requests** sent to the account holder's mobile device.

The target people are so overwhelmed that they **accidentally click the "Approve" button** or **simply accept the MFA request** to end the flood of notifications sent to their phone.

[Hackers use MFA fatigue to bypass multi-factor authentication - IT World Canada](#)

Case 1 : MFA Denials Timeline

Count the number of times MFA requests were denied within a specified time interval (e.g., every one hour) and evaluate the risk based on the number of failed attempts.

```
// case 1 : MFA Denials Timeline
AADSignInEventsBeta
| where Timestamp > ago(1d)
| where ClientAppUsed == "Browser"
| where AuthenticationRequirement == "multiFactorAuthentication"
| where ErrorCode == 50074
| extend Detail = strcat(Country, "¥¥", IPAddress, "¥¥", Application, "¥¥",
UserAgent)
| summarize MFA_Deny_Detail = make_list_if(Detail, ErrorCode == 50074) by
AccountUpn, bin(Timestamp, 1h)
| extend MFA_Deny = array_length(MFA_Deny_Detail)
| extend MFA_Risk = case(MFA_Deny >= 9, "High",
                        MFA_Deny >= 4, "Medium",
                        "Low")
| project Timestamp, AccountUpn, MFA_Deny, MFA_Risk, MFA_Deny_Detail
| order by Timestamp desc
```

AADSTS50074 UserStrongAuthClientAuthNRequiredInterrupt - Strong authentication is required and the user did not pass the MFA challenge.

[Defend your users from MFA fatigue attacks - Microsoft Community Hub](#)
[Azure AD authentication & authorization error codes - Microsoft Entra | Microsoft Learn](#)

Initial
Access

Execution

Persistence

Privilege
Escalation

Credential
Access

Collection

Exfiltration

Impact

