BENIGN 91/100

New-location sign-in for user2@example.com from Chicago matches her calendar-confirmed conference travel - MFA satisfied on her registered, Intune-compliant laptop with clean post-sign-in activity; no action required, auto-resolve the remaining travel-window alerts.

HOST Microsoft 365 (cloud) USER **user2@example.com** TIME **2026-07-08T18:12:44Z**

MITRE **T1078.004 (Valid Accounts: Cloud Accounts - ruled out)** SEVERITY LOW

Org: ORG001 · Alert ORG001-MSFT-1 · Generated 2026-07-08T18:41:19Z

EXECUTIVE SUMMARY

The "Sign-in from a new location" alert on `user2@example.com` (Sarah M., Marketing) is a false positive triggered by expected business travel. Her Outlook calendar contains a confirmed "B2B Marketing Summit - Chicago (McCormick Place)" event spanning 2026-07-06 to 2026-07-10, with a matching airline itinerary (MAN to ORD) and a hotel booking 0.8 mi from the venue in her mailbox. The flagged sign-in at 18:12:44Z originated from `203.0.113.87`, a hotel guest network in Chicago, on her registered Entra-joined, Intune-compliant laptop `DESKTOP-SM-4421` - the same device ID seen in 96% of her sign-ins over the trailing 30 days - and satisfied MFA via a Microsoft Authenticator push. The impossible-travel check passes against her prior Manchester sign-in 74 hours earlier, Entra ID Protection assessed the session risk as low with only the `unfamiliarFeatures` detection firing, and the Unified Audit Log shows routine Outlook, Teams, and SharePoint usage with no inbox rules, consent grants, or unusual data access. No action is required on this alert; the pattern will recur through the conference window and should auto-resolve when MFA, device compliance, and calendar travel corroborate.

ALERT DETAILS

CREATED AT	2026-07-08T18:12:44Z
HOST	Microsoft 365 (cloud); application: Office 365 Exchange Online (Outlook desktop), followed by Teams and SharePoint Online sessions
USER	`user2@example.com` (Sarah M., Marketing)
SEVERITY	LOW
MITRE	T1078.004 (Valid Accounts: Cloud Accounts - ruled out)
DETECTION	Entra ID Protection `unfamiliarFeatures` (Unfamiliar sign-in properties: new location); sign-in risk assessed low
SOURCE IP	`203.0.113.87` (US/Chicago, IL; ASN 64501 - Example Hospitality Networks, hotel guest Wi-Fi)
DEVICE	`DESKTOP-SM-4421` - Entra-joined, Intune-compliant, Windows 11; matches the user's primary laptop (96% of trailing-30-day sign-ins)

AUTH DETAIL	Password + Microsoft Authenticator push (MFA satisfied); CA policy `Require MFA - All Users` applied - success
BUSINESS SIGNAL	Calendar event "B2B Marketing Summit - Chicago (McCormick Place)" 2026-07-06 to 2026-07-10 (created 2026-06-11); airline itinerary MAN to ORD and hotel confirmation in mailbox
PRIOR CASES	No prior cases for this user; new-location alerts corroborated by travel context have historically resolved benign org-wide

INVESTIGATION QUESTIONS

Is the new sign-in location consistent with the user's expected whereabouts?

• The sign-in aligns with confirmed conference travel to Chicago, corroborated by the user's calendar, flight itinerary, and hotel booking.

- Outlook calendar contains an all-day event "B2B Marketing Summit - Chicago (McCormick Place)" from 2026-07-06 through 2026-07-10, created 2026-06-11 with a registration confirmation attached
- Mailbox shows an airline itinerary (MAN to ORD, arriving 2026-07-06) and a hotel confirmation for a property 0.8 mi from the conference venue
- Source IP `203.0.113.87` resolves to a hospitality/guest Wi-Fi ASN in Chicago, IL - consistent with a hotel network, not datacenter or hosting infrastructure
- Impossible-travel check passes: last prior sign-in was 2026-07-05T16:03Z from Manchester, UK - roughly 74 hours before the Chicago sign-in, far exceeding the required flight time
- Sign-in at 13:12 local (CDT) falls within the user's normal working-hours pattern

▸ How we got the answer (3 data points)

Was the authentication itself trustworthy - MFA, device, and session properties?

• MFA was satisfied via Authenticator push on the user's registered, Intune-compliant corporate device, with no anomalous session properties.

- Authentication requirement `multiFactorAuthentication` met via Microsoft Authenticator push notification, approved 41 seconds after challenge
- Device `DESKTOP-SM-4421` is Entra-joined and Intune-compliant; the same device ID appears in 96% of the user's sign-ins over the trailing 30 days
- User agent and client (Outlook desktop, modern auth) match the user's established profile - no legacy protocols (IMAP/POP/SMTP AUTH) observed
- Entra ID Protection sign-in risk assessed as low; only detection fired was `unfamiliarFeatures` (new location), with no anonymized-IP, token-anomaly, or password-spray detections
- No failed sign-in attempts against the account in the preceding 72 hours - no evidence of credential guessing before the successful login

▸ How we got the answer (2 data points)

Is there any anomalous post-sign-in activity - inbox rules, consent grants, or unusual data access?

- **Post-authentication activity is routine productivity usage consistent with conference attendance, with no persistence or exfiltration indicators.**

- Unified Audit Log for 2026-07-08T18:12Z to 2026-07-09T14:00Z shows only Outlook mail sync, Teams messaging, and reads of 6 SharePoint files the user already owned or had recently edited
- No `New-InboxRule`, `Set-Mailbox` (forwarding), or mailbox-permission changes during or after the session
- No OAuth application consent grants, MFA-method changes, or device registrations from the new location
- No mass download, sharing, or eDiscovery activity - SharePoint/OneDrive volumes are within the user's 30-day baseline
- Subsequent sign-ins on 2026-07-09 originate from the same Chicago IP block and the conference venue's guest network, both MFA-satisfied on the same device

▸ How we got the answer (3 data points)

Is the source IP (203.0.113.87) suspicious - VPN, proxy, or threat-actor infrastructure?

- **The IP is a shared hospitality NAT with no VPN, proxy, or Tor flags; two low-confidence threat-intel hits are consistent with guest-network noise.**

- ASN 64501 (Example Hospitality Networks) - classified as ISP/hospitality, not datacenter or hosting infrastructure
- All enrichment sources (IPAPI, IPRegistry, VirusTotal RDAP) return `is_vpn=false`, `is_proxy=false`, `is_tor=false`, `is_datacenter=false`
- 2 of 93 VirusTotal engines flagged the IP (GreyNoise, SOCRadar) - expected for a high-churn hotel guest NAT shared by hundreds of devices; 57 engines returned harmless
- Geolocation (Chicago, IL) is 0.8 mi from the user's hotel booking and matches the conference geography exactly
- No other tenant accounts authenticated from this IP in the 7-day window - no sign of shared attacker infrastructure targeting the org

▸ How we got the answer (2 data points)

CONCLUSION

This alert is a false positive produced by expected travel. The `unfamiliarFeatures` detection fired solely because Chicago was a new authentication location for `user2@example.com` - a user attending a multi-day marketing conference confirmed by her calendar, flight itinerary, and hotel booking. The sign-in satisfied MFA on her registered, Intune-compliant laptop, originated from a legitimate hospitality network whose two low-confidence threat-intel hits match ordinary guest-NAT noise, passed the impossible-travel check against her prior Manchester sign-in, and was followed by entirely routine mailbox and collaboration activity. There is no indication of credential compromise, session hijacking, or account misuse, and no follow-up action is required on this alert. The same pattern will recur through the conference window ending 2026-07-10 and should be auto-resolved when travel corroboration is present.

RECOMMENDED ACTIONS

RECOMMENDED

1 MEDIUM **Auto-resolve new-location alerts corroborated by travel context** - When a new-location sign-in satisfies MFA on a compliant registered device and the user's calendar contains overlapping travel to the sign-in geography, route the alert to auto-close with an audit note instead of the analyst queue. This pattern will recur throughout the conference window (2026-07-06 to 2026-07-10) and for future business travel.

2 LOW **Keep risk-based Conditional Access as the enforcement layer** - The existing `Require MFA - All Users` policy correctly challenged and cleared this sign-in. Confirm the sign-in risk policy continues to require MFA (or block) at medium/high risk so genuinely anomalous new-location sign-ins still receive step-up enforcement rather than notification only.

▾ Activity Timeline

2026-06-11 (prior month)	Calendar event "B2B Marketing Summit - Chicago (McCormick Place), Jul 6-10" created by user2@example.com with registration confirmation attached
2026-07-05T16:03:11Z	Last pre-travel sign-in from Manchester, UK (home geography) - login success, risk: none
2026-07-08T18:12:44Z	Sign-in from 203.0.113.87 (Chicago, IL - hotel guest network) to Exchange Online on DESKTOP-SM-4421 - MFA challenge issued; alert triggered (unfamiliarFeatures)
2026-07-08T18:13:25Z	Microsoft Authenticator push approved - MFA satisfied, CA policy passed, session established
2026-07-08T18:14-22:40Z	Routine Outlook mail sync, Teams messages, and reads of 6 user-owned SharePoint files - volumes within 30-day baseline
2026-07-09T13:05:52Z	Follow-on sign-in from the conference venue guest network (same Chicago IP block), MFA satisfied, same device - no new alert state