NEEDS ATTENTION **61/100**

IT lead user5@example.com disabled MFA on service account svc-zendesk@example.com from a legitimate admin session to unblock the Zendesk integration - plausible fix, but no change record exists and the account now sits password-only; confirm with the admin and restore a phishing-resistant auth path within 24h.

HOST Okta (cloud), org example.okta.com | USER **user5@example.com** | TIME **2026-07-09T11:08:36Z**

MITRE **T1556.006 (Modify Authentication Process: MFA) - policy change observed; malicious intent not established**

SEVERITY MEDIUM

Org: ORG001 · Alert ORG001-OKTA-1 · Generated 2026-07-09T11:58:22Z

EXECUTIVE SUMMARY

The "MFA disabled on an admin account" alert reflects a real, security-relevant change made through a legitimate channel with a plausible but unverified justification. At 11:08Z, `user5@example.com` (IT lead) used the Okta admin console to exclude `svc-zendesk@example.com` from the MFA sign-on policy and reset its enrolled factors. The admin session itself is clean: it originated from his managed device on office egress, was itself MFA-authenticated, and contains no other risky administrative actions. The timing correlates with a Zendesk integration outage visible in the ITSM queue (ticket `ITSM-5527`, "Zendesk sync failing since API update", opened 10:22Z) and a Zendesk sync-error burst in application logs - the integration authenticates with username/password and breaks when MFA is enforced. However, no change record covers the modification, the service account also holds the `Application Administrator` Okta role, and it is now protected by a single static password. Nothing indicates compromise, but the change created standing risk outside change management. The required outcome is a two-minute confirmation with the IT lead, then either restoring MFA with an integration-compatible auth method (OAuth/API token) or a documented, time-boxed exception with compensating controls.

ALERT DETAILS

CREATED AT	2026-07-09T11:08:36Z
HOST	Okta (cloud), org `example.okta.com`
USER	Actor: `user5@example.com` (IT lead, Super Administrator); Target: `svc-zendesk@example.com` (service account, Application Administrator role)
SEVERITY	MEDIUM
MITRE	T1556.006 (Modify Authentication Process: MFA) - policy change observed; malicious intent not established
PATTERN	Admin excluded a privileged service account from the MFA sign-on policy and reset its enrolled factors in a single console session

EVENTS	`policy.rule.update` (MFA policy exclusion added, 11:07:58Z), `user.mfa.factor.reset_all` (11:08:21Z)
ACTOR SESSION	Managed device `LT-IT-0051`, office egress `203.0.113.30`, admin sign-in MFA-satisfied (Okta Verify push) at 11:02:14Z
BUSINESS SIGNAL	ITSM ticket `ITSM-5527` "Zendesk sync failing since API update" opened 10:22Z; Zendesk integration auth errors 10:14-11:09Z
CHANGE RECORD	None - no change request, approval, or maintenance window covers this modification
PRIOR CASES	No prior MFA-modification cases for this actor or account; last MFA policy change in the org was 2026-05-18 via approved change CHG-2190

INVESTIGATION QUESTIONS

What exactly changed, and what is the resulting security posture of the account?

• The service account was excluded from the MFA sign-on policy and its factors were reset, leaving a privileged, internet-reachable account protected by a single static password.

- `policy.rule.update` at 11:07:58Z added `svc-zendesk@example.com` to the exclusion list of the "Require MFA - All Users" sign-on policy rule
- `user.mfa.factor.reset_all` at 11:08:21Z removed the account's enrolled Okta Verify factor
- The account holds the `Application Administrator` Okta admin role (granted 2025-11 for app provisioning) in addition to its Zendesk integration scope - broader than the integration requires
- Sign-in for the account is now password-only, with the password last rotated 148 days ago per credential metadata
- No network zone or client allowlist restricts where the account can authenticate from, so the exposure is internet-wide

▸ How we got the answer (2 data points)

Is the actor's admin session legitimate, or could the admin account itself be compromised?

• The session is consistent with the genuine IT lead: MFA-satisfied sign-in from his managed device on office egress, matching his behavioral baseline, with no other risky admin actions in the session.

- Admin sign-in at 11:02:14Z from managed device `LT-IT-0051` and office egress `203.0.113.30`, Okta Verify push satisfied
- Device, IP, browser fingerprint, and working-hours timing all match the actor's 90-day baseline; Okta ThreatInsight and behavioral detection raised no risk on the session
- Session actions were narrowly scoped: policy exclusion, factor reset, and viewing the Zendesk app configuration - no user creation, role grants, API token minting, or other policy edits
- No impossible-travel, new-device, or password-change events on the actor's account in the trailing 7 days
- The actor was active in the correlated ITSM ticket `ITSM-5527` eleven minutes before the change, commenting that the sync failure pointed at authentication

▸ How we got the answer (2 data points)

Is there corroborating business justification, and was the change properly authorized?

• The Zendesk outage is real and the timing fits a break-fix, but the change bypassed change management entirely: no ticket, no approval, no maintenance window, and no documented rollback plan.

- ITSM ticket `ITSM-5527` (opened 10:22Z) reports Zendesk sync failures; application logs show authentication errors for the integration starting 10:14Z, stopping at 11:09Z immediately after the MFA change
- The integration authenticates with username/password against Okta; MFA enforcement on the service account is incompatible with that flow, making the exclusion a plausible quick fix
- No change request references the modification; org policy classifies authentication-policy changes as normal changes requiring approval, and the last comparable change (2026-05-18) followed CHG-2190 properly
- The ITSM ticket was not updated to record the fix - the causal link is inferred from timing, not documented by the actor
- No time-box or rollback was set: the exclusion is permanent as configured, which converts a break-fix into standing risk

▸ How we got the answer (3 data points)

Has the weakened account been abused since the change?

• No misuse so far - the only sign-ins since the change are the integration's expected pattern - but the account is newly password-only with admin privileges, so the clean window is short and monitoring must continue until MFA or token auth is restored.

- Post-change sign-ins for `svc-zendesk@example.com` match the integration's baseline: Zendesk connector IP range, expected user agent, regular sync cadence
- No sign-in attempts from unfamiliar IPs, no failed-login bursts, and no ThreatInsight flags against the account since 11:08Z
- No admin-role usage by the service account (it has never exercised its Application Administrator role in 90 days of logs, supporting privilege reduction)
- No new API tokens, app assignments, or profile changes on the account since the modification
- Monitoring window is only a few hours; a password-only privileged account remains an attractive target until remediated

▸ How we got the answer (2 data points)

CONCLUSION

This is not an attack, but it is not closable as benign either. A legitimate, MFA-authenticated IT lead session made a real security regression - excluding a privileged service account from MFA and wiping its factors - to resolve a genuine Zendesk integration outage, and the fix worked. What is missing is everything change management exists for: authorization, documentation, a time-box, and a rollback plan. The account now runs password-only with an unused admin role and no network restriction, which is standing risk regardless of intent. The verdict is needs-attention: a two-minute confirmation with `user5@example.com` to validate intent, followed within 24 hours by a proper fix - migrate the Zendesk integration to OAuth or an API token

and re-enroll MFA, or document a time-boxed exception with a network-zone restriction and stepped-up monitoring. The unused Application Administrator role should be dropped in the same pass.

RECOMMENDED ACTIONS

MUST DO

1 HIGH **Confirm intent with the IT lead and file a retroactive change record** - Verify with user5@example.com that he made the change for ITSM-5527, link the fix to the ticket, and open a retroactive change request capturing scope, justification, and rollback so the modification is governed.

2 HIGH **Restore strong authentication for svc-zendesk within 24 hours** - Migrate the Zendesk integration to OAuth or a scoped API token (removing the password-auth dependency), then re-enroll MFA and remove the sign-on policy exclusion. If migration cannot land in 24h, apply a network-zone restriction limiting the account to the Zendesk connector IP range as an interim control.

RECOMMENDED

3 MEDIUM **Remove the unused Application Administrator role from the service account** - 90 days of logs show the role has never been exercised; dropping it reduces the blast radius of any future credential compromise to the Zendesk integration scope only.

4 MEDIUM **Rotate the service account password** - The password is 148 days old and is now the sole authentication factor; rotate it as part of the remediation regardless of which auth path is chosen.

5 MEDIUM **Alert on MFA policy exclusions for privileged accounts with change-record correlation** - Keep this detection, but enrich it with change-management lookup so approved changes route to auto-triage while unticketed modifications (like this one) escalate for confirmation.

6 LOW **Define a service-account authentication standard** - Document that integration service accounts use OAuth or API tokens, never interactive password auth, so MFA enforcement and integration functionality stop colliding in future break-fixes.

Activity Timeline

2026-07-09T10:14:32Z	Zendesk integration begins failing authentication against Okta (API update changed the auth handshake); sync errors accumulate
2026-07-09T10:22:05Z	ITSM ticket ITSM-5527 opened: "Zendesk sync failing since API update" (P2)
2026-07-09T10:51:47Z	user5@example.com comments on ITSM-5527 that the failure appears authentication-related
2026-07-09T11:02:14Z	user5@example.com signs in to the Okta admin console from managed device LT-IT-0051, office egress; Okta Verify push satisfied
2026-07-09T11:07:58Z	policy.rule.update: svc-zendesk@example.com added to the MFA sign-on policy exclusion list
2026-07-09T11:08:21Z	user.mfa.factor.reset_all: enrolled factors removed from the service account - alert triggered
2026-07-09T11:09:03Z	Zendesk integration authentication errors stop; sync jobs recover
2026-07-09T11:40Z	Post-change monitoring: only expected connector sign-ins observed; no unfamiliar sources, no failed-login activity