TEAMS & TELEFONIE

Teams: Granulare Conditional-Access-Anforderungen für einzelne Besprechungen (Preview ab Ende November 2026)

Executive Summary

Bisher kannte Conditional Access in Teams genau zwei Lautstärken: aus oder Vorschlaghammer. Entweder galt eine Richtlinie für die ganze Teams-App (und wegen der Abhängigkeiten gleich für halb Microsoft 365), oder eben gar nicht. Laut Microsoft-Ankündigung MC1532256 ändert sich das: Ab **Ende November 2026** startet die Public Preview für **granularen Conditional Access in Teams-Besprechungen**, die allgemeine Verfügbarkeit ist für **Januar 2027** angepeilt.

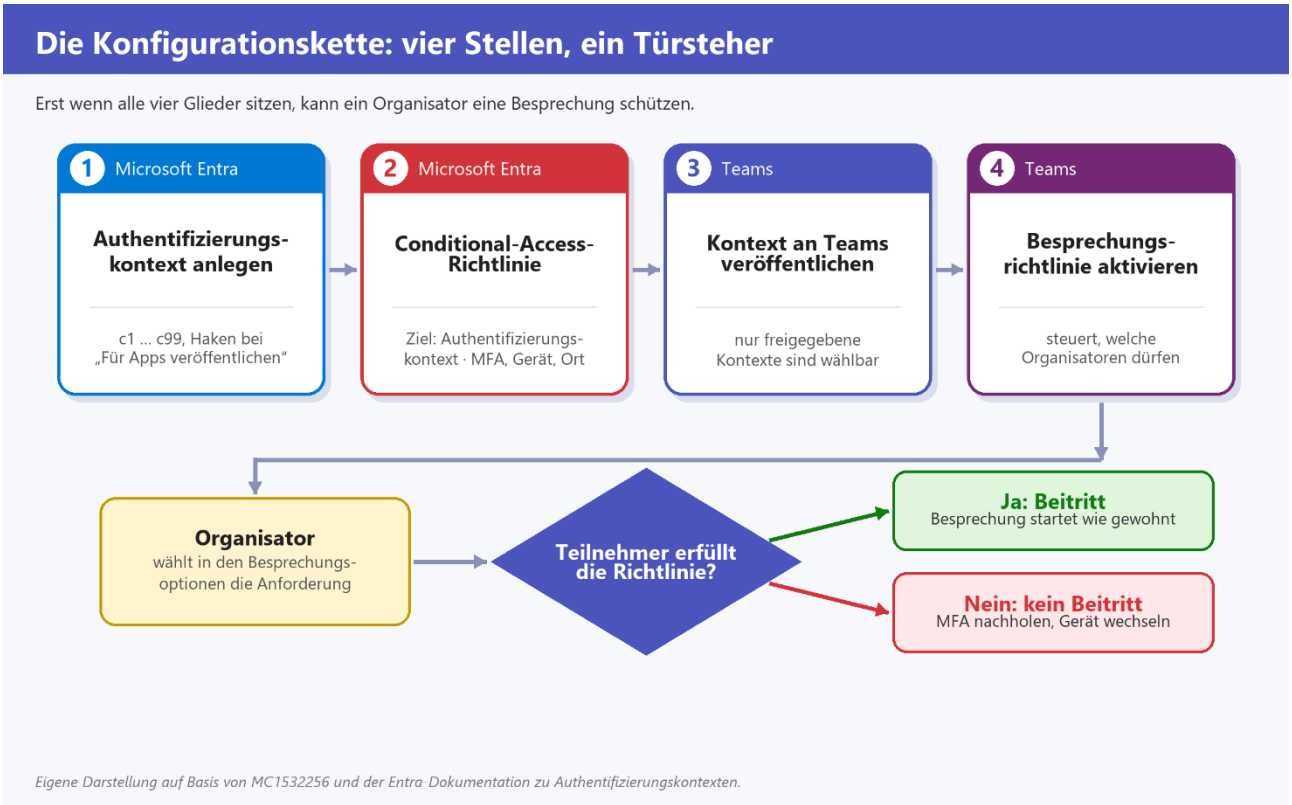
Das Prinzip: Ein Organisator markiert eine einzelne Besprechung als schutzbedürftig, und jeder Teilnehmer muss vor dem Beitritt eine Conditional-Access-Richtlinie erfüllen, also etwa MFA, ein konformes Gerät oder einen zugelassenen Standort. Die Vorstandssitzung bekommt einen Türsteher, das Kantinen-Standup bleibt Laufkundschaft.

- **Was:** Conditional Access pro Besprechung statt pro App, technisch über Authentifizierungskontexte aus Microsoft Entra.
- **Wer muss handeln:** Die Administration. Ohne vier vorbereitete Bausteine sieht kein Organisator die Funktion.
- **Wie dringend:** Opt-in, keine harte Frist. Aber die Preview ist dein Testfenster, und Betriebsrat oder Personalrat brauchen Vorlauf.
- **Empfehlung:** Im November Bestand prüfen, ab Preview-Start mit einer Pilotgruppe testen, ab Januar 2027 gezielt für Vorstand, Personalwesen und Gremien ausrollen.

Worum geht es im Detail?

Damit du verstehst, warum das mehr ist als ein neuer Schalter, lohnt ein Blick in den Maschinenraum. Conditional Access wertet Anmeldungen gegen **Zielressourcen** aus. Lange waren das Apps: Exchange, SharePoint, Teams. Microsoft empfiehlt selbst, die Microsoft-365-Dienste möglichst gebündelt als „Office 365“ anzusprechen, weil Teams intern auf SharePoint und Exchange zugreift und einzelne Richtlinien sonst Lücken oder Kollateralschäden erzeugen. Für eine einzelne Besprechung war da schlicht kein Platz.

Die Lösung heißt **Authentifizierungskontext**. Das Konzept ist nicht neu: SharePoint-Websites, Privileged Identity Management, Defender for Cloud Apps und eigene Anwendungen nutzen es seit Jahren. Ein Authentifizierungskontext ist ein Etikett mit einer ID von c1 bis c99, maximal 99 Stück pro Mandant. Eine Conditional-Access-Richtlinie zielt nicht auf eine App, sondern auf dieses Etikett. Und eine Anwendung, die den Kontext kennt, verlangt ihn genau dann, wenn jemand die geschützte Sache öffnen will. Neu ist, dass Teams diese Sprache jetzt auch für Besprechungen spricht.



Die Kette hat vier Glieder, und laut MC1532256 musst du alle vier selbst schmieden: Authentifizierungskontext in Entra anlegen, eine Conditional-Access-Richtlinie darauf ausrichten, den Kontext für Teams veröffentlichen und die Funktion über eine Teams-Besprechungsrichtlinie für die gewünschten Organisatoren freischalten. Erst dann taucht in den Besprechungsoptionen die Auswahl auf. Fehlt ein Glied, passiert nichts. Kein Fehler, kein Hinweis, einfach nichts. Das ist die bequemste Form von Fehlkonfiguration, weil sich niemand beschwert.

Fakten: Was Microsoft bisher bestätigt

Public Preview weltweit ab Ende November 2026, allgemeine Verfügbarkeit Anfang bis Ende Januar 2027 (MC1532256). Der Roadmap-Eintrag 571879 nannte zwischenzeitlich noch November 2026 für die GA und listet Desktop, Web, Mac, iOS und Android.

Unterstützte Anforderungen laut Meldung: zusätzliche Verifizierung wie MFA, Gerätekonformität und standortbasierte Kontrollen.

Das Feature ist opt-in: Ohne Admin-Konfiguration ändert sich für niemanden etwas.

Den aktuellen Stand verfolgst du im Microsoft-365-Roadmap-Eintrag 571879; die Grundlagen zum Anlegen von Kontexten erklärt Microsoft Learn im Artikel Zielressourcen in Conditional-Access-Richtlinien.

Wichtig ist die Abgrenzung zu dem, was du für Besprechungen schon hast. Lobby, Vertraulichkeitsbezeichnungen, Besprechungsvorlagen, Wasserzeichen und Ende-zu-Ende-Verschlüsselung regeln, **was in der Besprechung passiert**. Conditional Access regelt, **unter welchen Bedingungen jemand überhaupt hineinkommt**: mit welchem Gerät, von wo, mit welcher Authentifizierungsstärke. Die Lobby prüft Gesichter, Conditional Access prüft Ausweise.

Mechanismus	Prüft	Wer entscheidet	Lizenz
Lobby	Wer darf direkt rein, wer	Organisator, Richtlinie	Teams-Grundlizenz

Mechanismus	Prüft	Wer entscheidet	Lizenz
	wartet		
Vertraulichkeitsbezeichnung / Vorlage	Besprechungsoptionen erzwingen (Chat, Aufzeichnung, Lobby)	Organisator wählt Bezeichnung	Teams Premium
Wasserzeichen, Ende-zu-Ende-Verschlüsselung	Was mit Inhalten passiert	Bezeichnung, Vorlage, Organisator	Teams Premium
Granularer Conditional Access	MFA, Gerätezustand, Standort vor dem Beitritt	Admin stellt bereit, Organisator wählt	Entra ID P1 sicher; Teams-Seite noch offen

Und dann die Frage, die jedes Projekt eine Woche kostet: **Wen trifft die Prüfung überhaupt?** Conditional Access wirkt auf Identitäten, die sich in deinem Mandanten anmelden. Das sind deine eigenen Leute und B2B-Gäste. Externe aus Partnerorganisationen über den externen Zugriff (Federation) melden sich dagegen in ihrem eigenen Mandanten an; Microsoft Learn hält ausdrücklich fest, dass diese Form keine Entra-B2B-Konten nutzt und daher keine Conditional-Access-Richtlinien anwenden kann. Anonyme Teilnehmer und Einwahl per Telefon haben gar keine Identität, an der eine Richtlinie hängen könnte. Wie Teams diese Gruppen in einer geschützten Besprechung behandelt, hat Microsoft bisher nicht dokumentiert. Plane mit dem wahrscheinlichsten Fall: Sie kommen nicht rein.

Teilnehmergruppe	Richtlinie auswertbar?	Was du testen solltest
Eigene Belegschaft	Ja	Konformes Gerät, privates Gerät, mobil, unterwegs
B2B-Gäste	Ja, im Ressourcenmandanten	Vertrauen in MFA und Geräte des Heimatmandanten (mandantenübergreifende Zugriffseinstellungen)
Externer Zugriff (Federation)	Nach heutiger Doku nein	Ob der Beitritt geblockt oder in die Lobby gelenkt wird
Anonym	Nein	Blockade erwartet, Verhalten verifizieren
Telefoneinwahl	Nein	Ob Einwahl in geschützten Besprechungen möglich bleibt

Was sind Chancen? Was sind Risiken?

Fangen wir mit den Chancen an, denn die sind real. Viele Organisationen haben bisher mit einer unangenehmen Wahl gelebt: Entweder harte Gerätekonformität für ganz Teams, worauf sich der Außendienst mit dem Privathandy in den Chat-Untergrund verabschiedet. Oder lockere Regeln für alle, und die Aufsichtsratssitzung läuft auf demselben Sicherheitsniveau wie die Abstimmung über den Weihnachtsfeier-Termin. Granularer Conditional Access löst genau dieses Dilemma auf.

- **Schutz nach Inhalt, nicht nach Werkzeug:** Personalgespräche, Betriebsratssitzungen, Übernahmegespräche oder Beratungen über Sozialdaten bekommen strengere Regeln, alles andere bleibt bequem.
- **Phishing-resistente Anmeldung punktuell erzwingen:** Mit Authentifizierungsstärken kannst du für sensible Termine Passkeys oder FIDO2 verlangen, ohne gleich den ganzen Mandanten umzustellen.

- **Geräte-Hygiene sichtbar machen:** Wer an der Vorstandssitzung nicht teilnehmen kann, weil sein Laptop seit Juni kein Update gesehen hat, lernt schneller als in jeder Awareness-Schulung.
- **Nachweis gegenüber Prüfern:** Für Prüfungen nach ISO 27001, BSI IT-Grundschutz oder NIS2 ist dokumentierter Zugriffsschutz pro Vertraulichkeitsstufe ein sauberes Argument.

Jetzt zu den Risiken, und hier wird es dunkel. Spiel das Szenario durch, das bei SharePoint-Websites mit Authentifizierungskontext schon oft genug passiert ist: Die Geschäftsführung eines Maschinenbauers will drei Minuten vor der Bankenrunde vom privaten iPad beitreten. Die Richtlinie verlangt ein konformes Gerät. Das iPad ist konform mit genau einer Sache, nämlich dem Familien-Streaming-Abo. Der IT-Leiter erfährt von seiner neuen Sicherheitsarchitektur durch einen Anruf, den er noch beim Renteneintritt im Rücken spüren wird.

Warnung: Die Richtlinie ist schneller scharf als dein Helpdesk wach

Ein Organisator setzt die Anforderung mit zwei Klicks. Die Folgen tragen Teilnehmer, die davon erst beim Beitritt erfahren. Ohne Kommunikation produzierst du ausgerechnet in den wichtigsten Besprechungen die meisten Ausfälle.

Externe Partner, Steuerberater und Anwälte nehmen oft über den externen Zugriff oder anonym teil. Wenn sie draußen bleiben, ist das technisch korrekt und geschäftlich eine Katastrophe.

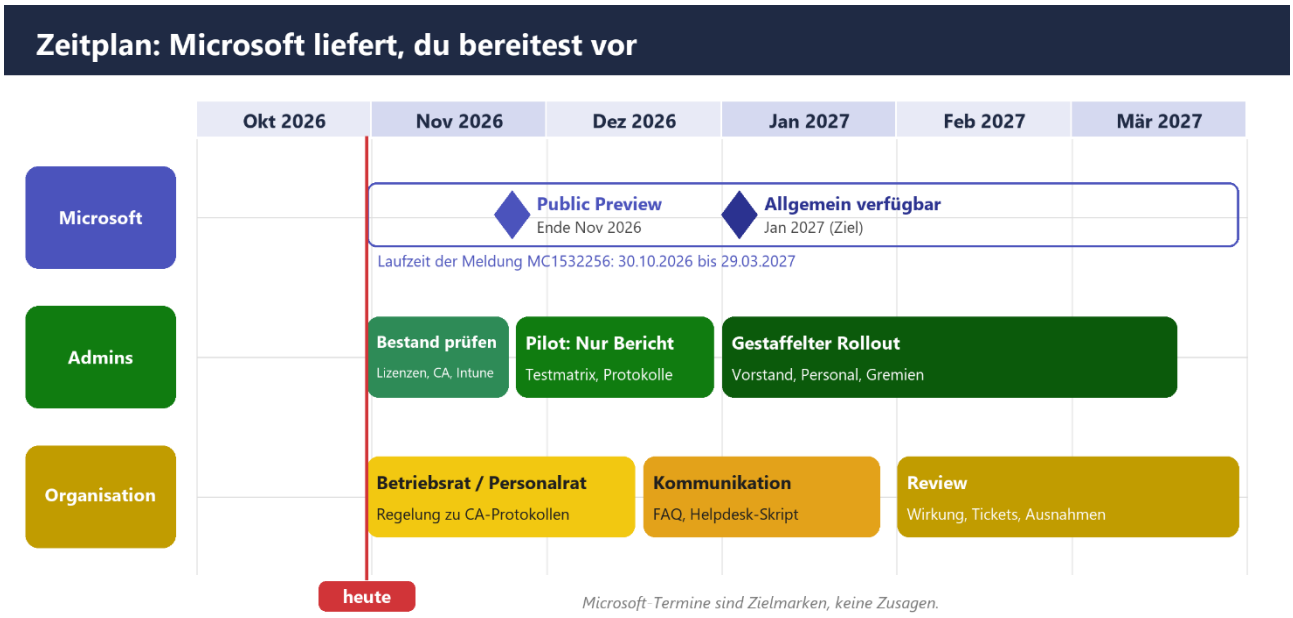
Dazu kommen handfeste Fragen für deutsche Organisationen. **Mitbestimmung:** Conditional Access protokolliert für jede Anmeldung Gerät, IP-Adresse, Standortbezug und Ergebnis. Neu ist, dass sich diese Daten jetzt auf konkrete Besprechungen beziehen lassen. Damit ist die Technik nach § 87 Abs. 1 Nr. 6 BetrVG zur Verhaltens- und Leistungskontrolle geeignet; die Personalvertretungsgesetze von Bund und Ländern kennen entsprechende Mitbestimmungstatbestände. Hast du eine Rahmenvereinbarung zu Microsoft 365, prüfe, ob Anmeldeprotokolle und Conditional Access abgedeckt sind. Wenn nicht: jetzt reden, nicht im Januar.

Datenschutz: Die Anmeldeprotokolle in Entra werden mit P1- oder P2-Lizenz 30 Tage vorgehalten, länger nur, wenn du sie in Log Analytics oder ein SIEM exportierst. Genau dort entsteht das Risiko, dass aus Sicherheitsprotokollen ein Teilnahmeregister wird. Ergänze das Verzeichnis der Verarbeitungstätigkeiten und lege Zugriffsrechte und Aufbewahrung fest.
Lizenzen: Conditional Access setzt Microsoft Entra ID P1 voraus, enthalten etwa in Microsoft 365 E3, E5 und Business Premium. Ob Microsoft die Teams-Seite der Funktion zusätzlich an Teams Premium bindet, steht in der Meldung nicht. Das wirst du spätestens zur allgemeinen Verfügbarkeit wissen; bis dahin gilt: kein Budget versprechen, das du nicht kennst.

Chance	Risiko	Gegenmittel
Strenger Schutz nur dort, wo nötig	Organisatoren setzen ihn überall „zur Sicherheit“	Besprechungsrichtlinie nur für definierte Organisatorengruppen
MFA und Gerätekonformität gezielt	Lockout kurz vor kritischen Terminen	Testbeitritt vorab, Helpdesk-Skript, Notfallkontakt
Nachweis für Audits	Anmeldeprotokolle werden zum Teilnahmeregister	Dienstvereinbarung, Zweckbindung, Rollenkonzept
Kein Vorschlaghammer für ganz Teams	Externe bleiben unbemerkt draußen	Einladungstext mit Anforderungen, Gastkonzept

Was müssen wir jetzt schon vorbereiten?

Gute Nachricht: Nichts brennt. Schlechte Nachricht: Gerade deshalb wird es liegen bleiben, bis im Januar jemand aus dem Vorstand fragt, warum das noch nicht läuft. Der folgende Zeitplan orientiert sich an den Terminen aus MC1532256 und lässt dir Luft für die Gremien.



Zeitpunkt	Schritt	Verantwortlich
Bis Mitte November 2026	Bestand prüfen: Entra-ID-P1-Abdeckung, bestehende Conditional-Access-Basisrichtlinien, Intune-Konformität, Gast- und Federation-Konzept	Identity-Team
Bis Mitte November 2026	Zwei bis drei Schutzstufen fachlich definieren und Namen festlegen, zum Beispiel „Vertraulich: verwaltetes Gerät“	IT-Sicherheit mit Fachbereichen
November 2026	Betriebsrat oder Personalrat informieren, Regelung zu Anmeldeprotokollen abstimmen, Datenschutz einbinden	IT-Leitung, Datenschutz
Ab Preview-Start Ende November	Authentifizierungskontext anlegen, „Für Apps veröffentlichen“ setzen, Richtlinie im Nur-Bericht-Modus, Pilotgruppe per Teams-Update-Richtlinie für Preview-Funktionen freischalten	Teams- und Identity-Admins
Dezember 2026	Testmatrix abarbeiten: alle Teilnehmergruppen, alle Plattformen, Anmeldeprotokolle auswerten	Teams-Admins
Ab Januar 2027 (GA)	Gestaffelter Rollout an Vorstand, Personalwesen, Gremien; Helpdesk-Skript und Kurzanleitung veröffentlichen	IT-Betrieb, Kommunikation
Bis Ende März 2027	Review: Tickets, Ausnahmen, tatsächliche Nutzung; Lizenzfrage final klären	IT-Leitung

Tipp: Kontexte sparsam benennen

Microsoft rät selbst, Authentifizierungskontexte ressourcenübergreifend zu benennen, etwa „Vertrauenswürdige Geräte“, statt für jede App einen eigenen zu bauen. Weniger Kontexte bedeuten weniger Umleitungen und weniger Verwirrung. Wenn du für SharePoint schon einen Kontext für vertrauliche Websites hast, prüfe, ob er für Besprechungen passt. Und lösche nie einen Kontext, der noch irgendwo hängt: Ohne Kontext ist die geschützte Ressource schlicht ungeschützt.

Wichtig: Erst Nur-Bericht-Modus, dann Ernstfall

Stell die Richtlinie zuerst auf „Nur Bericht“ und schau dir in den Anmeldeprotokollen an, wer durchgefallen wäre. Erfahrungsgemäß sind das deutlich mehr Leute, als die Gerätestatistik in Intune vermuten lässt, weil Konformität und Wirklichkeit selten befreundet sind.

Für die **Kommunikation an die Belegschaft** reichen drei Botschaften: Warum es die Funktion gibt (Schutz besonders sensibler Gespräche), woran man eine geschützte Besprechung erkennt, und was zu tun ist, wenn der Beitritt scheitert. Ergänze den Standard-Einladungstext für geschützte Termine um einen Satz wie „Teilnahme nur mit Firmengerät und Mehrfaktor-Anmeldung möglich“. Das kostet nichts und erspart dir die Hälfte der Tickets.

Tipp: Der Testbeitritt am Vortag

Führe für Gremiensitzungen eine Regel ein: Wer an einer geschützten Besprechung teilnimmt, klickt am Vortag einmal auf den Link. Klingt banal. Ist banal. Und rettet dir trotzdem jeden zweiten Montagmorgen.

Häufig gestellte Fragen

Ab wann kann ich Conditional Access für einzelne Teams-Besprechungen nutzen?

Laut Microsoft-Ankündigung MC1532256 startet die Public Preview weltweit Ende November 2026, die allgemeine Verfügbarkeit ist für Januar 2027 geplant. Die Funktion ist opt-in und wird erst sichtbar, wenn Administratoren Authentifizierungskontext, Conditional-Access-Richtlinie und Teams-Besprechungsrichtlinie eingerichtet haben.

Brauche ich Teams Premium für Conditional Access in Teams-Besprechungen?

Für Conditional Access selbst ist Microsoft Entra ID P1 nötig, das etwa in Microsoft 365 E3, E5 und Business Premium enthalten ist. Ob Microsoft die Besprechungsfunktion zusätzlich an Teams Premium bindet, ist bisher nicht veröffentlicht und sollte vor dem Rollout geprüft werden.

Können externe Teilnehmer an einer Teams-Besprechung mit Conditional-Access-Anforderung teilnehmen?

B2B-Gäste melden sich im Mandanten des Gastgebers an und können die Richtlinie grundsätzlich erfüllen, etwa über vertrauenswürdige MFA aus ihrem Heimatmandanten. Teilnehmer über den externen Zugriff, anonyme Teilnehmer und Telefoneinwahl lassen sich nicht per Conditional

Access prüfen und dürften daher keinen Zugang erhalten; das Verhalten sollte in der Preview getestet werden.

Was passiert, wenn ein Teilnehmer die Conditional-Access-Richtlinie nicht erfüllt?

Der Teilnehmer kann der geschützten Besprechung nicht beitreten, bis er die Anforderung erfüllt, zum Beispiel durch eine zusätzliche MFA-Anmeldung oder den Wechsel auf ein verwaltetes, konformes Gerät. Andere Besprechungen ohne diese Anforderung sind davon nicht betroffen.

Muss der Betriebsrat bei Conditional Access für Teams-Besprechungen zustimmen?

In der Regel ja, denn die Anmeldeprotokolle erfassen Gerät, IP-Adresse und Ergebnis pro Beitritt und sind damit zur Verhaltens- und Leistungskontrolle geeignet, was nach § 87 Abs. 1 Nr. 6 BetrVG mitbestimmungspflichtig ist. Im öffentlichen Dienst gelten entsprechende Regelungen der Personalvertretungsgesetze.