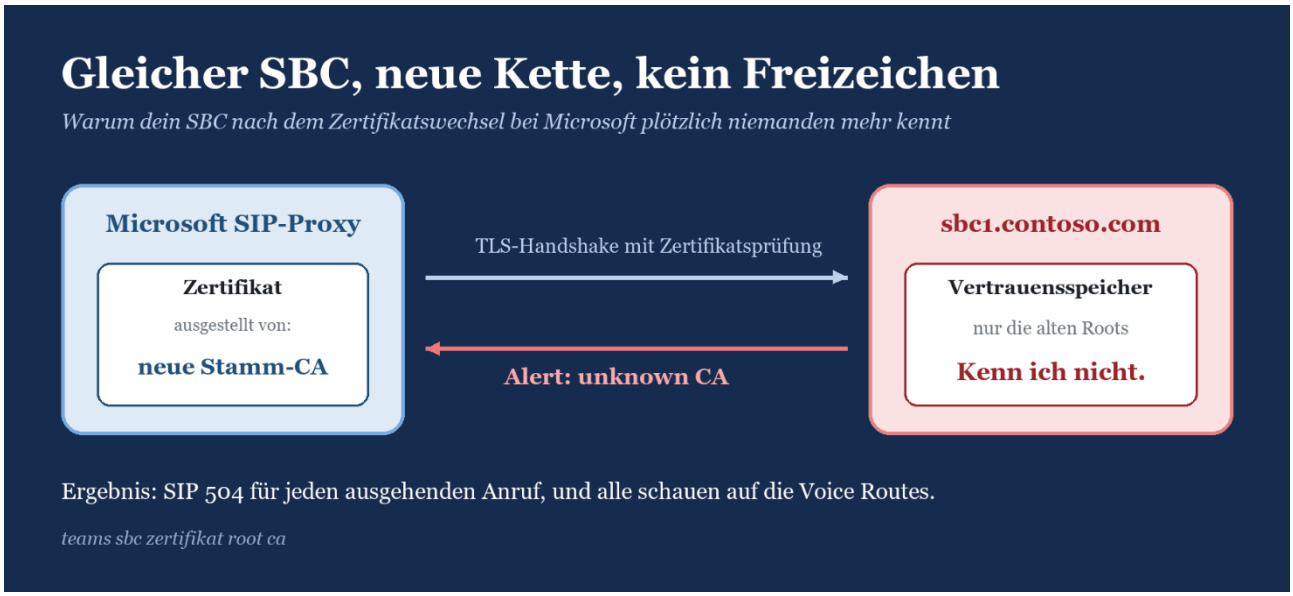
SIP 504 nach dem Zertifikatswechsel: Root-CAs am SBC aktualisieren



WISSEN
Alles zur Teams-Telefonie: Direct Routing, SBC, Wählpläne, Routing, Notruf und Betrieb an einem Ort.
› Teams-Telefonie

BERATUNG
Dein SBC und Microsoft reden nicht mehr miteinander, und keiner weiß, warum? Wir sortieren das mit dir.
› Beratung zur Teams-Telefonie

SCHULUNG
Für Admins, die Zertifikatsketten, SIP-Codes und SBC-Logs selbst lesen wollen, statt auf den nächsten Störfall zu warten.
› Schulung Teams-Telefonie

Es gibt Fehler, die kündigen sich an. Und es gibt Fehler, die Microsoft ein halbes Jahr lang ankündigt, die trotzdem niemand kommen sieht. Der Zertifikatswechsel an der SIP-Schnittstelle von Direct Routing gehört zur zweiten Sorte. Seit Ende Juli 2026 präsentiert Microsoft Zertifikate einer neuen Zertifizierungsstelle, und jeder Session Border Controller, der die passende Stamm-CA nicht in seinem Vertrauensspeicher hat, verweigert ab diesem Moment den Handschlag. Das Ergebnis ist so unspektakulär wie wirkungsvoll: Ausgehende Anrufe brechen mit SIP 504 ab, und zwar alle.

Dieser Beitrag ist für den Moment gedacht, in dem im Ticket „SIP 504“ steht und dir schwant, dass es diesmal nicht an der Voice Route liegt. Du erfährst, wie das Problem mit dem Teams-SBC-Zertifikat und der Root-CA technisch entsteht, wie du es mit lesenden Befehlen und dem Teams Admin Center sicher eingrenzt, welche Stammzertifikate Microsoft laut eigener Dokumentation verlangt und wie du sie herstellerneutral und am Beispiel anynode nachrüstest. Die Grundlagen zu Direct Routing, SBC und Routing findest du gesammelt auf der Seite Teams-Telefonie.

FAKTEN · Das Beispiel in diesem Beitrag

Erfundener Tenant Contoso (contoso.com) mit Standorten in Frankfurt, Köln, Berlin, Hamburg und München. Zwei Session Border Controller sbc1.contoso.com und sbc2.contoso.com, Rufnummern im Muster +49 69 555 0100 (Frankfurt) und +49 221 555 0100 (Köln). Die Testbenutzerin heißt Anna Berger (anna.berger@contoso.com), Durchwahl +49 69 555 0142.

Liste der Stammzertifikate, Fingerabdrücke, Termine und Fehlercodes stammen aus der Microsoft-

Dokumentation auf Microsoft Learn, Stand November 2026. Microsoft hat weitere Schritte in Aussicht gestellt; prüfe die Liste deshalb vor jeder Änderung noch einmal an der Quelle.

Das Symptom: Raus geht nichts, rein geht manchmal

Was Anwender sagen

Von einem Zertifikatswechsel bekommen Anwender nichts mit. Was ihnen auffällt, ist ein Teams, das beim Wählen kurz „Wird angerufen …“ zeigt und dann einfach aufgibt. Im Helpdesk klingt das ungefähr so:

- **„Ich kann niemanden mehr draußen anrufen, Teams legt sofort auf.“** Der Klassiker. Interne Teams-Anrufe funktionieren, weil sie den SBC gar nicht berühren.
- **„Bei den Kollegen in Köln geht es auch nicht.“** Das ist der wichtigste Satz im ganzen Ticket: Wenn alle Benutzer hinter demselben SBC betroffen sind, ist es kein Benutzerproblem.
- **„Angerufen werden klappt, aber ich kann nicht zurückrufen.“** Typisch für die erste Zeit nach der Umstellung. Warum eingehend noch eine Weile funktionieren kann, steht weiter unten.
- **„Es ging doch letzte Woche noch.“** Stimmt. Und am Wählplan hat auch niemand etwas geändert. Diesmal ausnahmsweise wirklich nicht.

Was Admins sehen

Im Teams Admin Center zeigt der PSTN-Nutzungsbericht auf dem Reiter Direct Routing eine auffällige Häufung von Versuchen mit dem finalen SIP-Code 504, alle über dasselbe Gateway, mit einer Phrase, in der „TLS negotiation failed“ vorkommt. Im Health Dashboard für Direct Routing sinkt die Netzwerkeffektivität des betroffenen SBC; Microsoft nennt 504 dort ausdrücklich als Beispiel für ein Problem auf der SBC-Seite. Je nach Zustand der Verbindungen in Gegenrichtung meldet das Dashboard zusätzlich Warnungen beim TLS-Konnektivitätsstatus oder beim Status der SIP-Optionen.

Was du dagegen nicht siehst: eine freundliche Meldung „Dir fehlt eine Stammzertifizierungsstelle“. Das Dashboard warnt dich zwar 30 Tage im Voraus, wenn dein eigenes SBC-Zertifikat abläuft. Ob dein SBC den Zertifikaten von Microsoft vertraut, prüft es nicht für dich. Diese Lücke ist der Grund, warum der Fehler so lange unentdeckt bleiben kann.

WICHTIG · Zwei Zertifikatsprobleme, die gern verwechselt werden

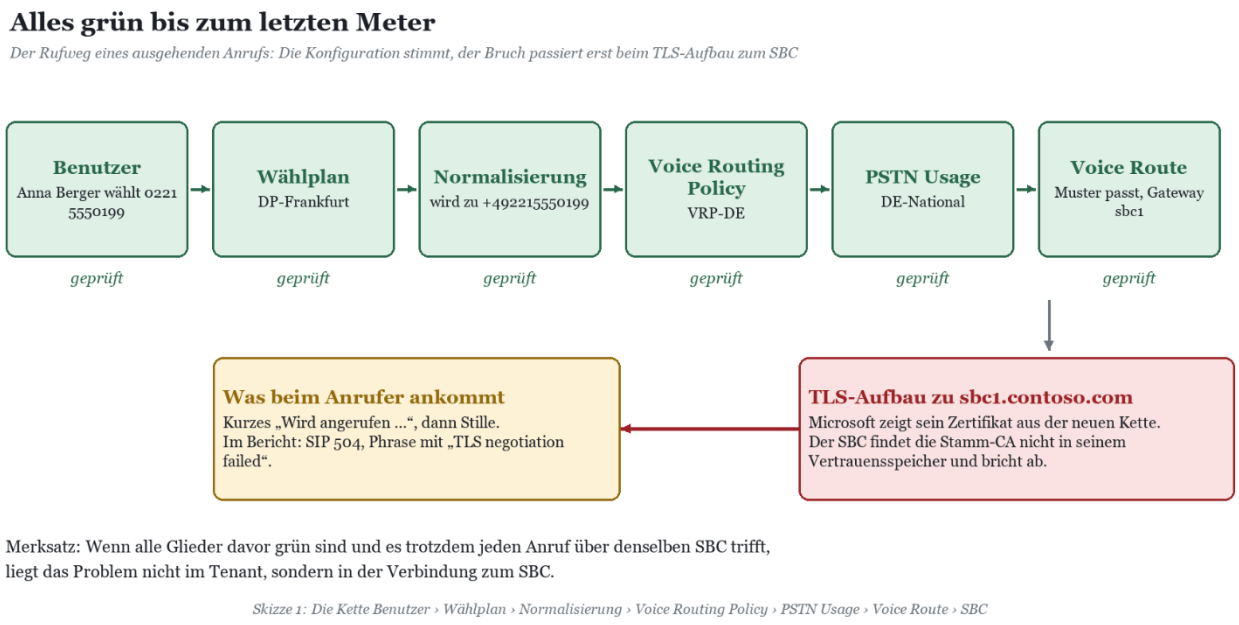
Problem 1: Microsoft vertraut deinem SBC-Zertifikat nicht, etwa weil es abgelaufen ist oder die Kette unvollständig ist. Das ist der Klassiker bei Zertifikatserneuerungen.

Problem 2: Dein SBC vertraut dem Zertifikat von Microsoft nicht, weil ihm die neue Stamm-CA fehlt. Darum geht es in diesem Beitrag. Ein neues eigenes Zertifikat zu kaufen, hilft hier genau gar nicht, ist aber eine beliebte und teure Erstmaßnahme.

Wie der Fehler technisch zustande kommt

Die Kette ist grün, bis auf das letzte Glied

Ein ausgehender Anruf durchläuft in Teams immer dieselbe Kette: Benutzer › Wählplan › Normalisierung › Voice Routing Policy › PSTN Usage › Voice Route › SBC. Bei einem Root-CA-Problem funktionieren alle Glieder bis zur Voice Route einwandfrei. Teams normalisiert die Nummer, findet die Route, wählt sbc1.contoso.com aus und versucht dann, den Anruf per SIP über TLS an den SBC zu übergeben. Genau dort reißt die Kette.

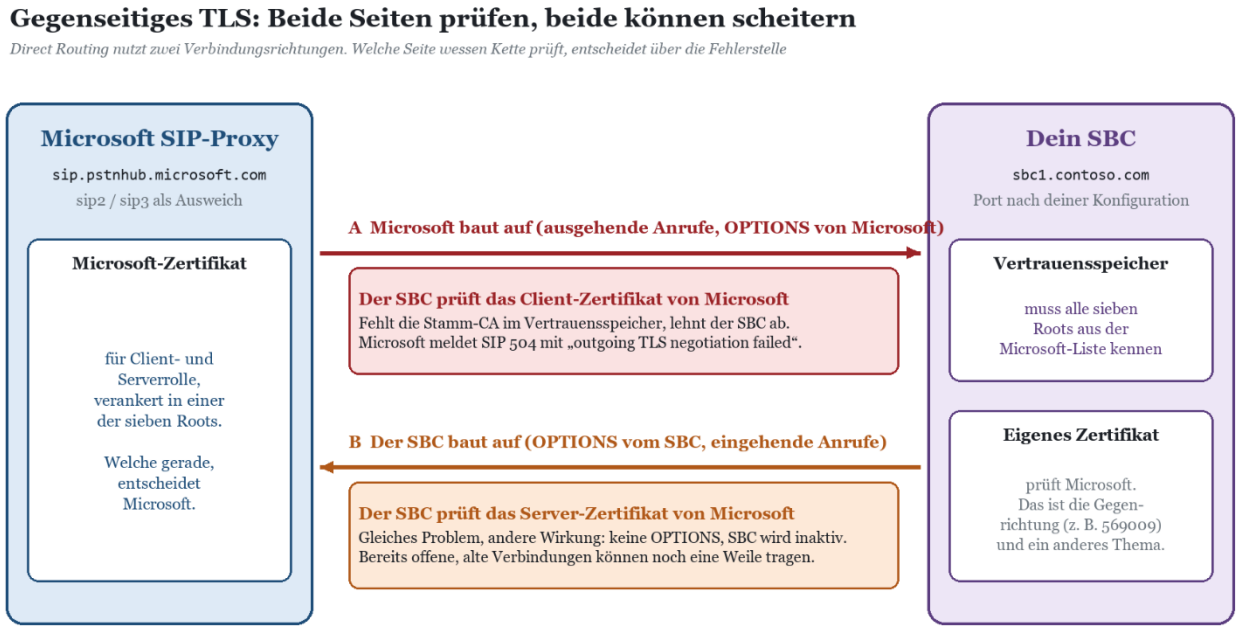


Skizze 1: Die Kette Benutzer › Wählplan › Normalisierung › Voice Routing Policy › PSTN Usage › Voice Route › SBC

Das ist auch der Grund, warum Root-CA-Probleme so viel Zeit kosten. Die übliche Fehlersuche beginnt vorne bei Benutzer und Wählplan, findet dort nichts, arbeitet sich bis zur Voice Route vor, findet wieder nichts und landet irgendwann beim Provider. Wie du die vorderen Glieder systematisch abhakst, steht in Teams-Anruf geht nicht raus: den Rufweg Schritt für Schritt prüfen. Hier nehmen wir an, dass diese Prüfung schon grün ist.

Gegenseitiges TLS: Beide Seiten prüfen

Direct Routing verwendet zwischen Microsoft und deinem SBC gegenseitiges TLS (mTLS). Beide Seiten zeigen ein Zertifikat, und beide Seiten prüfen das Zertifikat der Gegenseite gegen ihre Liste vertrauenswürdiger Stammzertifizierungsstellen. Dazu kommt, dass es zwei Verbindungsrichtungen gibt: Microsoft baut Verbindungen zu deinem SBC auf, unter anderem für ausgehende Anrufe aus Teams, und dein SBC baut Verbindungen zu sip.pstnhub.microsoft.com, sip2 und sip3 auf, etwa für die SIP-OPTIONS und für eingehende Anrufe.



Skizze 2: Bei fehlenden Roots am SBC scheitert Richtung A sofort, Richtung B spätestens beim nächsten Neuaufbau

Wenn Microsoft das eigene Zertifikat auf eine neue Kette umstellt, betrifft das beide Richtungen. Laut Microsoft trägt das Zertifikat der SIP-Schnittstelle die Rollen Server und Client, und der SBC muss beiden vertrauen. Fehlt die neue Stamm-CA, scheitert jede neu aufgebaute Verbindung. Bei Richtung A, also Microsoft zum SBC, merkst du das sofort: Microsoft bekommt den Anruf nicht zugestellt und meldet dem Teams-Client SIP 504. Bei Richtung B kann es dauern, denn bestehende TLS-Verbindungen, die noch mit dem alten Zertifikat aufgebaut wurden, laufen weiter, bis sie neu aufgebaut werden. Dazu kam, dass Microsoft die neuen Zertifikate gestaffelt über Regionen und Tage verteilt hat. „Rein geht, raus nicht“ oder „mal geht es, mal nicht“ sind deshalb keine Widersprüche, sondern das erwartbare Bild.

FAKTEN · Was Microsoft angekündigt und umgesetzt hat

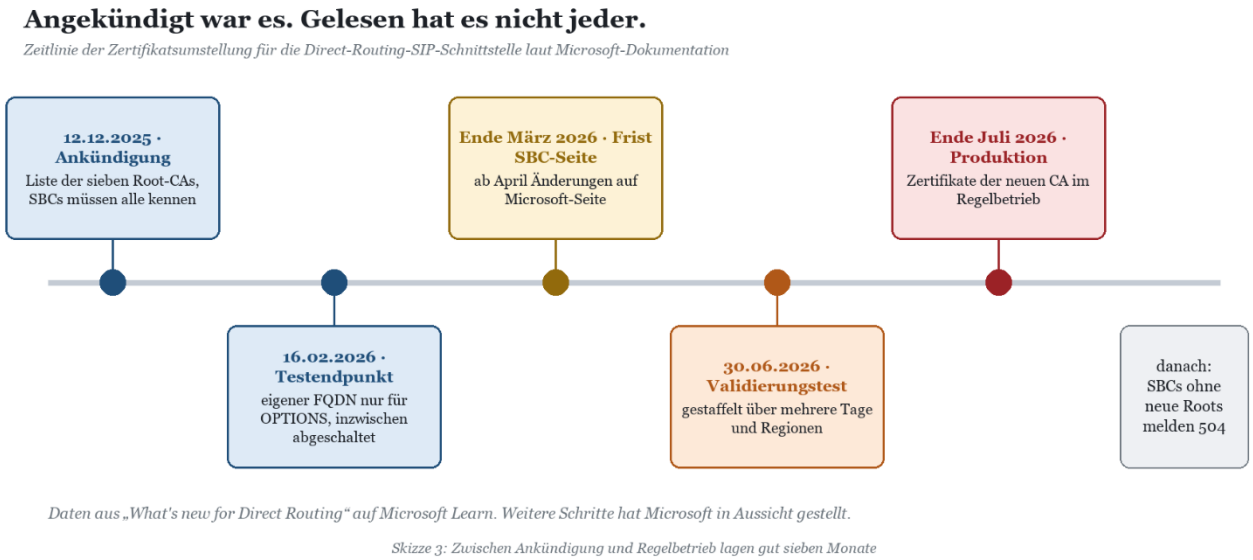
Dezember 2025: Microsoft veröffentlicht die Liste der Stammzertifizierungsstellen, aus denen die Zertifikate der Teams-SIP-Schnittstelle künftig stammen. Die Änderung gilt für Direct Routing und Operator Connect. SBCs müssen allen Stammzertifizierungsstellen der Liste vertrauen, und zwar für Client- und Serverzertifikate.

Februar 2026: Microsoft stellt einen Testendpunkt bereit, der ausschließlich für SIP-OPTIONS gedacht war. Als Frist für Änderungen auf SBC-Seite nennt Microsoft das Ende März, Änderungen auf Microsoft-Seite ab April.

30. Juni 2026: Validierungstest mit Zertifikaten der neuen CA, gestaffelt über mehrere Tage und Regionen. Microsoft schreibt dazu sinngemäß: Wenn SBCs in dieser Zeit keine ausgehenden TLS-Verbindungen mehr aufbauen oder eingehende ablehnen, deutet das auf ein Vertrauensproblem hin.

Ende Juli 2026: Die Zertifikate der neuen CA gehen in den Regelbetrieb, der Testendpunkt ist abgeschaltet.

› Neuerungen bei Direct Routing auf Microsoft Learn



Skizze 3: Zwischen Ankündigung und Regelbetrieb lagen gut sieben Monate

Die sieben Stammzertifizierungsstellen laut Microsoft

Die folgende Liste stammt aus der Ankündigung auf der Seite „What's new for Direct Routing“ und deckt sich mit dem Abschnitt Root Certificate Authorities der Microsoft-Seite zu den Azure-Zertifizierungsstellen. Die Fingerabdrücke sind SHA-1, so wie Microsoft sie angibt. Du brauchst sie, um nach dem Herunterladen zu prüfen, dass du die richtige Datei in der Hand hast.

Stammzertifizierungsstelle	SHA-1-Fingerabdruck laut Microsoft
DigiCert Global Root CA	A8985D3A65E5E5C4B2D7D66D40C6DD2FB19C5436

DigiCert Global Root G2	DF3C24F9BFD666761B268073FE06D1CC8D4F82A4
DigiCert Global Root G3	7E04DE896A3E666D00E687D33FFAD93BE83D349E
DigiCert TLS ECC P384 Root G5	17F3DE5E9F0F19E98EF61F32266E20C407AE30EE
DigiCert TLS RSA 4096 Root G5	A78849DC5D7C758C8CDE399856B3AAD0B2A57135
Microsoft ECC Root Certificate Authority 2017	999A64C37FF47D9FAB95F14769891460EEC4C3C5
Microsoft RSA Root Certificate Authority 2017	73A5E64A3BFF8316FF0EDCCC618A906E4EAE4D74

Welche dieser sieben Stammzertifizierungsstellen gerade am Ende der Kette steht, entscheidet Microsoft, und Microsoft behält sich ausdrücklich vor, zwischen ihnen zu wechseln. Deshalb ist die Anforderung eindeutig: alle sieben in den Vertrauensspeicher, nicht nur die, die heute benutzt wird. Wer nur die aktuelle Root importiert, hat das Problem lediglich auf einen Termin verschoben, den er nicht kennt.



Skizze 4: Plus heißt vorhanden, Minus heißt fehlt. Der linke SBC scheitert, sobald Microsoft eine der fehlenden Roots nutzt

WARNUNG · Nur aus der Microsoft-Quelle übernehmen

Root-Zertifikate aus Foren, Chatverläufen oder dem Mailanhang eines hilfsbereiten Kollegen gehören nicht in den Vertrauensspeicher eines Telefonie-Gateways. Lade die Dateien über die Verweise auf der Microsoft-Seite zu den Azure-Zertifizierungsstellen und vergleiche jeden Fingerabdruck mit der Tabelle oben. Ein falscher Root im Speicher ist schlimmer als ein fehlender: Er fällt nicht auf.

› Details zu den Azure-Zertifizierungsstellen auf Microsoft Learn

Diagnose Schritt für Schritt

Die Diagnose hat ein Ziel: in möglichst wenigen Schritten zu beweisen, dass Tenant und Routing in Ordnung sind und der Abbruch beim TLS-Aufbau zum SBC passiert. Alle Befehle in diesem Abschnitt lesen nur. Du brauchst das PowerShell-Modul MicrosoftTeams und eine Anmeldung mit Connect-MicrosoftTeams.

Schritt 1: Den Fehler im PSTN-Nutzungsbericht finden

Im Teams Admin Center öffnest du Analysen und Berichte › Nutzungsberichte, wählst den Bericht PSTN-Nutzung und darin den Reiter Direct Routing. Filtere auf die letzten Tage und sieh dir die Spalten für den finalen SIP-Code, den finalen Microsoft-Subcode und die finale SIP-Phrase an. Drei Fragen bringen dich weiter:

- **Steht dort 504?** Wenn ja, hat Microsoft den Anruf nicht an den SBC zustellen können.
- **Ist es immer dasselbe Gateway?** Wenn alle Fehlversuche über sbc1.contoso.com laufen und sbc2 sauber ist, hast du den Verdächtigen.
- **Was steht in der Phrase?** „outgoing TLS negotiation failed“ zeigt, dass die Verbindung beim TLS-Handschlag gescheitert ist, nicht im Netz davor.

Wie du solche Auswertungen über längere Zeiträume und mehrere Gateways hinweg anlegst, zeigt Teams-Anrufprotokolle auswerten: Call Records statt Bauchgefühl. Eine Übersicht aller SIP-Codes und Microsoft-Subcodes steht in SIP-Fehlercodes in Teams Direct Routing verstehen.

Schritt 2: Den Subcode richtig lesen

Microsoft dokumentiert für SIP 504 eine ganze Reihe von Subcodes. Nicht jeder davon passt zu einer fehlenden Root auf deinem SBC, und einige deuten genau in die Gegenrichtung. Die Tabelle hilft bei der Einordnung:

Was du im Bericht siehst	Was es laut Microsoft bedeutet	Passt zu fehlender Root am SBC?
504, 569009, SEC_E_UNTRUSTED_ROOT	Microsoft vertraut deinem SBC-Zertifikat nicht.	Nein. Gegenrichtung: Kette deines eigenen Zertifikats prüfen.
504, 569008, SEC_E_CERT_EXPIRED	Dein SBC-Zertifikat ist abgelaufen.	Nein. Eigenes Zertifikat erneuern.
504, 569002, „actively refused“ oder Zeitüberschreitung	SBC nicht erreichbar oder Firewall blockiert.	Nein. Erst Erreichbarkeit und Firewall prüfen.
504, 569015 oder 569016	FQDN des SBC nicht auflösbar oder falscher DNS-Eintragstyp.	Nein. DNS prüfen.
504 mit „outgoing TLS negotiation failed“ und einem anderen HRESULT, SBC-Log zeigt Abbruch bei der Prüfung des Microsoft-Zertifikats	TLS-Aushandlung gescheitert; die Ursache liegt im Handschlag selbst.	Ja, sehr wahrscheinlich. Weiter mit Schritt 4 und 5.

Welcher HRESULT genau erscheint, hängt davon ab, wie dein SBC den Handschlag beendet. Verlass dich deshalb nicht auf einen einzelnen Code, sondern bestätige den Verdacht im SBC-Log. Die vollständige Liste der 504-Varianten pflegt Microsoft auf der Seite SIP 504 und Microsoft-Antwortcodes auf Microsoft Learn.

Schritt 3: Tenant und Routing ausschließen

Bevor du am SBC arbeitest, schließ in zwei Minuten aus, dass im Tenant etwas schief ist. Die folgenden Befehle ändern nichts:

```
Connect-MicrosoftTeams

# Benutzer: Telefonie aktiv, Rufnummer und Richtlinien zugewiesen?
Get-CsOnlineUser -Identity anna.berger@contoso.com |
  Select-Object DisplayName, LineUri, EnterpriseVoiceEnabled, OnlineVoiceRoutingPolicy,
TenantDialPlan

# Wählplan: Was macht Teams aus der gewählten Nummer?
```

```
Get-CsEffectiveTenantDialPlan -Identity anna.berger@contoso.com |
  Test-CsEffectiveTenantDialPlan -DialedNumber "02215550199"

# Routen, die auf sbc1 zeigen
Get-CsOnlineVoiceRoute | Where-Object { $_.OnlinePstnGatewayList -contains "sbc1.contoso.com" }
|
  Select-Object Identity, NumberPattern, Priority, OnlinePstnUsages, OnlinePstnGatewayList

# Gateway: aktiviert, Port, OPTIONS, Failover-Codes
Get-CsOnlinePSTNGateway -Identity sbc1.contoso.com |
  Select-Object Identity, Enabled, SipSignalingPort, SendSipOptions, FailoverResponseCodes,
FailoverTimeSeconds
```

Wenn die übersetzte Nummer im E.164-Format mit +49 erscheint (bei einem deutschen Wählplan mit Normalisierung für nationale Nummern also +492215550199), eine Route mit sbc1 passt und das Gateway aktiviert ist, ist der Tenant aus dem Schneider. Dann bleibt die Verbindung zum SBC. Falls hier doch etwas auffällt, bist du in diesem Beitrag falsch und in Teams-Anruf geht nicht raus: den Rufweg Schritt für Schritt prüfen richtig.

TIPP · Der zweite SBC als Zeuge

Hast du zwei SBCs mit unterschiedlichem Pflegestand, ist der Vergleich Gold wert: Läuft sbc2.contoso.com sauber und sbc1.contoso.com nicht, obwohl beide in derselben Route stehen, ist die Konfiguration im Tenant als Ursache praktisch erledigt. Haben beide SBCs denselben alten Vertrauensspeicher, scheitern beide, und das Failover hilft dir genau gar nicht. Dazu mehr in SBC-Failover in Teams funktioniert nicht.

Schritt 4: Das Health Dashboard lesen

Unter Sprache › Direct Routing im Teams Admin Center findest du das Health Dashboard. Für diesen Fehler sind drei Werte interessant:

Anzeige	Was sie bei fehlender Root zeigen kann	Einordnung
Netzwerkeffektivität	sinkt deutlich, weil 504 als Fehler auf SBC-Seite zählt	Bei weniger als 100 Anrufen im Zeitraum laut Microsoft nur bedingt aussagekräftig.
TLS-Konnektivitätsstatus	Warnung, wenn Verbindungen nicht zustande kommen; Klick auf die Warnung zeigt Details	Warnt zusätzlich 30 Tage vor Ablauf deines eigenen Zertifikats, nicht vor fehlenden Roots.
Status der SIP-Optionen	Warnung oder SBC inaktiv, sobald der SBC seine OPTIONS nicht mehr loswird	Beruht laut Microsoft allein auf dem OPTIONS-Austausch; Anrufe können trotzdem teilweise gehen.

Wenn der SBC als inaktiv erscheint, lohnt der Blick in Teams SBC inaktiv: OPTIONS-Ping und Verbindungsstatus prüfen. Dort steht, wie die OPTIONS-Prüfung im Detail funktioniert und welche anderen Ursachen es für diesen Status gibt.

Schritt 5: Die Kette von außen ansehen

Mit ein paar Zeilen PowerShell kannst du dir von einem Rechner mit Internetzugang auf Port 5061 ansehen, welche Zertifikatskette Microsoft gerade präsentiert. Das Skript baut eine TLS-Verbindung auf, merkt sich die Kette und schließt die Verbindung wieder. Es sendet keine SIP-Nachrichten und ändert nichts.

```
# Liest nur: zeigt die Kette, die Microsoft auf Port 5061 präsentiert
$ziel = "sip.pstnhub.microsoft.com"
$script:kette = $null
$cb = [System.Net.Security.RemoteCertificateValidationCallback]{
  param($s, $cert, $chain, $err)
  $script:kette = $chain.ChainElements | ForEach-Object {
    [pscustomobject]@{ Subject = $_.Certificate.Subject; SHA1 = $_.Certificate.Thumbprint } }
  $true }
$tcp = [System.Net.Sockets.TcpClient]::new($ziel, 5061)
$ssl = [System.Net.Security.SslStream]::new($tcp.GetStream(), $false, $cb)
try { $ssl.AuthenticateAsClient($ziel) } catch { "Handshake: $($_.Exception.Message)" }
$script:kette | Format-Table -AutoSize
$ssl.Dispose(); $tcp.Dispose()
```

Die letzte Zeile der Ausgabe ist die Stamm-CA, bei der Windows die Kette verankert. Vergleiche ihren Fingerabdruck mit der Tabelle oben. Zwei Einschränkungen solltest du kennen: Erstens ist das die Sicht deines Windows-Rechners, nicht die deines SBC; ein SBC kann eine Kette anders verankern. Zweitens lassen viele Firmennetze ausgehend keinen Verkehr auf Port 5061 zu, dann kommst du von deinem Arbeitsplatz aus nicht weit. Gut ist es trotzdem, weil du danach weißt, welche Root du mindestens im SBC finden musst.

Schritt 6: Den Beweis im SBC-Log holen

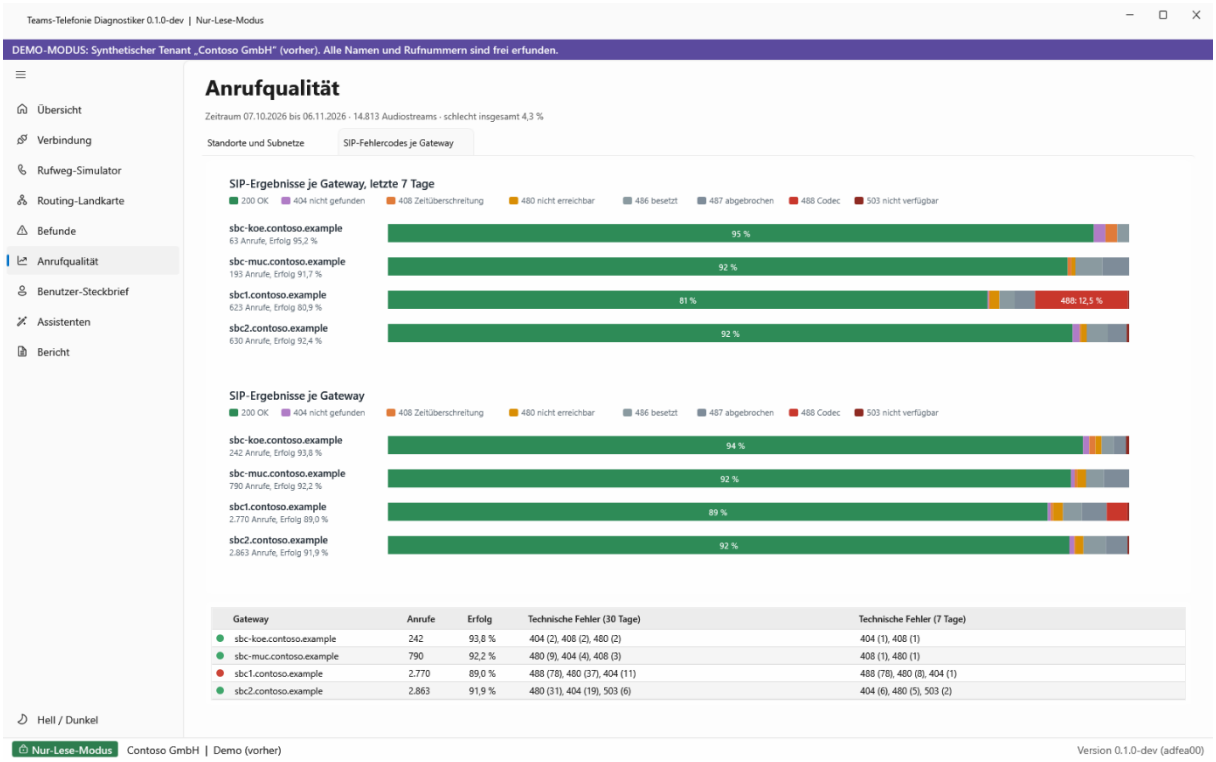
Den eigentlichen Beweis liefert das Log deines SBC. Such nach dem Zeitpunkt eines fehlgeschlagenen Anrufs aus dem PSTN-Nutzungsbericht und schau dir den TLS-Aufbau der eingehenden Verbindung von Microsoft an. Die Formulierungen unterscheiden sich je nach Hersteller, inhaltlich suchst du nach einer dieser Aussagen: Die Gegenstelle legt ein Zertifikat vor, dessen Aussteller unbekannt ist, die Kettenprüfung schlägt fehl, oder der SBC sendet einen TLS-Alert wie „unknown CA“ oder „bad certificate“. Steht so etwas neben einer Microsoft-Adresse, hast du den Fall gelöst. Fehlt dagegen jeder Verbindungsversuch im Log, liegt das Problem davor, typischerweise in Firewall oder DNS.

WERKZEUG · So findet es der Teams-Telefonie Diagnostiker

Der Teams-Telefonie Diagnostiker wertet die Anrufprotokolle deines Tenants aus und zeigt in der Ansicht Anrufqualität auf dem Reiter SIP-Fehlercodes je Gateway, wie sich die SIP-Ergebnisse je SBC verteilen, getrennt nach den letzten 7 Tagen und dem Gesamtzeitraum. Ein Root-CA-Problem fällt dort als plötzlich steigender Anteil von 504 auf einem einzelnen Gateway auf, während die übrigen Gateways unauffällig bleiben.

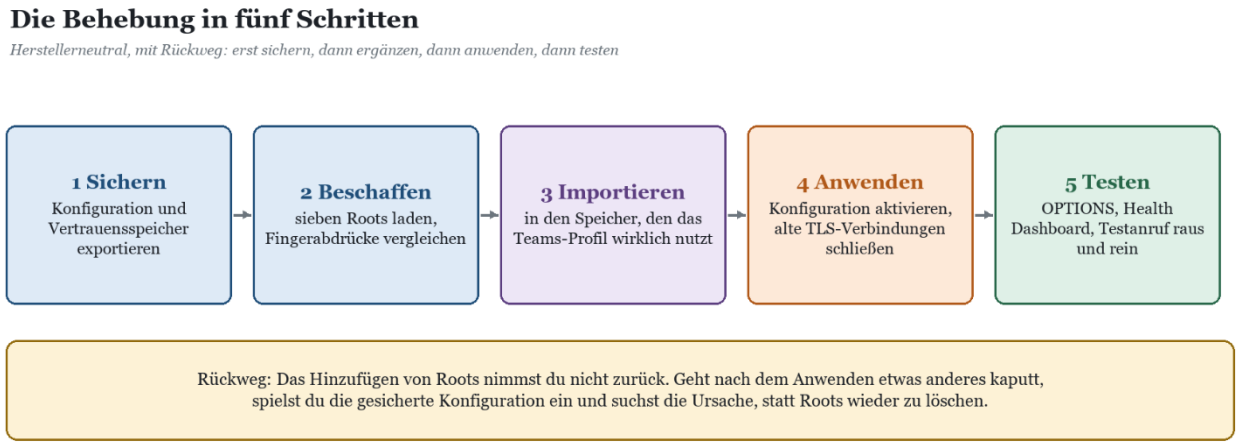
Aus diesen Anrufprotokollen entsteht ein Befund mit Prüffall, der das betroffene Gateway, den Fehlercode und den Zeitraum nennt, und die Ampel für SBC/Routing zeigt den Zustand auf einen Blick. Über den Bericht dokumentierst du den Stand vor und nach dem Import der Stammzertifikate. Der Diagnostiker liest dabei nur; den Vertrauensspeicher des SBC änderst du wie unten beschrieben am Gerät selbst.

Mehr zum Werkzeug: Teams-Telefonie Diagnostiker. Du kannst es 15 Tage kostenlos testen.



Demo-Daten: Auf dem Reiter SIP-Fehlercodes je Gateway siehst du je SBC, welche SIP-Codes in den letzten 7 Tagen und im Gesamtzeitraum auftreten.

Behebung: Root-CAs am SBC nachrüsten



Skizze 5: Schritt 3 ist der, an dem die meisten scheitern: richtiger Speicher, richtiges Profil

Die allgemeinen Schritte für jeden SBC

1. **Konfiguration sichern.** Exportiere die aktuelle SBC-Konfiguration und, falls dein SBC das getrennt anbietet, den Vertrauensspeicher. Notiere, welche TLS-Profile oder Sicherheitsprofile die Verbindung zu Microsoft verwenden.
2. **Ist-Zustand erfassen.** Lies im Vertrauensspeicher, welche der sieben Stammzertifizierungsstellen bereits vorhanden sind. Häufig sind DigiCert Global Root CA und G2 schon da, die G3, die beiden G5 und die beiden Microsoft-Roots von 2017 fehlen.
3. **Zertifikate beschaffen und prüfen.** Lade die fehlenden Stammzertifikate über die Verweise der Microsoft-Seite zu den Azure-Zertifizierungsstellen herunter und vergleiche die SHA-1-Fingerabdrücke mit der Tabelle. Der PowerShell-Block unten hilft dabei.

4. **Importieren, und zwar an der richtigen Stelle.** Viele SBCs kennen mehrere Vertrauenslisten: eine globale, eine je TLS-Profil oder eine Liste vertrauenswürdiger Peers je Schnittstelle. Die Roots müssen in der Liste landen, die das Profil für Microsoft Teams tatsächlich nutzt. Microsoft verlangt, dass der SBC Client- und Serverzertifikaten aus diesen Ketten vertraut; prüfe, ob dein SBC dafür getrennte Einstellungen hat.
5. **Konfiguration anwenden.** Speichern allein reicht bei vielen Geräten nicht. Aktiviere die Konfiguration so, wie es dein Hersteller vorsieht. Bestehende TLS-Verbindungen mit altem Stand solltest du schließen, damit sie neu aufgebaut werden; Microsoft empfiehlt für Zertifikatswechsel am SBC dafür einen Neustart in einem verkehrsarmen Wartungsfenster oder das Vorgehen laut Hersteller.
6. **Testen.** Prüfe, dass der SBC wieder OPTIONS mit sip.pstnhub.microsoft.com, sip2 und sip3 austauscht. Führe einen ausgehenden Testanruf aus Teams durch, etwa auf dein Diensthandy, und einen eingehenden auf eine Teams-Rufnummer wie +49 69 555 0142. Kontrolliere danach im PSTN-Nutzungsbericht, dass die neuen Anrufe mit 200 OK abgeschlossen sind. Die Werte im Health Dashboard brauchen etwas Zeit, bis sie nachziehen.

Zum Prüfen der heruntergeladenen Dateien vor dem Import genügt ein lesender PowerShell-Block. Er listet für jede Datei im Ordner den Inhaber, den SHA-1-Fingerabdruck und das Ablaufdatum:

```
Get-ChildItem .\roots\*.crt | ForEach-Object {
  $c = [System.Security.Cryptography.X509Certificates.X509Certificate2]::new($_.FullName)
  [pscustomobject]@{ Datei = $_.Name; Inhaber = $c.Subject; SHA1 = $c.Thumbprint; 'Gültig bis'
= $c.NotAfter }
} | Format-Table -AutoSize
```

WARNUNG · Nicht aufräumen, während du reparierst

Lösche beim Nachrüsten keine vorhandenen Roots, auch wenn sie dir alt vorkommen. DigiCert Global Root CA und G2 stehen weiterhin auf Microsofts Liste. Und tausch nicht im selben Wartungsfenster dein eigenes SBC-Zertifikat, nur weil du gerade in dem Menü bist. Zwei Änderungen auf einmal heißt im Fehlerfall: zwei Verdächtige und kein Alibi.

Beispiel anynode

Bei anynode liegt die Vertrauensliste für Teams am Knoten für Microsoft Teams Direct Routing. Sinngemäß führt der Weg im Web-Frontend über das Netzwerksicherheitsprofil dieses Knotens zum Bereich für digitales Vertrauen und dort zur Liste der vertrauenswürdigen Peer-Zertifikate. Die genauen Bezeichnungen können je nach Version und Sprache abweichen.

7. Konfiguration sichern, wie in anynode vorgesehen.
8. Im Netzwerksicherheitsprofil des Teams-Knotens die Liste der vertrauenswürdigen Peer-Zertifikate öffnen und mit den sieben Stammzertifizierungsstellen aus der Tabelle abgleichen.
9. Fehlende Stammzertifikate importieren und der Liste hinzufügen.
10. Die Konfiguration anwenden. Erst danach arbeitet anynode mit der neuen Liste.
11. Testen: OPTIONS-Status im anynode-Monitor, ausgehender und eingehender Testanruf, Kontrolle im PSTN-Nutzungsbericht.

Neuere anynode-Versionen bringen einen Mechanismus mit, der benötigte Stammzertifikate nachliefern kann. Ob und ab welcher Version das bei dir greift und ob dafür eine Bestätigung im Frontend nötig ist, klärst du in der Herstellerdokumentation. Verlass dich nicht blind darauf, sondern sieh in die Liste: Nur was dort steht, wird beim Handschlag auch geprüft.

AUS DER PRAXIS · Mein eigener anynode-SBC: wochenlang still nach draußen

Ich mache es kurz, weil es mir nicht ganz leichtfällt: Auch mein eigener anynode-SBC hat den Zertifikatswechsel nicht unbeschadet überstanden. Ausgehende Anrufe über Teams gingen wochenlang nicht. Die Ursache war genau die aus diesem Beitrag: Im Vertrauensspeicher fehlten die neuen Stammzertifikate.

Nach dem Import und dem Anwenden der Konfiguration ging der nächste Testanruf sofort raus. Kein Eingriff in Wählplan, Voice Routing Policy oder Voice Route, kein Anruf beim Provider. Der Schuster hat bekanntlich die schlechtesten Schuhe. Seitdem steht der Abgleich der Root-Liste bei mir im Kalender, gleich neben dem Ablaufdatum des eigenen Zertifikats.

Rückweg, falls etwas schiefgeht

Maßnahme	Risiko	Rückweg
Fehlende Roots hinzufügen	gering; erweitert nur die Liste vertrauenswürdiger Aussteller	Nicht zurücknehmen. Ohne die Roots kommt der Fehler sofort zurück.
Konfiguration anwenden	kurzzeitige Unterbrechung je nach SBC	Gesicherte Konfiguration einspielen, wenn danach etwas anderes gestört ist.
Alte TLS-Verbindungen schließen oder Neustart	laufende Gespräche können abbrechen	Im Wartungsfenster durchführen; kein Rückweg nötig, Verbindungen bauen sich neu auf.
Root versehentlich ins falsche Profil importiert	keine Wirkung, Fehler bleibt	Profilzuordnung prüfen, Import im richtigen Profil wiederholen.

Wichtig ist die Reihenfolge der Gedanken: Wenn nach dem Import etwas anderes nicht funktioniert, liegt das so gut wie nie an zusätzlichen Stammzertifikaten, sondern an einer Änderung, die beim Anwenden gleich mitgekommen ist. Deshalb sicherst du vorher und vergleichst hinterher.

Vorbeugung: damit der nächste Wechsel kein Ausfall wird

- **Microsofts Ankündigungen lesen.** Die Seite „What's new for Direct Routing“ hat diesen Wechsel mehr als ein halbes Jahr vorher angekündigt. Ein fester Termin im Betriebskalender, an dem jemand dort nachsieht, kostet zehn Minuten im Monat.
- **Root-Liste aller SBCs inventarisieren.** Schreib für jeden SBC auf, welche Stammzertifikate in welchem Profil stehen. Beim nächsten Wechsel weißt du dann in Minuten, wo etwas fehlt.
- **Testangebote nutzen.** Wenn Microsoft wieder einen Testendpunkt oder einen Validierungstermin anbietet, nimm ihn wahr. Ein gescheiterter Test im Juni ist erheblich billiger als ein Ausfall im August.
- **Beide SBCs gleich pflegen.** 504 löst standardmäßig ein Failover aus. Das nützt nur, wenn der zweite SBC den Zertifikaten vertraut. Gleicher alter Stand auf beiden heißt: doppelt ausgefallen.
- **Fehlerquote je SBC beobachten.** Ein Wochenblick auf den Anteil von 504 je Gateway zeigt einen Root-Fehler am ersten Tag, nicht in der dritten Woche.
- **Firmware und Zertifikatsdienste aktuell halten.** Viele Hersteller liefern Root-Listen mit Updates aus. Das ersetzt nicht die Kontrolle, verkürzt aber die Arbeit.
- **Änderungen dokumentieren.** Auch ein Root-Import ist eine Änderung. Wer sie protokolliert, findet sie bei der nächsten Fehlersuche wieder.

Der letzte Punkt führt direkt zu Konfigurationsdrift in der Teams-Telefonie erkennen und zur Frage, wer am SBC überhaupt etwas ändern darf; die beantwortet Microsoft Teams Telefonie-Governance. Wenn bei dir mehrere SBCs, Provider und Dienstleister im Spiel sind und niemand so

recht weiß, wer für die Zertifikatspflege zuständig ist, ist das ein gutes Thema für eine Beratung zur Teams-Telefonie. Wer Zertifikatsketten, TLS-Aufbau und SBC-Logs einmal in Ruhe üben möchte statt im Störfall, ist in der Schulung Teams-Telefonie richtig.

WEITERLESEN · Passend dazu

› SIP-Fehlercodes in Teams Direct Routing verstehen
› Teams SBC inaktiv: OPTIONS-Ping und Verbindungsstatus prüfen
› SBC-Failover in Teams funktioniert nicht
› Eingehende Anrufe kommen in Teams nicht an
› Teams SBC Grundlagen: der Session Border Controller
› Teams-Telefonie Probleme: die zehn häufigsten Ursachen

FAQ

Warum funktionieren eingehende Anrufe noch, ausgehende aber nicht?

Weil es zwei Verbindungsrichtungen gibt. Für ausgehende Anrufe aus Teams baut Microsoft eine Verbindung zu deinem SBC auf, und der SBC prüft dabei das Microsoft-Zertifikat neu. Eingehende Anrufe laufen über Verbindungen, die dein SBC zu Microsoft aufbaut. Solange eine solche Verbindung noch aus der Zeit vor dem Wechsel stammt, kann sie weiterlaufen. Spätestens beim nächsten Neuaufbau scheitert auch diese Richtung.

Reicht es, nur die eine Root zu importieren, die gerade in der Kette steht?

Nein. Microsoft verlangt ausdrücklich, dass der SBC allen Stammzertifizierungsstellen der Liste vertraut, weil die Kette in jeder davon verankert sein kann. Wer nur eine importiert, verschiebt das Problem auf den nächsten Wechsel.

Muss ich mein eigenes SBC-Zertifikat erneuern?

Für dieses Problem nicht. Hier geht es darum, ob dein SBC Microsoft vertraut. Dein eigenes Zertifikat muss unabhängig davon gültig sein, den SBC-FQDN im Common Name oder Subject Alternative Name tragen und von einer Zertifizierungsstelle aus dem Microsoft Trusted Root Program stammen. Meldet der Bericht 569009 oder 569008, ist das eigene Zertifikat das Thema, nicht die Roots.

Woher bekomme ich die Stammzertifikate sicher?

Über die Download-Verweise auf der Microsoft-Seite zu den Azure-Zertifizierungsstellen. Vergleiche nach dem Herunterladen jeden SHA-1-Fingerabdruck mit der Liste von Microsoft. Dateien aus anderen Quellen solltest du nicht verwenden.

Muss der SBC nach dem Import neu starten?

Das hängt vom Hersteller ab. Wichtig ist, dass die neue Konfiguration aktiv ist und bestehende TLS-Verbindungen mit altem Stand neu aufgebaut werden. Microsoft empfiehlt bei Zertifikatswechseln am SBC einen Neustart im Wartungsfenster oder das vom Hersteller beschriebene Schließen der alten Verbindungen.

Kann ich den Testendpunkt von Microsoft noch verwenden?

Nein. Microsoft hat den Testendpunkt aus dem Februar 2026 abgeschaltet, nachdem die neuen Zertifikate Ende Juli 2026 in den Regelbetrieb gegangen sind. Heute testest du direkt gegen die produktiven Endpunkte, am besten mit OPTIONS und einem Testanruf im Wartungsfenster.

Betrifft das auch Operator Connect?

Laut Microsoft gilt die Umstellung für Direct Routing und Operator Connect. Bei Operator Connect betreibt allerdings dein Anbieter die SBCs und ist für deren Vertrauensspeicher zuständig. Deine Aufgabe ist dann, bei Häufungen von 504 nachzufragen, nicht selbst zu importieren.

Warum hat mich das Health Dashboard nicht gewarnt?

Weil es eine solche Warnung nicht gibt. Das Dashboard warnt 30 Tage vor dem Ablauf deines eigenen Zertifikats und meldet Probleme mit OPTIONS und TLS-Verbindungen, sobald sie auftreten. Ob dein SBC die neuen Roots kennt, prüft es vorab nicht. Diese Kontrolle bleibt bei dir.

Fazit: Sieben Zertifikate gegen einen Ausfall

Ein SIP 504 nach dem Zertifikatswechsel sieht aus wie ein großes Problem und ist meistens ein kleines: Deinem SBC fehlen Stammzertifikate, die Microsoft lange angekündigt hat. Die Diagnose folgt einer klaren Linie: im Bericht den 504 und das betroffene Gateway finden, den Subcode richtig einordnen, Tenant und Routing in zwei Minuten ausschließen und den Beweis im SBC-Log holen. Die Behebung ist ein Import an der richtigen Stelle, ein Anwenden der Konfiguration und ein Testanruf.

Der eigentliche Lerneffekt liegt woanders. Zertifikatsketten ändern sich, und Microsoft hat weitere Schritte in Aussicht gestellt. Wer die Root-Liste seiner SBCs kennt, Ankündigungen liest und die 504-Quote je Gateway im Blick hat, erlebt den nächsten Wechsel als Wartungstermin. Alle anderen erleben ihn wieder als Helpdesk-Welle. Galgenhumor hilft dann zwar, aber ein Eintrag im Betriebskalender hilft mehr.