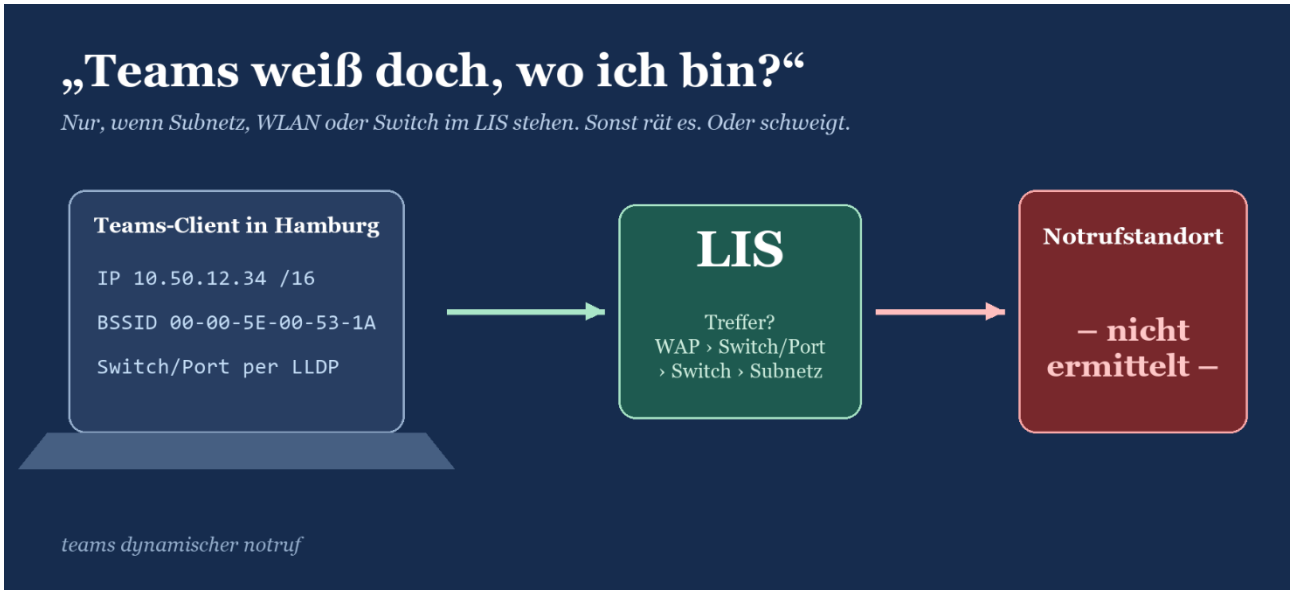
Dynamischer Notruf in Teams funktioniert nicht



WISSEN

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

› **Teams-Telefonie**

BERATUNG

Du willst wissen, ob LIS, Netzwerkstandorte und Notruf-Routing zu deinen Standorten passen? Wir prüfen das mit dir.

› **Beratung zur Teams-Telefonie**

SCHULUNG

Für Admins, die Subnetze, WLAN-Zugangspunkte, Switches und Notrufrichtlinien selbst sicher pflegen wollen.

› **Schulung Teams-Telefonie**

Dynamischer Notruf ist die Funktion, bei der Teams selbst herausfinden soll, wo du gerade bist. Im Büro in Köln, im Besprechungsraum in Hamburg, am Gastarbeitsplatz in München. Klingt nach Magie. Ist aber Buchhaltung: Teams fragt mit ein paar Netzwerkkennungen beim Location Information Service (LIS) nach, und das LIS antwortet nur, wenn jemand diese Kennungen vorher ordentlich eingetragen hat. Hat niemand, antwortet es nicht. Und Teams verrät dir das erst, wenn du genau hinschaust. Oder wenn jemand 112 wählt, was der schlechteste Zeitpunkt für eine Entdeckung ist.

Dieser Beitrag ist für den Fall gedacht, dass teams dynamischer notruf bei dir nicht tut, was er soll: Der Client zeigt keinen oder den falschen Notrufstandort, der Sicherheitsdienst bekommt Benachrichtigungen mit der Adresse der Zentrale, oder Notrufe aus einer Niederlassung laufen über den falschen SBC. Du erfährst, wie der Client seinen Standort ermittelt, an welchen Stellen die Kette typischerweise reißt (Subnetz, BSSID, Switch und Port, Homeoffice, VPN, Richtlinien) und wie du das mit lesenden PowerShell-Befehlen und dem Teams Admin Center eingrenzt. Die Grundlagen der Einrichtung stehen in Notruf in Microsoft Teams konfigurieren; der Beitrag gehört zur Serie rund um die Teams-Telefonie.

FAKTEN · Kurz gesagt

Der Teams-Client schickt beim Start, regelmäßig danach und bei jedem Netzwechsel seine Netzwerkkennungen an Microsoft. Passt etwas im LIS, bekommt er einen Notrufstandort. Die Reihenfolge ist fest: WLAN-Zugangspunkt (BSSID), Switch und Port, Switch, Subnetz. Der erste Treffer gewinnt.

Die Subnetz-Abfrage gibt es nur, wenn die öffentliche IP des Clients als vertrauenswürdige IP

(Trusted IP) eingetragen ist. Abfragen nach BSSID, Switch und Port laufen laut Microsoft unabhängig davon.

Bei Direct Routing kommen zwei Richtlinien dazu: Die Emergency Call Routing Policy legt Notrufnummern und Weg fest, die Emergency Calling Policy die Benachrichtigung. Beide lassen sich Benutzern und Netzwerkstandorten zuweisen; am Standort schlägt die Standortrichtlinie die des Benutzers.

FAKTEN · Das Beispiel in diesem Beitrag

Erfundener Tenant Contoso (contoso.com) mit Zentrale in Frankfurt und Standorten in Köln, Berlin, Hamburg und München. Direct Routing über sbc1.contoso.com und sbc2.contoso.com, Rufnummern im Muster +49 69 555 0100. Subnetze: Frankfurt 10.10.0.0/16, Köln 10.20.0.0/16, Berlin 10.30.0.0/16, Hamburg 10.50.0.0/16, München 10.60.0.0/16, VPN-Pool 10.99.0.0/16. Die BSSIDs stammen aus dem für Dokumentation reservierten Bereich 00-00-5E-00-53-xx.

Das Symptom: Teams weiß nicht, wo du bist, und sagt es keinem

So erleben es Anwender

Anwender bemerken einen kaputten dynamischen Notruf selten selbst. Wenn doch, klingt das im Helpdesk ungefähr so:

- „Unter der Wähltastatur steht bei mir in Hamburg die Adresse in Frankfurt. Ist das schlimm?“
- „Bei mir steht da gar nichts. Bei der Kollegin am Nebentisch steht was. Gleiches WLAN.“
- „Im Homeoffice will Teams, dass ich meine Adresse eintrage. Im Büro nicht. Woher weiß es das?“
- „Seit wir das neue WLAN haben, zeigt Teams im zweiten Stock keinen Standort mehr an.“
- „Wenn ich im VPN bin, sagt Teams, ich sei in der Zentrale. Ich sitze zu Hause im Garten.“

So erleben es Admins

Admins stoßen meistens auf indirektem Weg darauf. Bei einer Übung erhält der Sicherheitsdienst eine Benachrichtigung ohne brauchbaren Standort. Ein Revisor fragt, wie Notrufe aus Niederlassungen geroutet werden, und die Antwort beginnt mit „eigentlich“. Oder der Netzwerkkollege stellt das Hamburger Netz von /24 auf /23 um, und am nächsten Morgen hat ein ganzes Stockwerk keinen Standort mehr, ohne dass irgendwo eine Fehlermeldung auftaucht. Das Teams Admin Center zeigt unter Standorte alle Subnetze, Zugangspunkte und Switches brav als vorhanden an. Ob sie zu dem passen, was die Clients melden, zeigt es nicht.

WARNUNG · Der Fehler meldet sich nicht

Normale Anrufe funktionieren ohne Notrufstandort völlig problemlos. Es gibt kein Ticket, kein rotes Symbol, keinen Alarm. Ein falscher dynamischer Notrufstandort ist ein Fehler mit sehr guter Tarnung und genau einem Auftritt. Plane die Prüfung deshalb ein, statt auf eine Meldung zu warten.

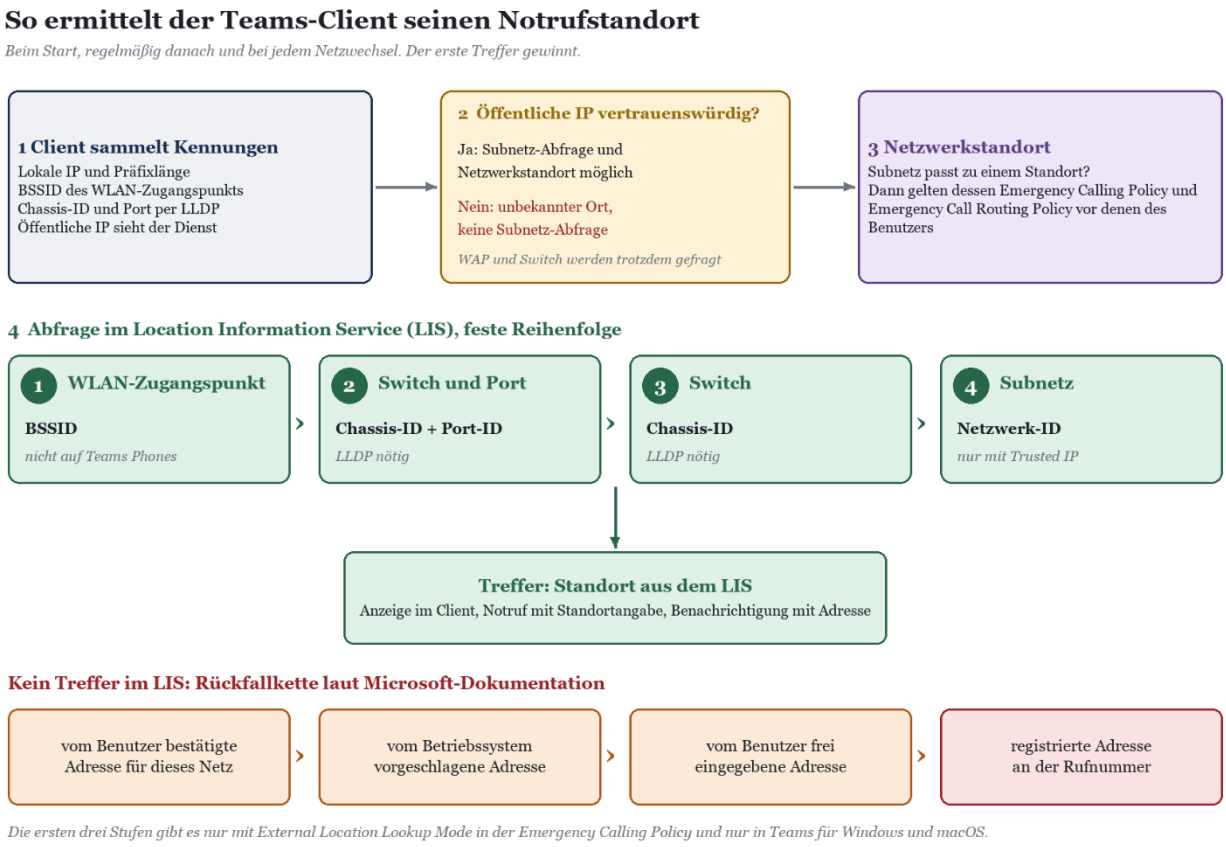
Die typischen Fehlerbilder auf einen Blick

Was du siehst	Wahrscheinliche Ursache	Wo du zuerst schaust
Kein Standort an einem ganzen Standort	Subnetz nur als Netzwerkstandort, nicht im LIS; oder öffentliche IP nicht als Trusted IP	Get-CsOnlineLisSubnet, Get-CsTenantTrustedIPAddress
Kein Standort nach	Maske geändert, Netzwerk-ID passt nicht	ipconfig am Client, Get-

Netzumbau	mehr	CsOnlineLisSubnet
Im WLAN kein oder falscher Standort	BSSID mit Doppelpunkten, Ethernet-MAC statt BSSID, neue Funkzellen nach Austausch	netsh wlan show interfaces, Get-CsOnlineLisWirelessAccessPoint
Am Kabel falscher Stock	Switch-Eintrag ohne Port, LLDP aus, Chassis-ID-Format	Get-CsOnlineLisSwitch, Get-CsOnlineLisPort
Im VPN Adresse der Zentrale	VPN-Pool im LIS oder im Netzwerkstandort Frankfurt	Get-CsOnlineLisSubnet, Get-CsTenantNetworkSubnet
Homeoffice ohne Adresse	External Location Lookup Mode aus, Ortungsdienste gesperrt	Get-CsTeamsEmergencyCallingPolicy
Benachrichtigung geht an falsches Team	Standortrichtlinie fehlt oder überschreibt Benutzerrichtlinie	Get-CsTenantNetworkSite
Notruf aus Hamburg über Frankfurt	ECRP am Standort fehlt, Route zeigt auf falschen SBC	Get-CsTeamsEmergencyCallRoutingPolicy, Get-CsOnlineVoiceRoute

Wie der Fehler technisch zustande kommt

Damit du die Fehler sauber zuordnen kannst, brauchst du die Kette, die der Client durchläuft. Sie hat drei Glieder: Erst prüft der Dienst anhand der öffentlichen IP, ob der Client im Firmennetz ist. Dann sucht er den Netzwerkstandort, der die Richtlinien liefert. Und schließlich fragt er das LIS nach einem Notrufstandort. Die Skizze zeigt den Ablauf; die Details folgen darunter.



Änderungen an Netzwerkeinstellungen und LIS können laut Microsoft bis zu vier Stunden brauchen, bis Clients sie sehen.

Benutzer › Netzwerk › LIS › Notrufstandort

Laut Microsoft-Dokumentation sendet der Client beim Start, danach regelmäßig und bei jeder Änderung der Netzverbindung eine Standortanfrage mit seinen Netzwerkinformationen. Gibt es einen Treffer bei einem Netzwerkstandort, holt sich der Client dessen Notrufrichtlinien. Gibt es einen Treffer im LIS, bekommt er den Notrufstandort des Netzelements, an dem er hängt. Die Reihenfolge ist festgelegt: WLAN-Zugangspunkt, Switch mit Port, Switch, Subnetz. Der erste Treffer zählt, alles danach wird gar nicht mehr gefragt.

Das hat eine unangenehme Konsequenz: Ein falscher BSSID-Eintrag schlägt ein richtiges Subnetz. Steht der Zugangspunkt im dritten Stock versehentlich mit der Adresse des Erdgeschosses im LIS, hilft dir das perfekt gepflegte Subnetz des dritten Stocks nicht mehr. Teams fragt es nicht.

Kennung	Format im LIS	Woher der Client sie hat	Unterstützung laut Microsoft
WLAN-Zugangspunkt	BSSID als nn-nn-nn-nn-nn-nn, Platzhalter * an den letzten ein bis zwei Zeichen	BSSID der verbundenen Funkzelle	alle Teams-Clients außer Teams Phones
Switch und Port	Chassis-ID und Port-ID; als MAC mit Bindestrichen, sonst so wie am Switch konfiguriert	LLDP vom Switch	Windows 10 und neuer, macOS nur mit LLDP-Software, Teams Phones ab bestimmter App-Version, Teams Rooms
Switch	Chassis-ID	LLDP vom Switch	wie Switch und Port
Subnetz	Netzwerk-ID, zum Beispiel 10.50.12.0	eigene IP und Präfixlänge	alle Teams-Clients; nur bei Trusted IP

FAKTEN · Was nicht funktioniert

Der Teams-Webclient unterstützt dynamischen Notruf einschließlich Benachrichtigung des Sicherheitsdienstes laut Microsoft nicht. Microsoft empfiehlt, für Benutzer des Webclients das Telefonieren ins öffentliche Netz über eine Calling Policy abzuschalten.

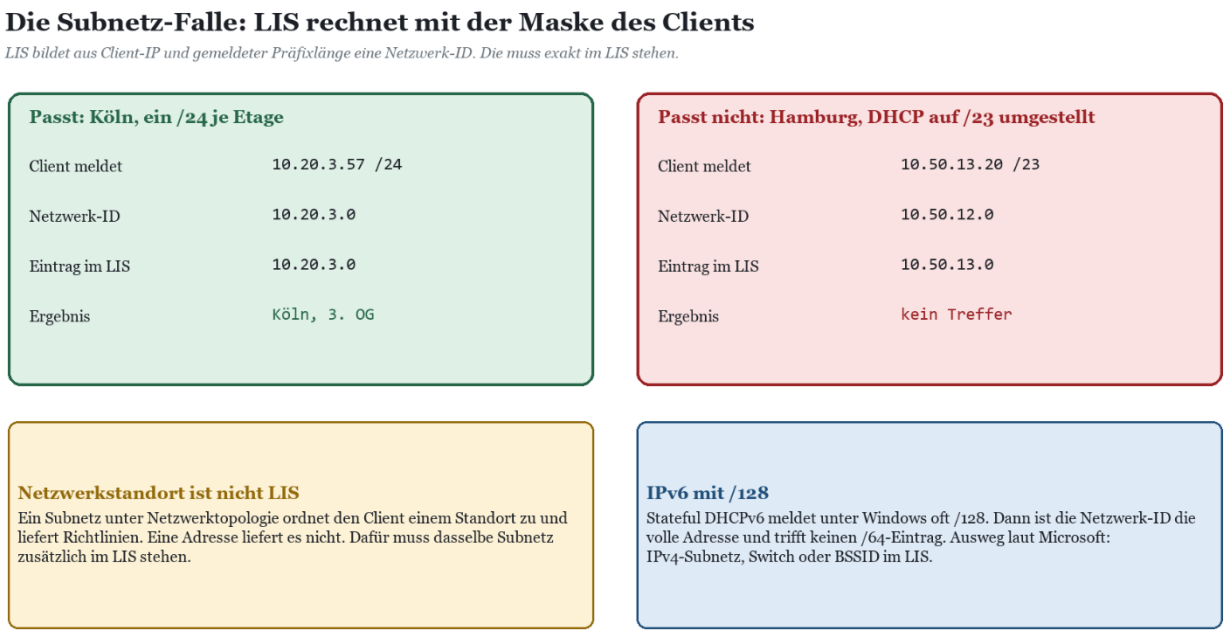
Cloud-Proxys, die die Quell-IP der Teams-Clients verändern, unterstützen die Abfrage der Netzwerkeinstellungen nicht.

Änderungen an Netzwerkeinstellungen und LIS, etwa eine neue Adresse oder Kennung, können bis zu vier Stunden brauchen, bis Clients sie sehen.

Fehler 1: Das Subnetz fehlt im LIS oder hat die falsche Netzwerk-ID

Der Klassiker. Netzwerkstandorte und LIS sind zwei getrennte Tabellen, die im Admin Center nebeneinander wohnen und sich trotzdem nicht kennen. Ein Subnetz unter Netzwerktopologie ordnet den Client einem Netzwerkstandort zu und liefert Richtlinien, etwa für Location-Based Routing oder Notruf-Routing. Eine Adresse liefert es nicht. Microsoft schreibt dazu ausdrücklich: Wer Subnetze in Netzwerkstandorten nutzt, muss sie im LIS noch einmal anlegen, damit dynamische Standorte entstehen. Die Pflege der Netzwerkstandorte selbst beschreibt Netzwerkstandorte und Subnetze in Teams richtig pflegen.

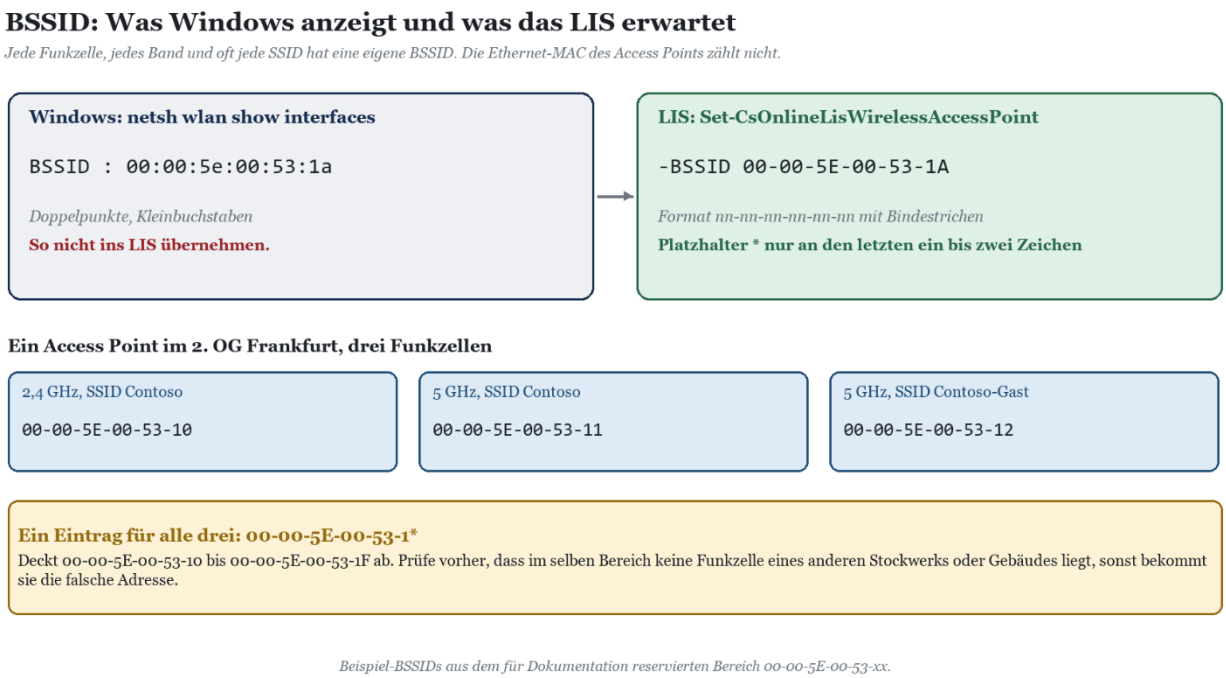
Der zweite Teil der Falle ist die Netzwerk-ID. Das LIS rechnet aus der IP-Adresse und der Präfixlänge, die der Client meldet, die Netzwerk-ID und sucht genau diese. Microsofts Beispiel: 10.10.10.150/25 ergibt 10.10.10.128. Es gibt kein „liegt irgendwie drin“. Wird das Hamburger Netz von zwei /24 auf ein /23 zusammengelegt, meldet ein Client mit 10.50.13.20/23 die Netzwerk-ID 10.50.12.0. Steht im LIS nur 10.50.13.0, gibt es keinen Treffer, obwohl die Adresse scheinbar passt.



Bei IPv6 gibt es eine zusätzliche Hürde, die Microsoft inzwischen ausführlich dokumentiert: Vergibt stateful DHCPv6 die Adressen, meldet Windows oft die Präfixlänge /128. Dann ist die Netzwerk-ID die vollständige Adresse und trifft keinen /64-Eintrag im LIS. Gleichzeitig kann derselbe Client über den Netzwerkstandort seine Richtlinien bekommen, weil dort mit der konfigurierten Maske geprüft wird. Ergebnis: Richtlinien ja, Adresse nein. Microsoft rät davon ab, einzelne /128-Einträge anzulegen, und nennt als Auswege das IPv4-Subnetz bei Dual Stack, Switch oder Port bei kabelgebundenen und die BSSID bei WLAN-Geräten.

Fehler 2: Die BSSID steht im falschen Format oder ist die falsche

Die BSSID ist die MAC-Adresse der Funkseite eines Zugangspunkts, nicht die des Ethernet-Anschlusses, auf den das Netzwerkteam bei der Inventur schaut. Das LIS erwartet sie im Format nn-nn-nn-nn-nn-nn, also mit Bindestrichen. Windows zeigt sie mit netsh wlan show interfaces dagegen mit Doppelpunkten und in Kleinbuchstaben an, und genau so landet sie dann per Copy and Paste in der CSV-Datei für den Upload.



Dazu kommt die Vervielfältigung: Ein moderner Zugangspunkt funkt auf mehreren Bändern und oft mit mehreren SSIDs, jede Kombination mit eigener BSSID. Wer pro Zugangspunkt nur eine BSSID einträgt, erwischt mit etwas Glück ein Drittel der Clients. Für genau diesen Fall erlaubt Set-CsOnlineLisWirelessAccessPoint einen Platzhalter an den letzten ein oder zwei Zeichen. 00-00-5E-00-53-1* deckt alles von -10 bis -1F ab. Prüfe vorher, ob im Bereich nicht auch Funkzellen eines anderen Stockwerks liegen. Und denk daran: Nach einem Austausch der Zugangspunkte sind alle BSSIDs neu, auch wenn die SSID gleich heißt.

TIPP · Platzhalter und Einzeleinträge vertragen sich nicht beliebig

Laut Dokumentation lehnt das LIS einen neuen Einzeleintrag ab, wenn bereits ein Platzhaltereintrag mit derselben Location-ID den Bereich abdeckt. Das ist kein Fehler, sondern Absicht. Willst du einen einzelnen Zugangspunkt in diesem Bereich anders zuordnen, passt du die Platzhalter so an, dass sie sich nicht überschneiden.

Fehler 3: Switch und Port melden nichts oder etwas anderes

Am Kabel arbeitet Teams mit LLDP. Der Switch sagt dem Client, wer er ist (Chassis-ID) und an welchem Port der Client hängt (Port-ID). Ist LLDP am Switch oder am Port abgeschaltet, meldet der Client nichts, und es geht mit dem Subnetz weiter. Ist LLDP an, kommt es auf das Format an: Ist der Subtyp eine MAC-Adresse, erwartet das LIS wieder nn-nn-nn-nn-nn-nn mit Bindestrichen. Ist er ein Schnittstellenname, muss der Eintrag exakt so lauten, wie er am Switch konfiguriert ist. Ein Gi1/0/12 ist eben kein GigabitEthernet1/0/12.

Auf dem Mac braucht es laut Microsoft eine zusätzliche LLDP-Software, auf Teams Phones eine Mindestversion der Teams-App. Und ein Switch-Eintrag ohne Port gilt für alle Ports dieses Switches, was bei einem Stack über zwei Etagen zu sehr selbstbewussten, aber falschen Stockwerksangaben führt.

Fehler 4: Homeoffice und die Rückfallkette

Zu Hause ist die öffentliche IP des Clients die des Heimanschlusses. Die steht nicht in den Trusted IPs, also gibt es keine Subnetz-Abfrage, und die BSSID des Heimrouters steht nicht im LIS. Das ist

kein Fehler, sondern genau das gewünschte Verhalten: Sonst würde jedes 192.168.178.0 dieser Welt zur Zentrale in Frankfurt.

Was dann passiert, beschreibt Microsoft als Rangfolge: Zuerst zählt eine dynamisch aus dem LIS ermittelte Adresse, danach eine vom Benutzer für dieses Netz bestätigte oder bearbeitete Adresse, dann ein Vorschlag des Betriebssystems, dann eine frei eingegebene Adresse und zuletzt die registrierte Adresse an der Rufnummer. Die Punkte zwei bis vier gibt es nur, wenn in der Emergency Calling Policy der External Location Lookup Mode eingeschaltet ist. Microsoft beschreibt das Verfahren im Kontext der US-Vorgaben; die Rangfolge selbst ist aber das, was der Client tut. Unterstützt wird die Eingabe durch den Benutzer in Teams für Windows und macOS, Teams Phones können das nicht, Teams mobil erkennt den Standort automatisch, lässt aber keine Eingabe zu.

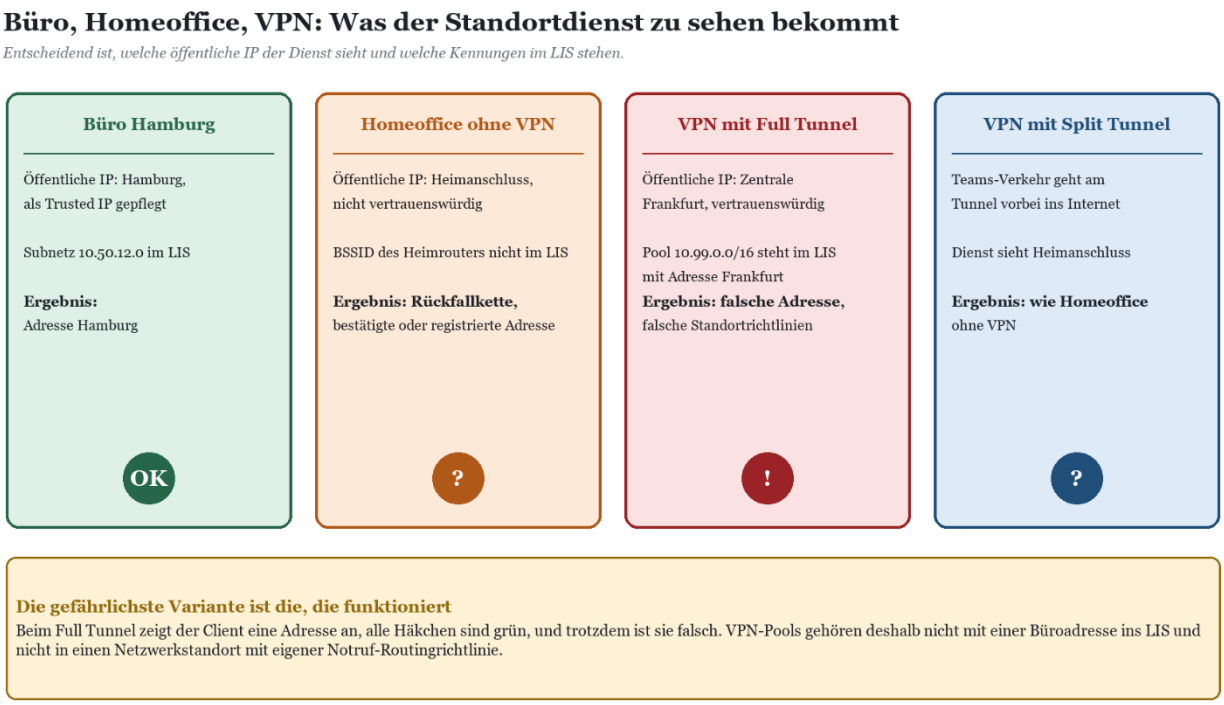
WICHTIG · Ortungsdienste und Datenschutz

Der Vorschlag des Betriebssystems funktioniert nur, wenn Teams auf die Ortungsdienste zugreifen darf. Unter Windows steuerst du das per Gruppenrichtlinie oder MDM. Ob ihr das wollt, ist eine Frage für Datenschutz und Betriebsrat, nicht für die Telefonie-Konfiguration allein. Ohne Ortungsdienste bleibt die manuelle Eingabe.

Fehler 5: VPN macht aus dem Garten die Zentrale

Beim VPN wird es interessant, weil zwei Fragen gleichzeitig entscheiden: Welche öffentliche IP sieht der Standortdienst, und steht das Subnetz des VPN-Pools im LIS? Bei einem Full Tunnel verlässt der gesamte Verkehr das Netz über die Zentrale. Der Dienst sieht eine vertrauenswürdige IP, der Client meldet eine Adresse aus dem VPN-Pool. Steht dieser Pool im LIS mit der Adresse der Zentrale, zeigt Teams im heimischen Garten zuverlässig Frankfurt an. Steht er zusätzlich in einem Netzwerkstandort mit eigener Notruf-Routingrichtlinie, gelten auch noch die Richtlinien von Frankfurt.

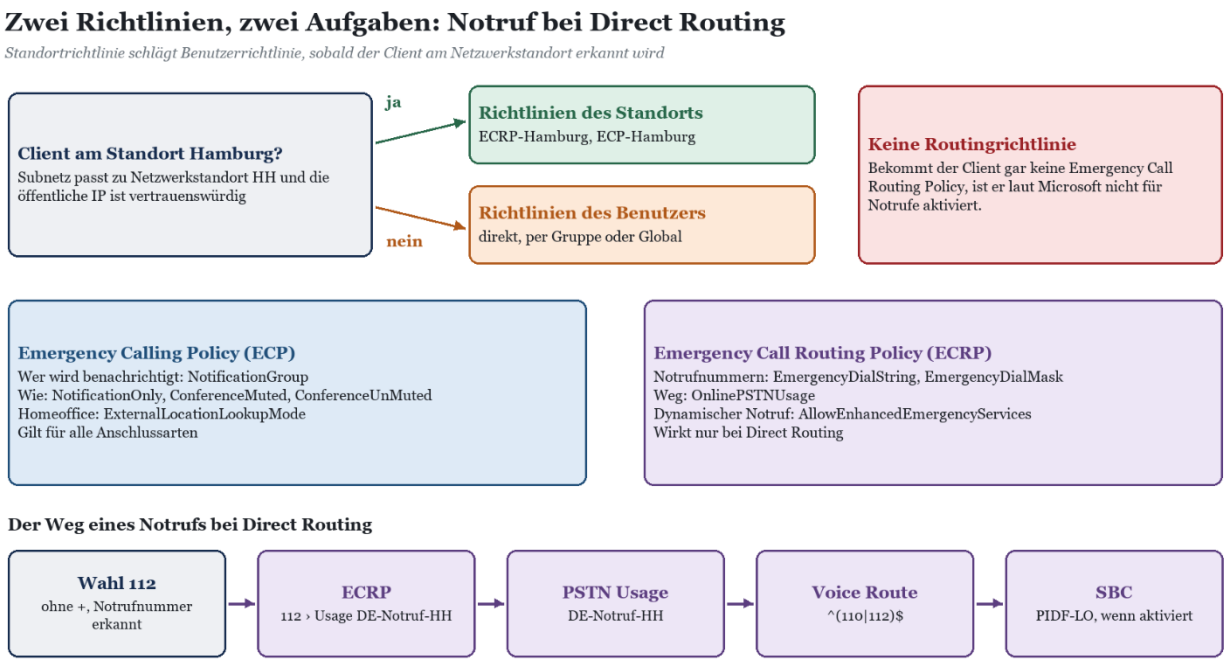
Bei einem Split Tunnel, den Microsoft für Teams-Medien ohnehin empfiehlt, geht der Teams-Verkehr direkt ins Internet. Dann sieht der Dienst den Heimanschluss, und der Client landet in der Rückfallkette wie ohne VPN. Welcher Teil des Teams-Verkehrs welchen Weg nimmt, legt deine VPN-Konfiguration fest; prüfe deshalb am Client, welcher Standort tatsächlich angezeigt wird. Wie du den Tunnel sauber schneidest, steht in Teams-Telefonie über VPN: Split Tunneling richtig einrichten.



Situation	Öffentliche IP	LIS-Treffer	Ergebnis
Büro, korrekt gepflegt	Trusted IP des Standorts	Subnetz, BSSID oder Switch	richtige Adresse
Büro, lokaler Internetausgang ohne Trusted IP	unbekannt	nur BSSID oder Switch möglich	ohne WLAN- oder LLDP-Eintrag kein Standort
Homeoffice ohne VPN	Heimanschluss	keiner	Rückfallkette, bei aktivem Lookup Mode Benutzereingabe
VPN Full Tunnel, Pool im LIS	Trusted IP der Zentrale	VPN-Subnetz	falsche Adresse, wirkt aber korrekt
VPN Full Tunnel, Pool nicht im LIS	Trusted IP der Zentrale	keiner	Rückfallkette
VPN Split Tunnel	je nach Weg meist Heimanschluss	keiner	Rückfallkette

Fehler 6: Die Richtlinien passen nicht zum Standort

Die Emergency Calling Policy (ECP) regelt, wer bei einem Notruf benachrichtigt wird und wie: nur per Chat, mit stummer Konferenzteilnahme oder mit Mitsprache. Außerdem schaltet sie den External Location Lookup Mode und einen Hinweistext im Client. Sie wirkt bei allen Anschlussarten. Die Emergency Call Routing Policy (ECRP) gibt es nur für Direct Routing. Sie legt fest, welche Nummern als Notruf gelten, welche Masken auf sie umgeschrieben werden, über welche PSTN Usage sie laufen und ob dynamischer Notruf aktiv ist. Im Admin Center ist das der Schalter für dynamische Notrufe (Dynamic emergency calling), in PowerShell der Parameter AllowEnhancedEmergencyServices.



Namen im Contoso-Beispiel. Dynamisches Routing zur zuständigen Leitstelle per Standort beschreibt Microsoft für Direct Routing nur für USA und Kanada.

Für die Routingrichtlinie beschreibt Microsoft die Auswahl genau: Hat der Netzwerkstandort eine ECRP, gilt diese. Hat er keine, ist der Client an keinem definierten Standort oder passt die gewählte Nummer zu keiner Notrufnummer der Standortrichtlinie, gilt die Richtlinie des Benutzers. Bekommt der Client gar keine ECRP, ist er nicht für Notrufe aktiviert. Bei der ECP gilt ebenfalls: Ist der Benutzer am Standort, schlägt die Standortrichtlinie die Benutzerrichtlinie. Wer die Global-Richtlinie nie angefasst hat, erlebt hier die üblichen Überraschungen, siehe Teams-Benutzer fällt auf die globale Richtlinie zurück.

	Emergency Calling Policy	Emergency Call Routing Policy
Wirkt bei	Calling Plan, Operator Connect, Teams Phone Mobile, Direct Routing	nur Direct Routing
Aufgabe	Benachrichtigung, Homeoffice-Eingabe, Hinweistext	Notrufnummern, Masken, PSTN Usage, dynamischer Notruf ein oder aus
Wichtige Parameter	NotificationGroup, NotificationMode, NotificationDialOutNumber, ExternalLocationLookupMode	EmergencyNumbers (EmergencyDialString, EmergencyDialMask, OnlinePSTNUsage), AllowEnhancedEmergencyServices
Zuweisung	Benutzer, Gruppe, Netzwerkstandort	Benutzer, Gruppe, Netzwerkstandort
Vorrang	Standort vor Benutzer, wenn Client am Standort	Standort vor Benutzer, Ausnahmen siehe Text

WARNUNG · Notrufnummern ohne Pluszeichen

Microsoft weist darauf hin, dass Teams-Clients bei Direct Routing kein „+“ mehr vor die Notrufnummer setzen. Das Muster der Voice Route für Notrufe muss also auf 112 passen, nicht auf +112. Für 110 und 112 in Deutschland ist ^(110|112)$ das passende Muster. Ein Muster wie ^\+?112$ schadet nicht, ein Muster, das nur ^\+112$ akzeptiert, schon.

Achte außerdem darauf, dass dein Wählplan 110 und 112 nicht in E.164 umschreibt. Eine Normalisierungsregel, die alle dreistelligen Nummern mit der Ortsvorwahl versieht, macht aus 112 eine +49 40 112. Dann trifft keine Notrufnummer mehr.

Was dynamischer Notruf in Deutschland leistet und was nicht

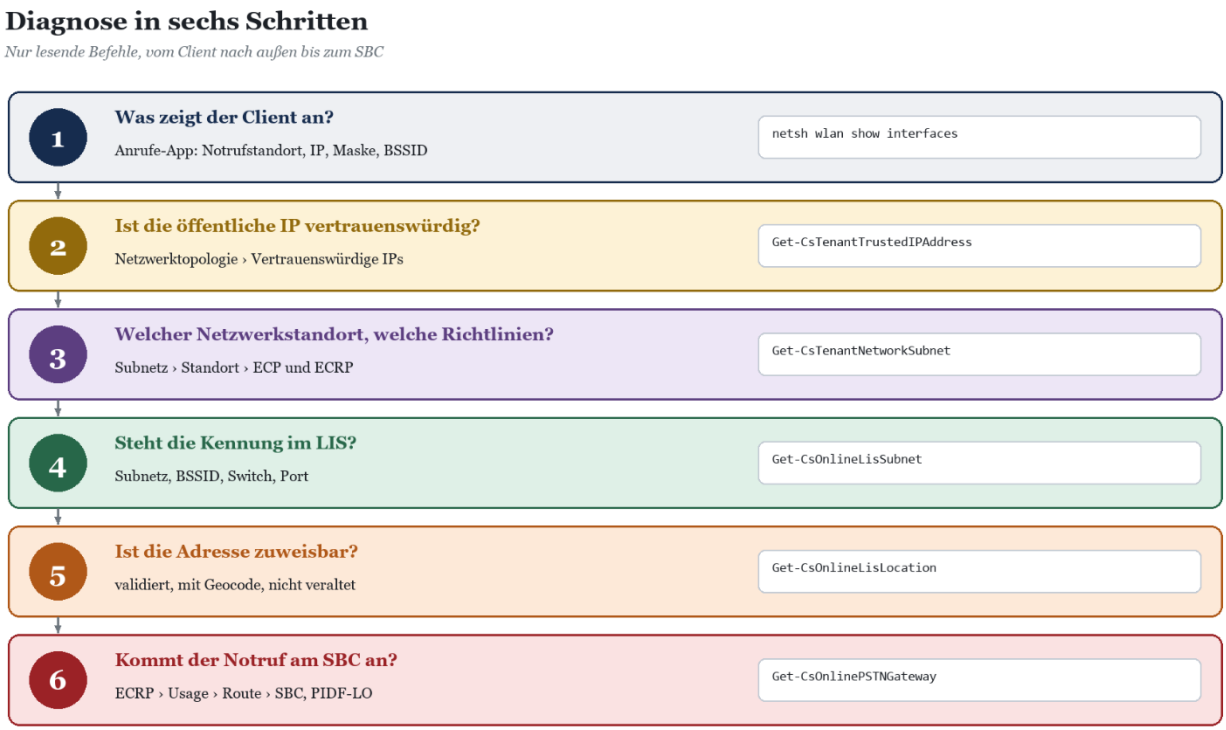
Hier lohnt ein ehrlicher Blick in die Dokumentation, bevor du Erwartungen weckst. Das automatische Routing an die zuständige Leitstelle anhand des dynamisch ermittelten Standorts beschreibt Microsoft für Direct Routing nur für die USA und Kanada, dort über spezialisierte Notruf-Routing-Dienstleister oder ELIN-Anwendungen im SBC. In Deutschland bringt dir der dynamische Notruf trotzdem eine Menge: Die Standortrichtlinie am Netzwerkstandort schickt den Notruf über den SBC und Anschluss der Niederlassung, der Sicherheitsdienst bekommt die Adresse des tatsächlichen Standorts, der Client zeigt sie an, und mit aktiviertem PidfloSupported am Gateway gibt Teams die Standortangabe im INVITE an deinen SBC weiter. Was dein Netzbetreiber damit macht, regelt dein Vertrag, nicht Teams.

AUS DER PRAXIS · Mein eigener anynode-SBC

In meinem eigenen Netz läuft ein anynode-SBC an Teams Direct Routing. Wenn ich dort prüfe, ob die Standortangabe ankommt, schaue ich in den SIP-Trace des INVITE und nicht auf die Konfiguration in Teams. Der Trace beantwortet aber nur die halbe Frage: Ob und wie der Netzbetreiber eine Standortangabe nutzt, steht nirgends im Trace, sondern nur in seiner Leistungsbeschreibung. Beides gehört in die Doku, sonst glaubt der Nachfolger, PIDF-LO löse die Leitstellenzuordnung von allein.

Diagnose Schritt für Schritt

Die Diagnose geht vom Client nach außen. Erst klärst du, was der Client meldet und anzeigt, dann, was der Dienst daraus machen kann. Alle Befehle hier sind lesend; sie ändern nichts am Tenant. Du brauchst das Modul MicrosoftTeams und eine Verbindung mit Connect-MicrosoftTeams.



Schritt 1: Am Client nachsehen, was er meldet

Öffne in Teams die Anrufe-App. Unter der Wähltastatur zeigt Teams den aktuellen Notrufstandort an, sofern einer ermittelt wurde. Steht dort nichts, die Zentrale oder eine Adresse, die der Benutzer

irgendwann selbst bestätigt hat, weißt du schon, in welchem Zweig der Rückfallkette du bist. Dann sammelst du die Kennungen, die der Client melden würde:

```
# IP-Adresse und Präfixlänge (daraus rechnet das LIS die Netzwerk-ID)
Get-NetIPAddress -AddressFamily IPv4 | Where-Object PrefixOrigin -ne 'WellKnown' |
    Format-Table InterfaceAlias, IPAddress, PrefixLength

# BSSID der verbundenen Funkzelle (Ausgabe mit Doppelpunkten!)
netsh wlan show interfaces

# Öffentliche IP: am einfachsten über die Firewall- oder Proxy-Protokolle bestimmen
```

Rechne die Netzwerk-ID aus IP und Präfixlänge aus und schreibe die BSSID gleich in das Format um, das das LIS erwartet: Großbuchstaben, Bindestriche. Für Switch und Port brauchst du die Sicht des Netzwerkteams: Welche Chassis-ID und welche Port-ID sendet der Switch per LLDP an diesen Port?

Schritt 2: Trusted IPs prüfen

Im Teams Admin Center findest du die vertrauenswürdigen IPs unter Standorte › Netzwerktopologie im Reiter für vertrauenswürdige IPs. In PowerShell:

```
Get-CsTenantTrustedIPAddress | Format-Table Identity, IPAddress, MaskBits, Description
```

Fehlt die öffentliche IP eines Standorts mit eigenem Internetausgang, bekommt dort kein Client einen Subnetz-Treffer und keinen Netzwerkstandort. Microsoft weist darauf hin, dass bei IPv4- und IPv6-Ausgang beide Adressen eingetragen sein müssen, weil der Abgleich vom Format des Pakets abhängt.

Schritt 3: Netzwerkstandort und Richtlinien prüfen

```
# Welcher Netzwerkstandort gehört zum Subnetz?
Get-CsTenantNetworkSubnet | Format-Table Identity, MaskBits, NetworkSiteID

# Welche Notrufrichtlinien hängen am Standort?
Get-CsTenantNetworkSite | Format-Table Identity, NetworkRegionID,
    EmergencyCallingPolicy, EmergencyCallRoutingPolicy

# Welche Richtlinien hat der Benutzer selbst?
Get-CsOnlineUser -Identity lena.hoffmann@contoso.com |
    Format-List TeamsEmergencyCallingPolicy, TeamsEmergencyCallRoutingPolicy
```

Ist bei einem Benutzer nichts eingetragen, gilt die Global-Richtlinie. Steht am Standort Hamburg keine EmergencyCallRoutingPolicy, nimmt der Client in Hamburg die Richtlinie des Benutzers, und wenn dessen Routingrichtlinie auf die Frankfurter PSTN Usage zeigt, geht der Notruf über Frankfurt raus. Im Admin Center siehst du dasselbe unter Standorte › Netzwerktopologie › Netzwerkstandorte.

Schritt 4: LIS-Einträge prüfen

```
Get-CsOnlineLisSubnet | Format-Table Subnet, LocationId, Description
Get-CsOnlineLisWirelessAccessPoint | Format-Table BSSID, LocationId, Description
Get-CsOnlineLisSwitch | Format-Table ChassisID, LocationId, Description
Get-CsOnlineLisPort | Format-Table ChassisID, PortID, LocationId, Description

# Gezielte Suche nach der Netzwerk-ID aus Schritt 1
Get-CsOnlineLisSubnet | Where-Object Subnet -eq '10.50.12.0'
```

Vergleiche die Ausgabe Zeichen für Zeichen mit dem, was der Client meldet. Sieben Subnetze, die im Netzwerkstandort Hamburg stehen, aber im LIS fehlen, sind keine Seltenheit, sondern eher der Normalfall nach einem Netzumbau. Im Admin Center findest du die Einträge unter Standorte › Netzwerke und Standorte in den Reitern Subnetze, WLAN-Zugriffspunkte, Switches und Ports.

Schritt 5: Ist die Adresse überhaupt zuweisbar?

```
Get-CsOnlineLisLocation -LocationId <LocationId aus Schritt 4> |
    Format-List CompanyName, HouseNumber, StreetName, City, PostalCode,
    Location, Latitude, Longitude, ValidationStatus
```

Für dynamische Standorte verlangt Microsoft eine validierte Adresse mit Geocode. Adressen ohne Geocode lassen sich Netzwerkkennungen nicht zuweisen, Adressen, die älter als ein paar Jahre sind, laut Dokumentation ebenfalls nicht; die musst du neu anlegen. Was passiert, wenn die Adresse ganz fehlt, beschreibt Notrufadresse fehlt in Teams: was bei 112 wirklich passiert.

Schritt 6: Notruf-Routing bis zum SBC prüfen

```
# Notrufnummern und Usages der Routingrichtlinie
(Get-CsTeamsEmergencyCallRoutingPolicy -Identity 'ECRP-Hamburg').EmergencyNumbers
Get-CsTeamsEmergencyCallRoutingPolicy | Format-Table Identity, AllowEnhancedEmergencyServices

# Welche Voice Route bedient die Usage und auf welchen SBC zeigt sie?
Get-CsOnlineVoiceRoute | Where-Object OnlinePstnUsages -contains 'DE-Notruf-HH' |
    Format-Table Identity, NumberPattern, Priority, OnlinePstnGatewayList

# Gibt der SBC die Standortangabe weiter?
Get-CsOnlinePSTNGateway | Format-Table Identity, Enabled, PidfloSupported
```

Prüfe, ob das NumberPattern 110 und 112 ohne Pluszeichen trifft, ob die Route auf einen aktiven SBC zeigt und ob keine Route mit höherer Priorität dazwischenfunkt. Die Regeln für Prioritäten und überdeckte Muster erklärt Teams Voice Route greift nicht: Regex, Priorität und überdeckte Routen. Einen echten Notruf brauchst du für diese Prüfung nicht; wie du sinnvoll testest, steht in Notruf in Teams testen, ohne die Leitstelle zu verärgern.

TIPP · Erst warten, dann zweifeln

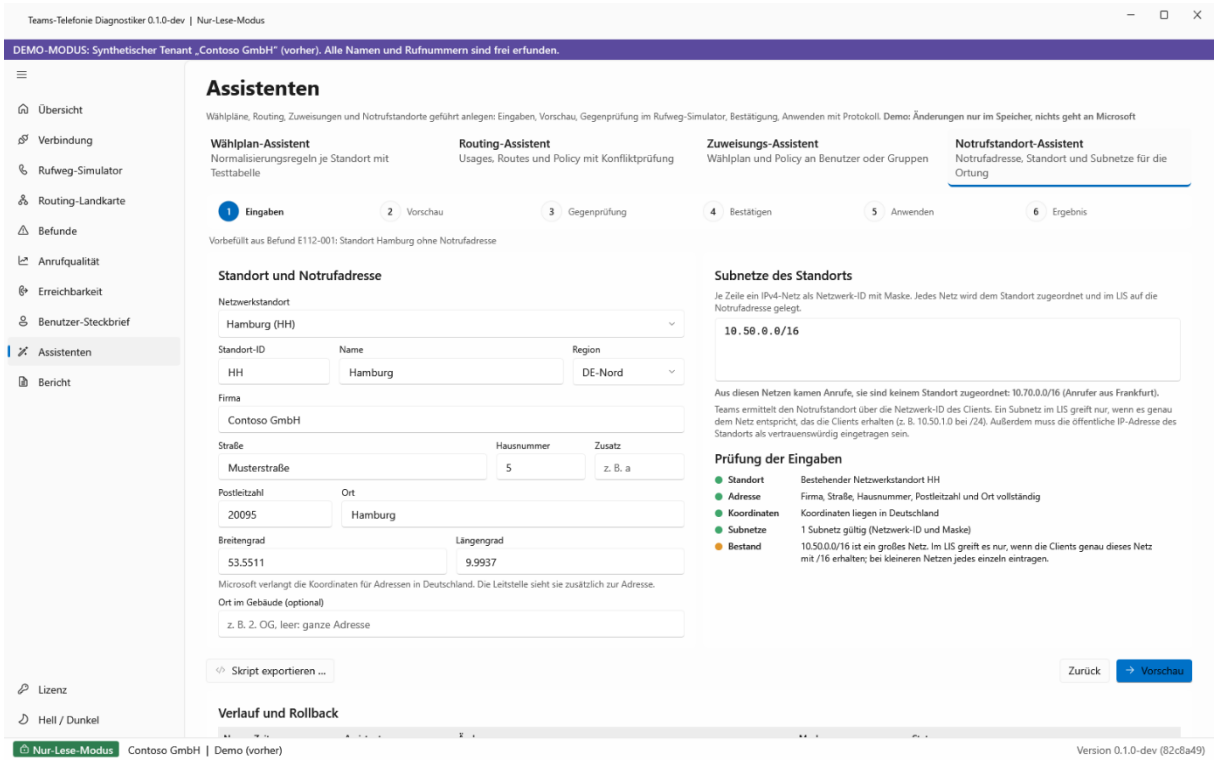
Hast du gerade etwas geändert und der Client zeigt noch den alten Stand, sind die bis zu vier Stunden Verteilzeit der wahrscheinlichste Grund. Teams neu starten oder das Netz wechseln löst eine neue Abfrage aus, beschleunigt aber nicht die Verteilung im Dienst.

WERKZEUG · So findet es der Teams-Telefonie Diagnostiker

Der Teams-Telefonie Diagnostiker liest die Notrufkonfiguration im Nur-Lese-Modus aus und legt Befunde mit Prüffall an, etwa für Subnetze, aus denen telefoniert wird, die aber keinem Notrufstandort zugeordnet sind. Die Ampel zeigt, in welchem Bereich die Befunde liegen. Im Benutzer-Steckbrief siehst du für einen einzelnen Benutzer Notrufstandort und effektive Richtlinien nebeneinander.

Die Drift-Erkennung vergleicht den aktuellen Stand mit einem früheren und zeigt, wenn nach einem Netzumbau LIS-Einträge oder Standortzuordnungen verändert wurden. Im Bericht lassen sich die Befunde an Netzwerk- oder Sicherheitsverantwortliche weitergeben.

Mehr dazu auf der Produktseite Teams-Telefonie Diagnostiker. 15 Tage kostenlos testen.



So trägst du für einen Notrufstandort Adresse und Subnetze ein und siehst die Prüfung der Eingaben (Demo-Daten).

Behebung mit Rollback-Plan

Bevor du schreibst, sicherst du den Ist-Stand. Das ist bei LIS-Daten besonders wichtig, weil Set-Befehle bestehende Einträge mit gleicher Kennung ohne Rückfrage ersetzen.

```
$stamp = Get-Date -Format 'yyyyMMdd-HHmm'
Get-CsOnlineLisSubnet              | Export-Csv "lis-subnet-$stamp.csv" -NoTypeInformation
Get-CsOnlineLisWirelessAccessPoint | Export-Csv "lis-wap-$stamp.csv" -NoTypeInformation
Get-CsOnlineLisSwitch              | Export-Csv "lis-switch-$stamp.csv" -NoTypeInformation
Get-CsOnlineLisPort                | Export-Csv "lis-port-$stamp.csv" -NoTypeInformation
Get-CsTenantNetworkSite            | Export-Csv "sites-$stamp.csv" -NoTypeInformation
```

Subnetz im LIS nachtragen oder korrigieren

1. **Netzwerk-ID ermitteln:** aus IP und Präfixlänge, die die Clients tatsächlich bekommen, nicht aus dem Netzplan von vor drei Jahren.
2. **Location-ID holen:** Im Admin Center unter Standorte › Notfalladressen die Adresse öffnen und die Location-ID des passenden Orts im Gebäude kopieren, oder per Get-CsOnlineLisLocation.
3. **Eintragen:** Set-CsOnlineLisSubnet -Subnet 10.50.12.0 -LocationId <Location-ID> -Description "Hamburg 1. OG". Alternativ im Admin Center unter Standorte › Netzwerke und Standorte › Subnetze, bei vielen Einträgen per CSV-Upload.
4. **Verifizieren:** Get-CsOnlineLisSubnet erneut abfragen, nach der Verteilzeit am Client in der Anrufe-App nachsehen.

BSSIDs sauber eintragen

5. **BSSIDs vom WLAN-Controller exportieren,** nicht die Ethernet-MACs der Zugangspunkte.
6. **Format umbauen:** Doppelpunkte durch Bindestriche ersetzen, Großbuchstaben verwenden.

7. **Platzhalter bewusst setzen:** Set-CsOnlineLisWirelessAccessPoint -BSSID 00-00-5E-00-53-1* -LocationId <Location-ID> -Description "Frankfurt 2. OG". Nur, wenn der Bereich wirklich nur Funkzellen dieses Orts enthält.
8. **Falsche Einträge entfernen:** Remove-CsOnlineLisWirelessAccessPoint für Einträge, die mit Doppelpunkten oder der Ethernet-MAC angelegt wurden, damit sie nicht später verwirren.

VPN-Pool aus der Gleichung nehmen

Steht der VPN-Pool 10.99.0.0/16 im LIS mit der Adresse der Zentrale, entfernst du diesen Eintrag. Steht er in einem Netzwerkstandort, der eine eigene Notruf-Routingrichtlinie hat, ordnest du ihn einem eigenen Standort ohne Notrufrichtlinien zu oder nimmst ihn heraus. Dann greifen die Benutzerrichtlinien und die Rückfallkette mit bestätigter Adresse. Prüfe die Auswirkungen auf andere Funktionen wie Location-Based Routing, bevor du Netzwerkstandorte änderst.

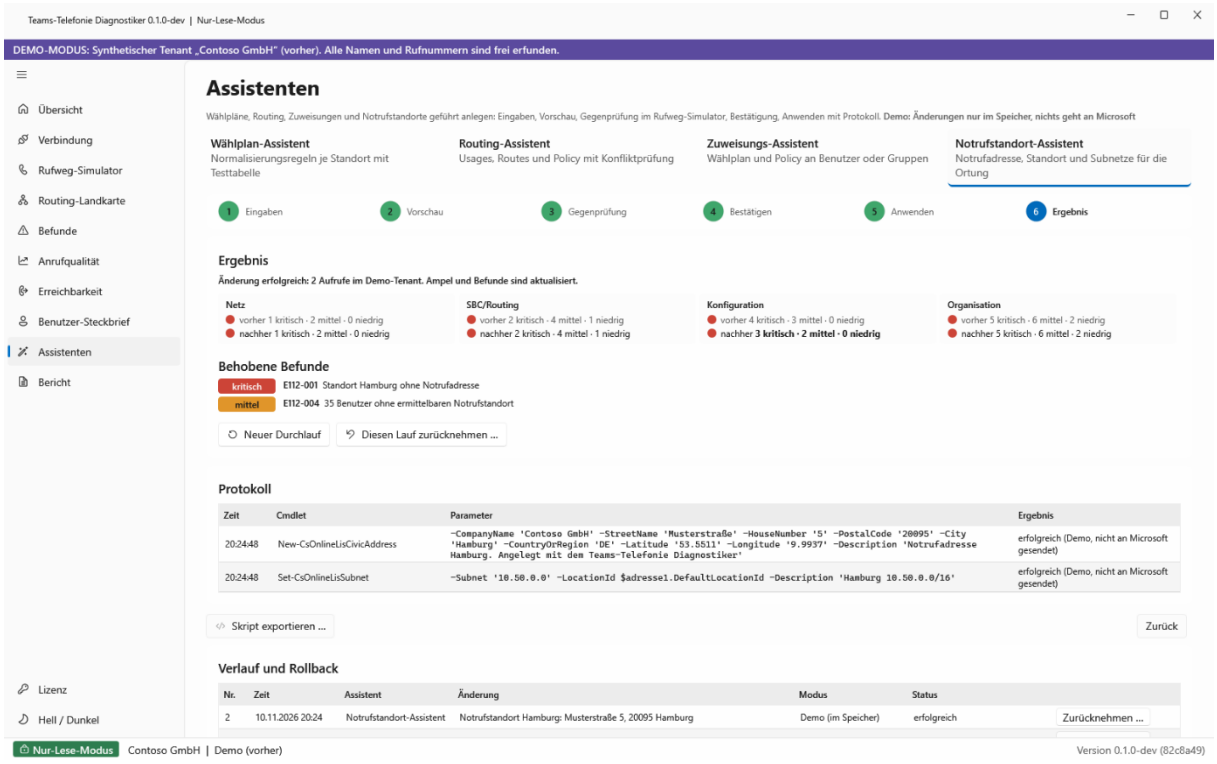
Richtlinien an Standorte binden

Für jeden Standort mit eigenem SBC oder Anschluss legst du eine ECRP an, die 110 und 112 auf die Usage dieses Standorts lenkt, und weist sie dem Netzwerkstandort zu. Die Benachrichtigung regelst du über eine ECP je Standort, damit in Hamburg nicht der Frankfurter Empfang angerufen wird:

```
$n112 = New-CsTeamsEmergencyNumber -EmergencyDialString '112' -EmergencyDialMask '911' `
        -OnlinePSTNUsage 'DE-Notruf-HH'
$n110 = New-CsTeamsEmergencyNumber -EmergencyDialString '110' -OnlinePSTNUsage 'DE-Notruf-HH'
New-CsTeamsEmergencyCallRoutingPolicy -Identity 'ECRP-Hamburg' -EmergencyNumbers $n112,$n110 `
        -AllowEnhancedEmergencyServices:$true
Set-CsTenantNetworkSite -Identity 'HH' -EmergencyCallRoutingPolicy 'ECRP-Hamburg'

New-CsTeamsEmergencyCallingPolicy -Identity 'ECP-Hamburg' -NotificationGroup 'empfang-
hh@contoso.com' `
        -NotificationMode NotificationOnly -ExternalLocationLookupMode Enabled
Set-CsTenantNetworkSite -Identity 'HH' -EmergencyCallingPolicy 'ECP-Hamburg'
```

Die PSTN Usage DE-Notruf-HH muss vorher existieren und eine Voice Route mit dem Muster ^(110|112)$ auf den Hamburger SBC haben. Wählpläne, die 110 und 112 unangetastet lassen, sind die Voraussetzung. Die Reihenfolge von Usage und Route erklärt Voice Routing Policy, PSTN Usage und Voice Route: Reihenfolge verstehen. Den Schalter PIDF/LO aktivierst du am SBC im Admin Center unter Sprache › Direct Routing oder per Set-CsOnlinePSTNGateway -PidfloSupported $true, nachdem du mit dem SBC-Hersteller geklärt hast, dass er damit umgehen kann. Die SBC-Seite beschreibt Teams Direct Routing einrichten.



So sieht das Ergebnis nach dem Eintragen einer Notrufadresse und eines Subnetzes aus, mit Protokoll der ausgeführten Cmdlets und Rücknahme im Verlauf (Demo-Daten).

Rollback

Änderung	Rücknahme
Neues LIS-Subnetz	Remove-CsOnlineLisSubnet -Subnet 10.50.12.0
Geändertes LIS-Subnetz	Set-CsOnlineLisSubnet mit alter Location-ID aus dem CSV-Export
Neuer WLAN-Eintrag	Remove-CsOnlineLisWirelessAccessPoint -BSSID <Eintrag>
Switch oder Port	Remove-CsOnlineLisSwitch bzw. Remove-CsOnlineLisPort, alte Werte per Set-Befehl aus dem Export
Richtlinie am Netzwerkstandort	Set-CsTenantNetworkSite mit dem vorherigen Wert aus sites-*.csv
Neue ECRP oder ECP	erst vom Standort lösen, dann Remove-CsTeamsEmergencyCallRoutingPolicy bzw. Remove-CsTeamsEmergencyCallingPolicy
PidfloSupported	Set-CsOnlinePSTNGateway -Identity sbc2.contoso.com -PidfloSupported $false

WARNUNG · Rollback braucht auch Zeit

Die Verteilzeit von bis zu vier Stunden gilt in beide Richtungen. Wer um 16 Uhr eine Änderung zurücknimmt, sollte nicht um 16:05 Uhr den Erfolg melden. Ändere Notrufkonfiguration deshalb nicht am Freitagnachmittag, auch wenn der schwarze Humor in der IT dafür einen eigenen Ordner hat.

Vorbeugung: damit der Notrufstandort stimmt, wenn es darauf ankommt

- **LIS an den Netzbetrieb koppeln:** Jede Änderung an Subnetzen, Masken, Zugangspunkten oder Switches bekommt im Change-Prozess die Frage „Ist das LIS angepasst?“. Ohne diese Frage veraltet das LIS mit jedem Umbau ein bisschen mehr.
- **Eine Quelle der Wahrheit:** Subnetze für Netzwerkstandorte und LIS aus derselben Liste pflegen, am besten aus dem IP-Adressmanagement exportiert und per CSV hochgeladen.
- **WLAN-Tausch als Notruf-Thema behandeln:** Neue Zugangspunkte bedeuten neue BSSIDs. Der Export aus dem Controller gehört zum Abnahmeprotokoll.
- **VPN-Pools dokumentieren:** Welche Pools gibt es, stehen sie in einem Netzwerkstandort, stehen sie im LIS? Die richtige Antwort auf die letzte Frage ist fast immer nein.
- **Stichproben am Client:** Einmal im Quartal je Standort in der Anrufe-App nachsehen, was angezeigt wird, im Büro, im WLAN, am Kabel, im Homeoffice.
- **Abweichungen automatisch erkennen:** Ein regelmäßiger Export der LIS- und Standortdaten mit Vergleich zum Vormonat zeigt Änderungen, die niemand angekündigt hat.

Wie solche Vergleiche aufgebaut werden, beschreibt Konfigurationsdrift in der Teams-Telefonie erkennen. Wer die Verantwortung für Notrufdaten zwischen Netzwerk-, Telefonie- und Sicherheitsteam regeln will, findet Ansätze in Microsoft Teams Telefonie-Governance. Und wenn du das Thema an einem Stück mit deinen Standorten durchgehen willst: In der Beratung zur Teams-Telefonie schauen wir uns LIS, Netzwerkstandorte und Notruf-Routing gemeinsam an; in der Schulung Teams-Telefonie übt dein Team die Pflege selbst.

WEITERLESEN · Passend zum Thema

› Notrufadresse fehlt in Teams: was bei 112 wirklich passiert
› Netzwerkstandorte und Subnetze in Teams richtig pflegen
› Teams-Telefonie über VPN: Split Tunneling richtig einrichten
› Notruf in Teams testen, ohne die Leitstelle zu verärgern

FAQ zum dynamischen Notruf in Teams

Warum zeigt Teams im Büro keinen Notrufstandort an, obwohl das Subnetz im Netzwerkstandort steht?

Weil Netzwerkstandort und LIS getrennte Tabellen sind. Der Netzwerkstandort liefert Richtlinien, das LIS liefert die Adresse. Das Subnetz muss zusätzlich im LIS mit der richtigen Netzwerk-ID und einer validierten Adresse stehen, und die öffentliche IP des Standorts muss als Trusted IP eingetragen sein.

In welchem Format trage ich die BSSID ein?

Mit Bindestrichen im Format nn-nn-nn-nn-nn-nn, zum Beispiel 00-00-5E-00-53-1A. Windows zeigt die BSSID mit Doppelpunkten an; die musst du umbauen. Ein Platzhalter * ist an den letzten ein bis zwei Zeichen erlaubt.

Funktioniert der dynamische Notruf auf Teams-Telefonen im WLAN?

Nein. Laut Microsoft werden WLAN-basierte Standorte auf allen Teams-Clients außer Teams Phones unterstützt. Für Tischtelefone nutzt du Subnetz oder Switch und Port per LLDP.

Was passiert im Homeoffice?

Die öffentliche IP ist nicht vertrauenswürdig, das LIS liefert nichts. Teams greift dann auf eine vom Benutzer bestätigte Adresse, einen Vorschlag des Betriebssystems, eine manuelle Eingabe oder zuletzt die registrierte Adresse an der Rufnummer zurück. Die Eingabe durch den Benutzer setzt den External Location Lookup Mode in der Emergency Calling Policy voraus.

Warum zeigt Teams im VPN die Adresse der Zentrale an?

Weil der VPN-Pool im LIS mit dieser Adresse steht und der Dienst über den Full Tunnel eine vertrauenswürdige IP sieht. Nimm den Pool aus dem LIS und aus Netzwerkstandorten mit eigenen Notrufrichtlinien.

Brauche ich bei Calling Plans eine Emergency Call Routing Policy?

Nein. Die ECRP wirkt nur bei Direct Routing. Man kann sie Calling-Plan-Benutzern zwar zuweisen, laut Microsoft hat sie dort aber keine Wirkung. Die Emergency Calling Policy für die Benachrichtigung gilt dagegen für alle Anschlussarten.

Wie lange dauert es, bis eine LIS-Änderung beim Client ankommt?

Microsoft nennt bis zu vier Stunden für die Verteilung. Ein Neustart des Clients oder ein Netzwechsel löst danach die neue Abfrage aus.

Routet Teams in Deutschland den Notruf anhand des dynamischen Standorts zur richtigen Leitstelle?

Für Direct Routing beschreibt Microsoft das automatische Routing anhand des dynamischen Standorts nur für die USA und Kanada. In Deutschland steuerst du den Weg über die Notruf-Routingrichtlinie am Netzwerkstandort, also über SBC und Anschluss der Niederlassung. Was der Netzbetreiber mit einer Standortangabe im INVITE macht, regelt dein Vertrag.

Fazit: Teams weiß nur, was du ihm beigebracht hast

Dynamischer Notruf in Teams scheitert selten an Teams und fast immer an einer Tabelle, die nicht mit dem Netz mitgewachsen ist. Ein Subnetz, das nur im Netzwerkstandort steht. Eine Maske, die sich geändert hat. BSSIDs mit Doppelpunkten oder vom alten WLAN. Ein VPN-Pool mit der Adresse der Zentrale. Eine Standortrichtlinie, die nie zugewiesen wurde. Jeder dieser Fehler ist für sich banal, und keiner meldet sich von allein.

Die gute Nachricht: Mit einer Handvoll lesender Befehle bekommst du den Zustand in einer Stunde auf den Tisch. Prüfe vom Client nach außen, sichere vor jeder Änderung den Ist-Stand und bau das LIS in den Change-Prozess deines Netzwerkteams ein. Dann ist die Antwort auf die Frage „Wo sind Sie genau?“ schon unterwegs, bevor jemand sie stellen muss. Ausführliche Hintergründe liefert Microsoft in Planen und Konfigurieren dynamischer Notrufe.