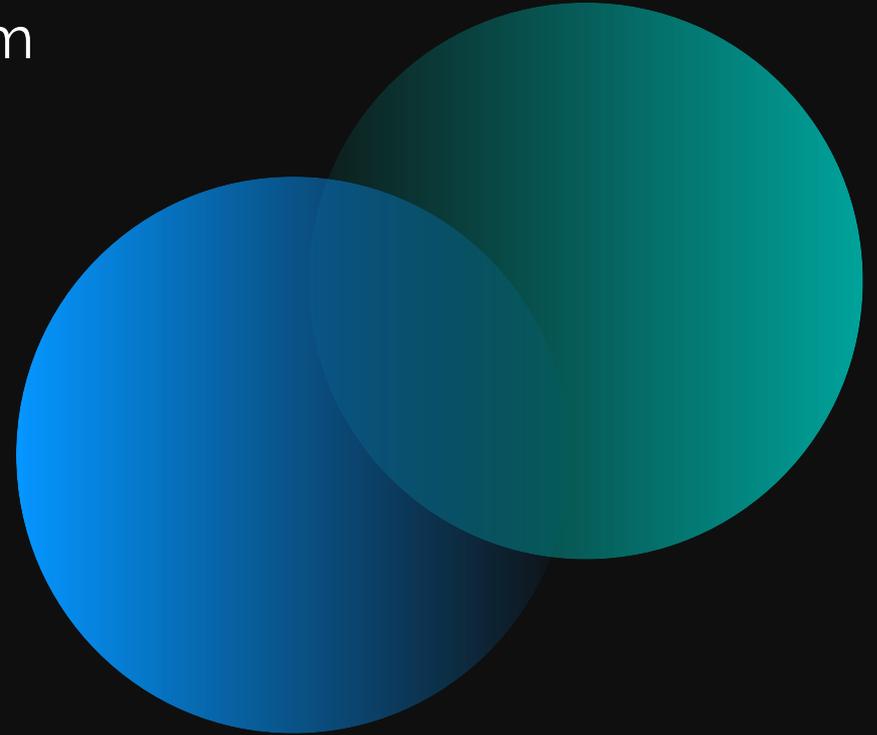


 Unify Remote Service Platform

Kunden Präsentation



Remote Service Platform

Überblick Remote Service Platform



Anforderungen für den
Remote Support



Was ist die Unify Remote
Service Platform?

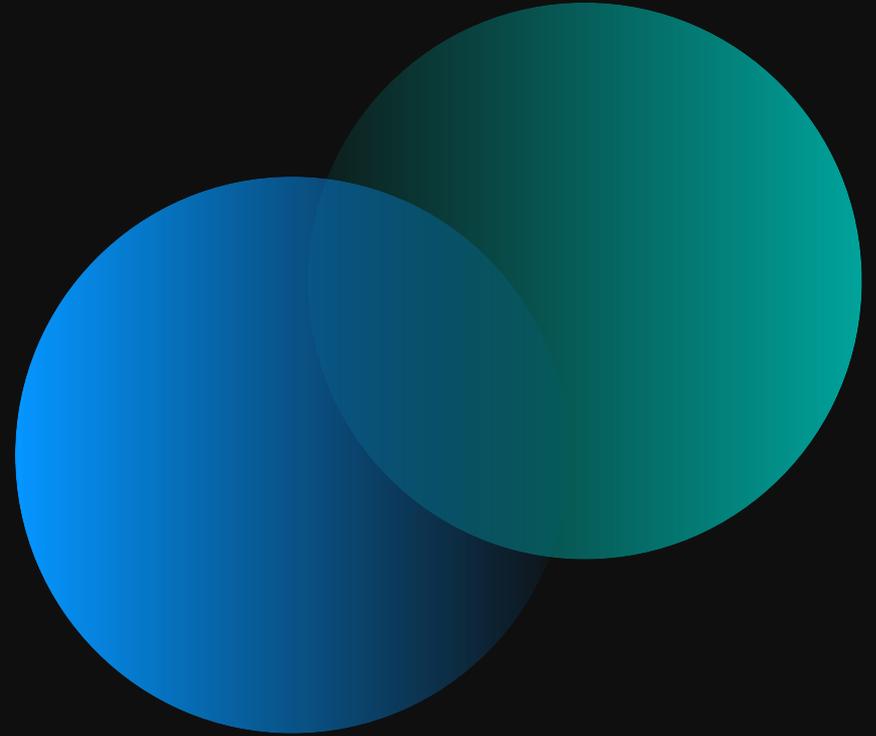


Verbindungsszenarien



Security

Anforderungen für den Remote Support



Remote Service Platform

Anforderungen für den Remote Support

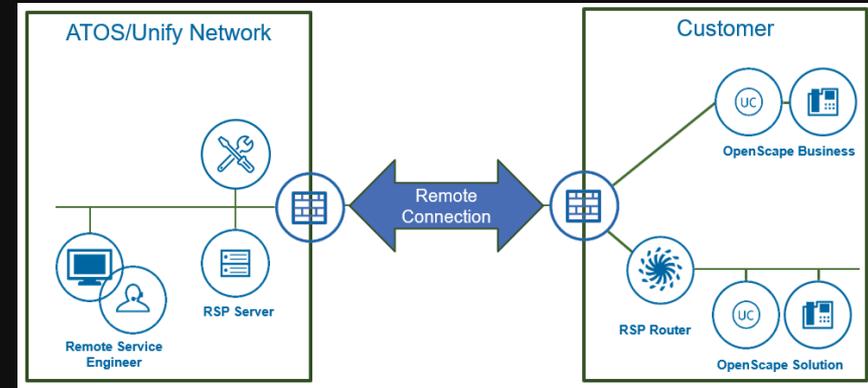
Kontrollierter, sicherer Zugang



Schnellere Lösung



Zusätzliche Möglichkeiten



Remote Service Platform

Was bietet die ATOS / Unify Remote Service Platform?

Einfache Unterstützung

Schnelle Problemanalyse

Unmittelbarer Fernzugriff auf
Systeme

Verfügbar 24/7

Effiziente Leistungserbringung

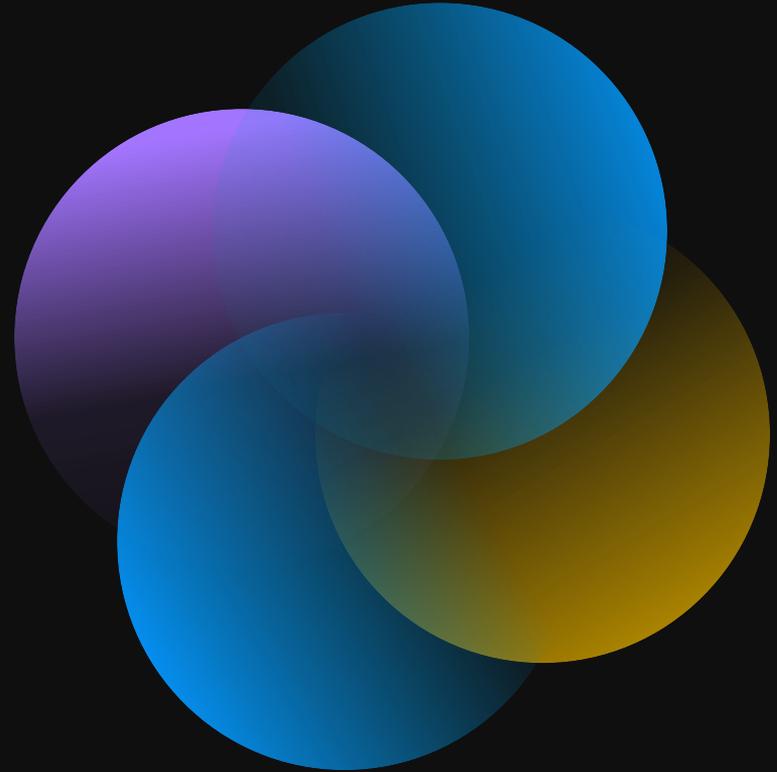
Vermeidung von Anfahrten

Zugriff auf die Kompetenz eines
kompletten Unify-Expertenteams

Optimierte Servicebereitstellung
seitens Unify

RSP hat alle Vorteile eines vollständig gehosteten Dienstes

Was ist die Unify
Remote Service
Plattform?



Remote Service Plattform

Überblick

Die Remote Service Plattform (RSP) bietet effizienten Remote Service für ATOS / Unify Kunden.

RSP ist eine Infrastruktur zur Verwaltung der Geräteinformationen, zur Konnektivität und des Dateiaustauschs bei hoher Verfügbarkeit und hoher Sicherheit.

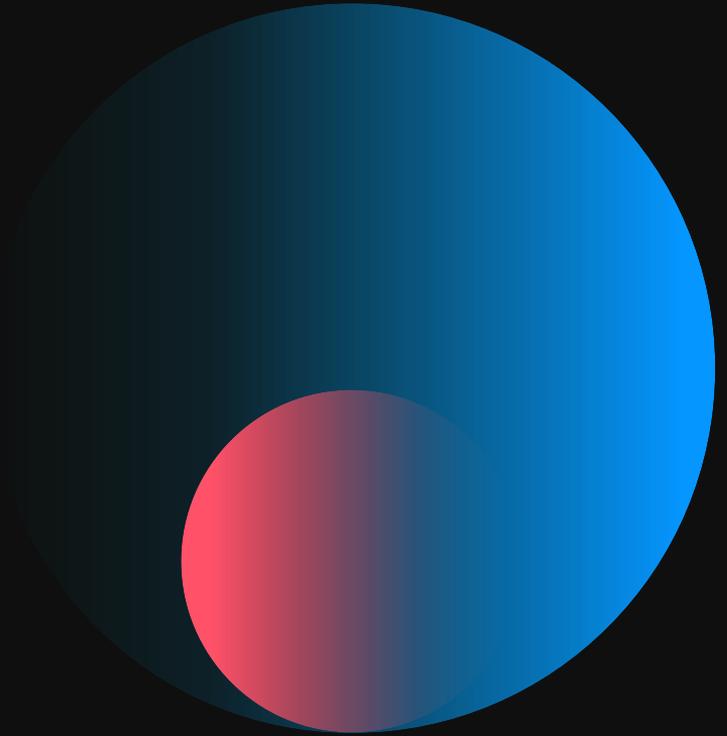
Die Remote Service Plattform bietet zwei Verbindungstypen:

RSP.servicelink (bevorzugte Lösung). Basierend auf OpenVPN-Technologie (SSL VPN). Vor Ort wird der RSP-Router platziert. Anmerkung: OpenScape Business benötigt diesen Router nicht.

Site-to-Site VPN (IPSec-Option) zur Unterstützung des etablierten Industriestandards

RSP ist eine zukunftssichere Plattform und unterstützt das gesamte ATOS / Unify Produktportfolio

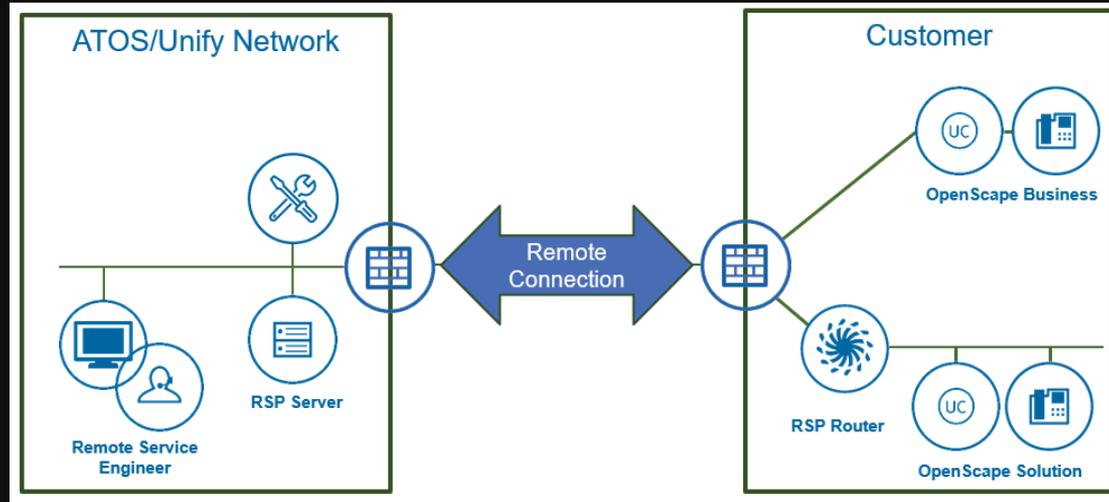
Verbindungsszenarien



Remote Service Platform

RSP.servicelink

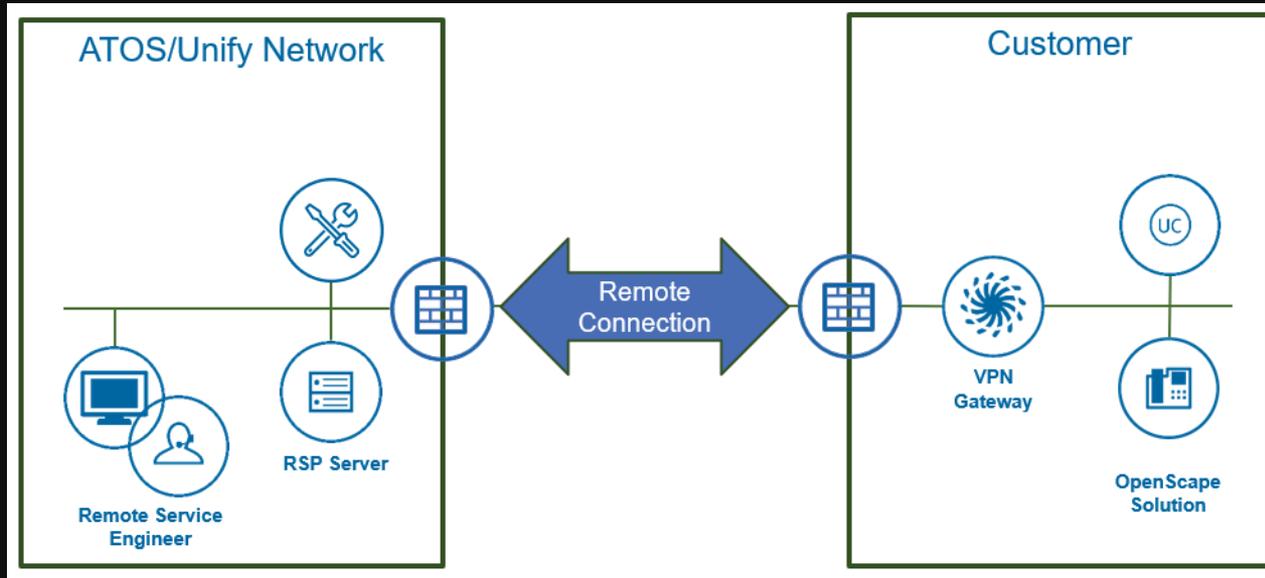
RSP.servicelink, basierend auf OpenVPN-Technologie (SSL VPN). Vor Ort wird der RSP-Router platziert. Anmerkung: OpenScape Business benötigt diesen Router nicht.



Remote Service Platform

Site-to-Site VPN

Site-to-Site VPN (IPSec-Option) zur Unterstützung des etablierten Industriestandards. Voraussetzung ist ein kundeneigenes VPN-Gateway.



Remote Service Platform

Technische Voraussetzungen

RSP.servicelink

Port 443 für ausgehende Verbindungen basierend auf dem Standard-HTTP-Protokoll zulassen

SSL-Tunneling muss in der Firewall zugelassen sein (OpenVPN lässt keine "Man in the middle"-Prüfungen zu)

Verbindung zu RSP IP-Adressen zulassen (max. 4)

Site-to-Site VPN

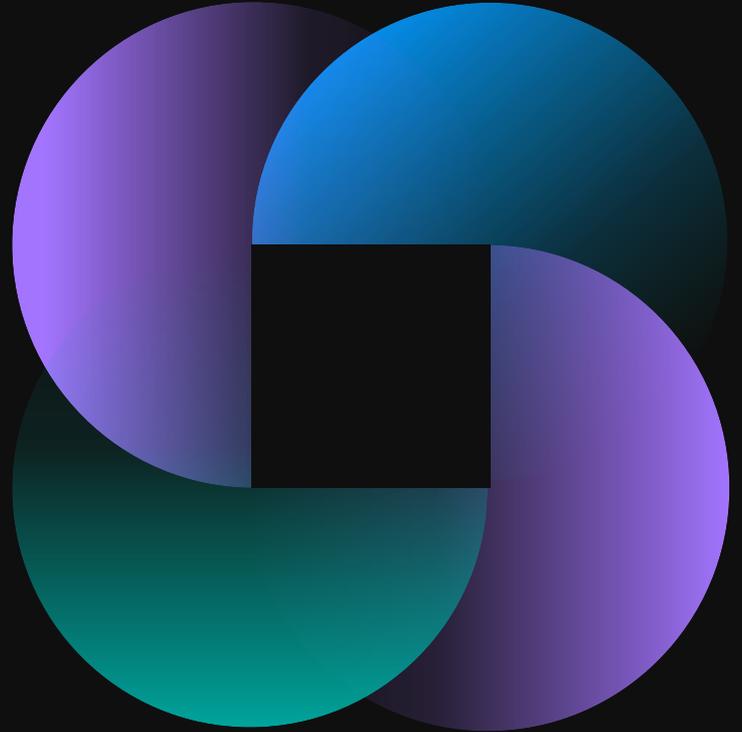
Dauerhafter Zugang auf Remote Hosts

Nutzung von IKE V2 und V1

Verschlüsselung AES 256, SHA 512 und Diffie-Hellman group 24

Wählen Sie die Konnektivität je nach Ihren Anforderungen

Security



Remote Service Platform

Security Aspekte 1



Sicherer Zugang über die Remote Service Plattform

- Nur registrierte Benutzer können die RSP-Plattform nutzen
- Zugriffsbeschränkung der Servicetechniker je nach Rolle und Region
- Protokollierung aller Verbindungen zu Kundensystemen oder Auslesen von Passwortinformationen

Remote Service Platform

Security Aspekte 2



Um Ihr Intranet vor wechselseitigen Problemen und Angriffen zu schützen, haben wir unsere RSP in demilitarisierten Zonen (DMZ) gesichert. Verbindungen vom Servicetechniker zum Kundensystem und umgekehrt werden nicht direkt "durchgestellt". Sie terminieren auf den RSP-Servern mit Hilfe einer Reverse-Proxy-Funktion.

Das Serverzertifikat auf unserer RSP garantiert, dass der installierte RSP.servicelink Router oder die Produkte mit integriertem RSP.servicelink Plug-in (z. B. OpenScape Business) nur eine Verbindung zur Unify Remote Service Platform herstellen.

Remote Service Platform

Security Aspekte 3



RSP.servicelink

RSP.servicelink basiert auf OpenVPN. OpenVPN verwendet ein industrietaugliches Sicherheitsmodell, das zum Schutz vor passiven und aktiven Angriffen entwickelt wurde. Das Sicherheitsmodell basiert auf der Verwendung von SSL/TLS mit Client- und Serverzertifikaten für die bidirektionale Authentifizierung und den Schlüsselaustausch. Wenn die SSL/TLS-Authentifizierung erfolgreich ist, wird die Verschlüsselung/Entschlüsselung und das HMAC-Schlüsselquellmaterial zufällig generiert.

Um sicherzustellen, dass nur zertifizierte Kundenprodukte eine Verbindung zu unserem zentralen RSP Server herstellen können, werden vor Ort Client-Zertifikate verwendet,

Remote Service Platform

Security Aspekte 4



Site-to-Site VPN

- Site-to-Site VPN auf Basis von IPsec verbindet Unify RSP mit dem Kundennetzwerk und erfordert ein kundeneigenes VPN-Gateway
- Unterstützung der höchsten verfügbaren Verschlüsselung mit bis zu AES256, SHA512 und DH-Gruppe 24

Vielen Dank!



Atos, the Atos logo, Atos | Syntel are registered trademarks of the Atos group.
August 2021. © 2021 Atos. Confidential information owned by Atos, to be used by the
recipient only. This document, or any part of it, may not be reproduced, copied,
circulated and/ or distributed nor quoted without prior written approval from Atos.