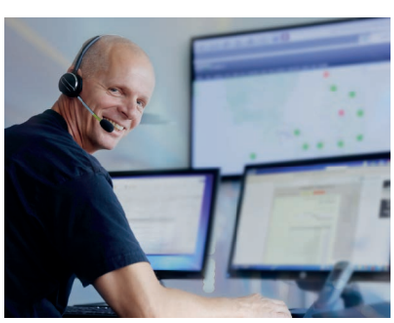
Ascom Remote Access

Ascom-systemen onderhouden en optimaliseren via beveiligde remote toegang op basis van Microsoft Azure



Als u Ascom de mogelijkheid biedt om remote toegang te krijgen tot uw installaties, heeft dat een aantal belangrijke voordelen. Zo kan remote access reactie- en oplostijden bij voorkomende problemen op locatie verkorten. Tevens kunnen onze technici software-updates uitvoeren, logbestanden ophalen en programeerwijzigingen doorvoeren.

Ondanks de voordelen zijn sommige IT-beheerders huiverig voor toegang op afstand; hierdoor worden kritische netwerken immers toegankelijk voor buitenstaanders. Om aan deze zorgen tegemoet te komen, maakt de Ascom Remote Access-service gebruik van beproefde standaard componenten, die bevoegd Ascom-personeel en geautoriseerde onderaannemers toestemming geven om via beveiligde toegangspunten het netwerk van de klant binnen te gaan.

Hoewel Ascom Remote Access een gecentraliseerde oplossing is, garandeert het een strikte scheiding tussen uw netwerk en dat van Ascom.

Ascom Remote Access is aan strenge testen onderworpen om u te beschermen tegen binnendringen door onbevoegden. Als oplossing gebouwd in een digitale omgeving, is Ascom Remote Access volledig schaalbaar, om in de behoeften van zelfs de grootste bedrijven te voorzien, en alleen beschikbaar als onderdeel van een Ascom Solution Lifecycle Plan.

ascom

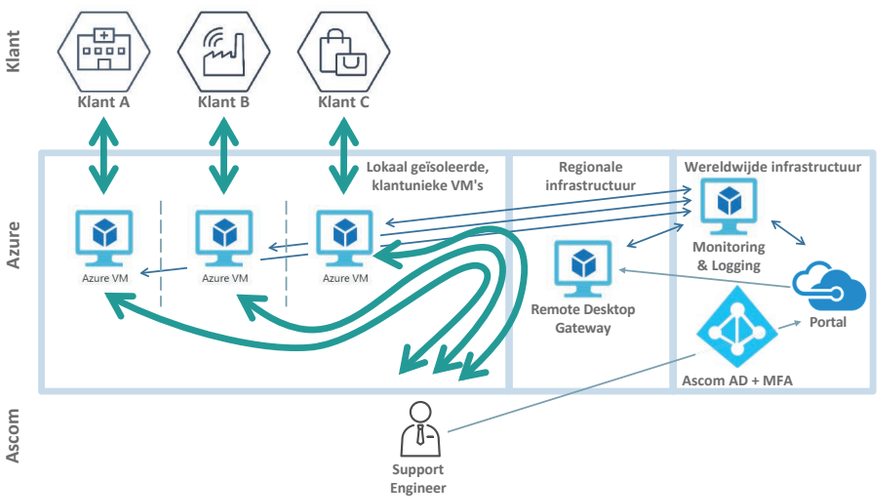
Ascom Remote Access configureren

De toegang op afstand kan op twee manieren worden geconfigureerd:

1. **Client VPN**
2. **Site-to-site VPN**

De support engineers van Ascom krijgen toegang door middel van een 2 factor authenticatieprocedure, bestaande uit een Ascom Active Directory-authenticatie plus een eenmalig wachtwoord. Ascom-personeel mag alleen netwerken binnengaan waarvoor ze voorafgaande authorisatie hebben gekregen, en via applicatietunnels in de portal.

Ascom Remote Access-architectuur



Configuratiemethode 1: **Client VPN**

Bij deze methode wordt een Client Virtual Private Network (VPN) geconfigureerd op het virtuele werkstation in het Ascom Remote Access netwerk. Het virtuele werkstation is toegankelijk via een webbrowser met behulp van het beveiligde HTTPS-communicatieprotocol. Dit virtuele werkstation wordt vervolgens gebruikt om toegang te krijgen tot die diensten in het netwerk van de klant, die door Ascom beheerd worden. Het virtuele werkstation is geïsoleerd en heeft alleen toestemming om te communiceren met een specifiek netwerk van de klant. Communicatie met het netwerk van de klant is pas toegestaan nadat de Ascom support engineer zich met succes heeft geauthenticeerd via de authenticatieprocedure.

Configuratiemethode 2: **Site-to-site VPN**

Bij deze methode wordt een site-to-site Virtual Private Network (VPN) link geconfigureerd tussen het Ascom Remote Access netwerk en een netwerk van de klant. Een virtueel werkstation is toegankelijk via een webbrowser met behulp van het beveiligde HTTPS-communicatieprotocol. Het wordt vervolgens gebruikt om verbinding te maken met die diensten in het netwerk van de klant, die door Ascom beheerd worden. Het virtuele werkstation is geïsoleerd en heeft alleen toestemming om te communiceren met een specifiek netwerk van de klant. Communicatie met het netwerk van de klant is alleen toegestaan via het geïsoleerde virtuele werkstation en pas nadat de Ascom support engineer zich met succes heeft geauthenticeerd via de authenticatieprocedure.

Verbinden met het netwerk van de klant

Ongeacht welke configuratiemethode wordt gebruikt, nemen de Ascom support engineers de volgende stappen wanneer ze verbinding maken met netwerken van klanten:

- De Ascom support engineer verschaft zich toegang tot de supportportal via een webbrowser.
- De support engineer authenticeert zich met zijn gebruikersnaam en wachtwoord en een eenmalig wachtwoord.
- Na succesvolle authenticatie krijgt de Ascom support engineer een portal te zien met links die exclusief verbinding maken met de specifieke systemen waarvoor autorisatie is verleend.
- Wanneer de Ascom support engineer verbinding maakt met één van de links, wordt hem of haar door de portal toegang verleend tot de virtuele Azure Machine, met unieke instellingen voor de klant in kwestie.
- De virtuele computer bevindt zich geografisch gezien zo dicht mogelijk bij de klant. Verkeer en dataopslag blijven binnen een land, een regio of duidelijk gedefinieerd gebied, zoals de Europese Unie.

ascom

Beveiligde hosting op het Microsoft Azure cloudplatform

De virtuele computers worden gehost op het Microsoft Azure cloudplatform in een datacenter dat zich zo dicht mogelijk bij de klant bevindt. De servers staan zich op diverse locaties over de hele wereld, onder andere (maar niet uitsluitend) in West-Europa, Noord-Amerika en Australië. Hiervoor is gekozen om de gegevens van de klant zoveel mogelijk lokaal te houden en te kunnen voldoen aan de wettelijke voorschriften in alle landen waar Ascom klanten ondersteunt. IP-verkeer van een klant wordt naar een openbaar Microsoft Azure IP-adres in het land of de regio gestuurd, naar de specifieke virtuele computers die eveneens in Microsoft Azure gehost worden binnen het land of de regio. Ook de Ascom support engineer maakt lokaal verbinding met de portal, zodat het verkeer binnen het land of de regio in kwestie blijft.

Het systeemontwerp wordt uitgevoerd door vertrouwde partners van Microsoft, en de architectuur wordt beoordeeld door zowel Microsoft als externe IT-beveiligingsspecialisten, om te waarborgen dat aan de hoogst mogelijke beveiligingsnormen wordt voldaan.

Naleving van AVG en andere regelgeving

Tijdens een supportsessie worden technische logbestanden opgehaald, overgedragen en geanalyseerd door werknemers of partners van Ascom. Persoonsgegevens en andere gevoelige informatie worden tijdens het supportproces normaliter aan niemand bekendgemaakt, maar in bepaalde situaties kan het voorkomen dat sommige persoonsgegevens deel uitmaken van uitgebreide logbestanden, etc. Een Gegevensverwerkingsovereenkomst is een standaard onderdeel van alle supportcontracten tussen de klant en Ascom. In deze overeenkomst wordt uiteengezet hoe wij met gevoelige informatie omgaan.

Ascom en de partners waarmee we deze dienst inrichten zijn ISO27001 gecertificeerd en houden zich aan de Algemene verordening gegevensbescherming (Verordening (EU) 2016/679), en gelijkwaardige voorschriften in andere landen. Door gebruik te maken van de Microsoft Azure cloud kunnen we het verkeer binnen de administratieve (d.w.z. EU-)grenzen houden, of binnen specifieke nationale jurisdicties, voor klanten buiten de EU.

Neem voor meer informatie over de voordelen van Ascom Remote Access contact op met de Ascom vertegenwoordiger bij u in de buurt. U vindt een volledige lijst met Ascom vertegenwoordigers wereldwijd op: ascom.com

Ascom (Nederland) B.V.
Postbus 40242 3504 AA Utrecht
T: +31 30 240 91 00
E: info.nl@ascom.com
www.ascom.nl

Over Ascom

Ascom is een internationale aanbieder van ICT-oplossingen en mobiele werkstroomsystemen voor de gezondheidszorg. De visie van Ascom is erop gericht om hiaten in de digitale informatievoorziening te dichten en optimale beslissingen mogelijk te maken – overal en altijd. De missie van Ascom is missiekritische, realtime oplossingen te bieden voor zeer mobiele, ad hoc- en tijdgevoelige omgevingen. Ascom gebruikt zijn unieke product- en systeemportfolio en kennis van softwarearchitectuur om integratie- en mobilisatieoplossingen te creëren die voor soepele, complete en efficiënte workflows zorgen in zowel de gezondheidszorg als industriële sectoren en de detailhandel.

Ascom, waarvan het hoofdkantoor in Baar (Zwitserland) is gevestigd, heeft bedrijfsonderdelen in 18 landen en telt wereldwijd zo'n 1.300 medewerkers. Ascoms aandelen op naam (ASCN) zijn genoteerd aan de SIX Swiss Exchange in Zürich.