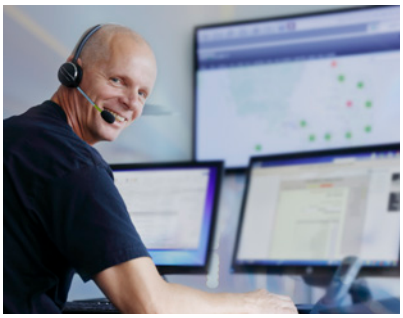
Ascom Remote Access

Maintaining and optimizing Ascom solutions via secure off-site access



Allowing Ascom to remotely monitor and access your installations offers several compelling benefits. Proactive monitoring, for instance, can alert our technicians to issues before they develop into more serious problems. And with remote access, our technicians can update software, fetch log files, and change settings.

Despite its benefits, some IT administrators are wary of remote access. It does after all give outsiders access to critical networks. To meet these concerns, the Ascom Remote Access service uses standard, well proven components that give authorized Ascom personnel permission to enter customer networks through secure access points.

Although a centralized solution, Ascom Remote Access ensures strict separation between your and Ascom networks.

Ascom Remote Access is rigorously tested to safeguard against unauthorized penetration. Built in a digital environment, the solution is fully scalable to meet the needs of even the largest, Access is available only as part of an Ascom Solution Lifecycle Plan.

ascom

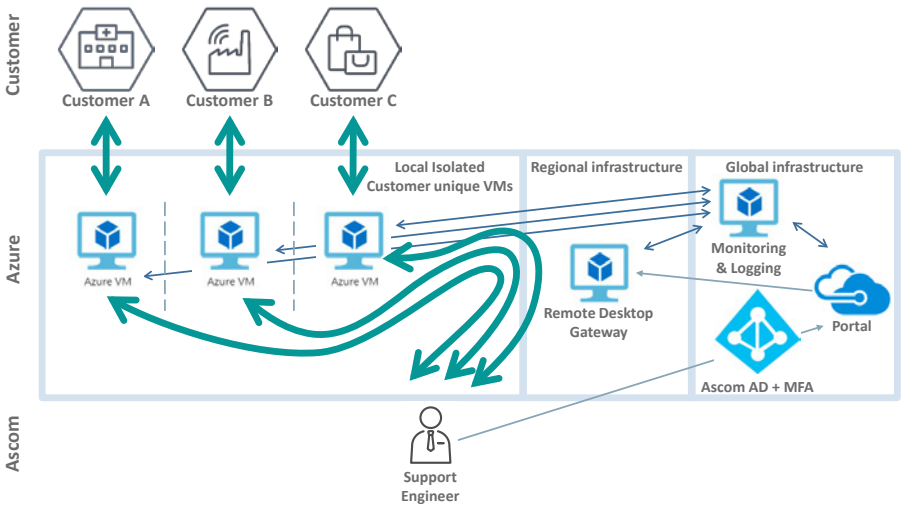
Configuring Ascom Remote Access

Remote access can be configured in two ways:

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

Ascom support engineers are authenticated by two-factor authentication consisting of Ascom AD authentication plus a one-time password. Ascom personnel may only access networks for which they have received prior authorization, and via application tunnels in the portal.

Ascom Remote Access Architecture



Configuration method 1: **Client VPN**

This method involves configuring a client Virtual Private Network (VPN) in the virtual workstation within the remote access network. The virtual workstation is accessed via a web browser using the secure HTTPS communication protocol. This virtual workstation is then used to access those services in the customer network managed by Ascom. The virtual workstation is isolated, and is only permitted to communicate with a specified customer's network. Communication with the customer's network is only permitted once the Ascom support engineer successfully authenticates himself/herself via the two-factor authentication portal.

Configuration method 2: **Site-to-site VPN**

This method involves configuring a site-to-site Virtual Private Network (VPN) link between the remote access system and a customer network. A virtual workstation is accessed via a web browser using the secure HTTPS communication protocol. It is then used to connect to those services in the customer network managed by Ascom. The virtual workstation is isolated, and is only permitted to communicate with a specified customer's network. Communication with the customer's network is only permitted through the isolated virtual workstation once the Ascom support engineer successfully authenticates himself/herself via the two-factor authentication portal.

Connecting to customer networks

Whichever configuration method is used, Ascom support engineers take the following steps when connecting to customer networks:

- The Ascom support engineer accesses the remote support portal via a web browser.
- The support engineer authenticates himself/herself with a username, password and a one-time password.
- Following successful authentication, the Ascom support engineer is presented with a portal containing links that connect exclusively to the specific systems for which authorization has been granted.
- When the Ascom support engineer accesses one of the links, the support engineer is granted access by the portal to the Azure virtual machine uniquely set up for the specific customer.
- The virtual machine is geographically located as close as possible to the customer. Traffic and data storage is kept within a country, or within a region or clearly defined bloc such as the European Union.

ascom

Secure hosting in the Microsoft Azure cloud platform

The virtual machines are hosted in the Microsoft Azure cloud platform in a data center located as close as possible to the customer. Servers are located in multiple locations around the globe, including (but not limited to) Western Europe, North America and Australia. This is done to keep customer data as local as possible and to fulfill legal regulations in all countries where Ascom supports customers. IP traffic from a customer is routed to a public Microsoft Azure IP address in the country or region, to the specific virtual machines also hosted in Microsoft Azure within the country/region. The Ascom support engineer also accesses the portal locally to keep the traffic within each country/region.

System design is carried out by Microsoft trusted partners, and architecture is reviewed by both Microsoft and third-party IT security specialists to ensure the highest possible security standards.

GDPR and other regulatory compliance

During a support session technical logs are fetched, transferred and analyzed by Ascom employees or partners. Personal data or other sensitive information is normally not exposed to anyone in the support process, but it may happen in certain situations that some personal data can be part of extended log files, etc. As part of all support contracts, a Data Processing Agreement is made between the customer and Ascom. This agreement details how we handle sensitive information.

Ascom and partners are ISO27001 certified, and adhere to the EU General Data and Protection Regulation (2016/679), and equivalent regulations in other countries. Using the Microsoft Azure cloud lets us keep traffic within administrative (e.g. EU) borders, or within specific national jurisdictions if outside the EU.

Contact your nearest Ascom representative to learn more about the benefits of Ascom Remote Access. A full list of Ascom representatives worldwide is available at: ascom.com

Ascom Holding AG
Zugerstrasse 32
CH-6340 Baar, Switzerland
info@ascom.com
Phone: +41 41 544 78 00
ascom.com

About Ascom

Ascom is a global solutions provider focused on healthcare ICT and mobile workflow solutions. The vision of Ascom is to close digital information gaps allowing for the best possible decisions – anytime and anywhere. Ascom's mission is to provide mission-critical, real-time solutions for highly mobile, ad hoc, and time-sensitive environments. Ascom uses its unique product and solutions portfolio and software architecture capabilities to devise integration and mobilization solutions that provide truly smooth, complete, and efficient workflows for healthcare as well as for industry and retail sectors.

Ascom is headquartered in Baar (Switzerland), has operating businesses in 18 countries and employs around 1,300 people worldwide. Ascom registered shares (ASCN) are listed on the SIX Swiss Exchange in Zurich.