Ascom Remote Monitoring

How monitoring by Ascom experts can help maximize system uptime

What it is and how you benefit
Ascom Remote Monitoring is an optional support service within the Ascom Solution Lifecycle Plan, a customizable after-sales support package. It lets our experts keep a watchful eye on the performance of your critical systems. Your organization benefits in three key ways:

Authorized Ascom specialists can take corrective action before minor issues become critical errors.

Quick pre-emptive action by Ascom experts can help ensure maximum uptime of your systems. Roles and responsibilities are agreed in advance, and are activated when needed.

You can focus resources on your organization's core activities, secure in the knowledge that your systems are being continuously monitored by Ascom specialists.

Ascom Remote Monitoring is a proven way to maintain uptime and functionality of critical systems in healthcare, industry, hospitality, retail, security, and other sectors.

The service works by collecting event info from Ascom and non-Ascom equipment such as servers, infrastructure and devices. It then presents the info in a dashboard view to authorized Ascom service technicians, who can issue warnings and/or take corrective action.

Why choose Ascom Remote Monitoring?
Errors can swiftly spread throughout interdependent systems. It is essential to maintain an overview, and to have the capability to pre-emptively intervene.

Systems are often vital to staff/customer/patient security and satisfaction. Compromised systems can expose confidential data to unnecessary risk.

ascom

01416-02 ENX 17.12 © Ascom (Sweden) AB

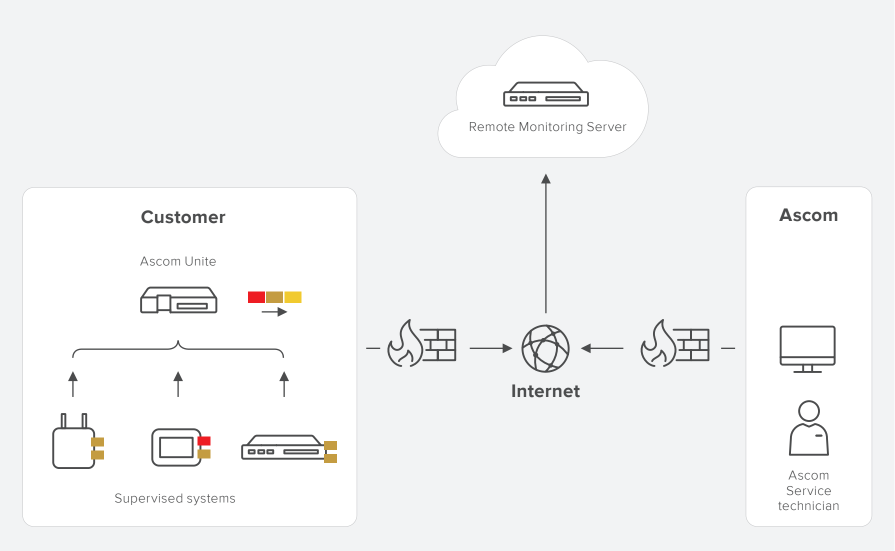
It is essential—and usually legally mandated—to quickly identify and remedy issues, while maintaining system uptime.

Systems maintenance requires expertise and experience. All Ascom Remote Monitoring technicians are specially trained and certified in this mission-critical area.

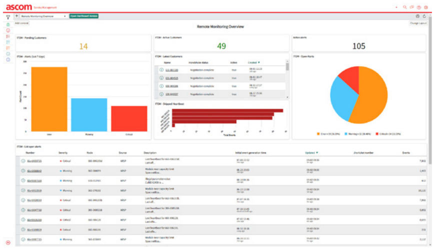
- Detects glitches before they become critical errors
- Helps maximize system uptime
- Frees resources that can be used for core operations

Secure data traffic

Outbound data is encrypted (https/443), and only technical logs are transferred—no confidential data. Access is rigorously controlled and restricted to authorized Ascom specialists.



Ascom equipment is monitored by a combination of Ascom Unite fault logs and supervision. For non-Ascom equipment, ICMP ping is used to verify equipment availability. We also use SNMP traps to collect notifications from a wide range of equipment. All irregularities are sent to Ascom to be handled in accordance with your Service Level Agreement.



How it works:

- Collects non-critical events that may indicate a risk of critical issues; helps with the early detection of potential critical errors
- Critical errors are immediately sent to the Ascom duty engineer, and handled as agreed upon in your Service Level Agreement.
- Helps to identify an error’s root cause, enabling easier corrective action
- Uses established remote connections to remotely intervene and pre-empt/ mititagate issues

Examples of equipment that can be monitored:

- Ascom IP-DECT (infrastructure components)
- Ascom Elise 3 modules (MMG, Cardio-max, Unite CM, Unite Connect)
- Ascom mobile devices (Ascom Myco 2, Ascom Myco 3, Ascom i63)
- Ascom teleCARE IP® and Telligence
- Non-Ascom equipment (SNMP-enabled products such as servers, routers, etc.)
- Ascom applications running as virtual appliance on a server

01679-03 ENX 2021.09 © Ascom (Sweden) AB