AirLink® Management Service Security: The Questions to Ask

When it comes to partnering with a cloud service provider for device management, one of the most important things to consider is the provider's approach to security. Your provider will be trusted with a vital part of your business, so it's essential to choose an organization that shares your concerns and makes security a top priority.

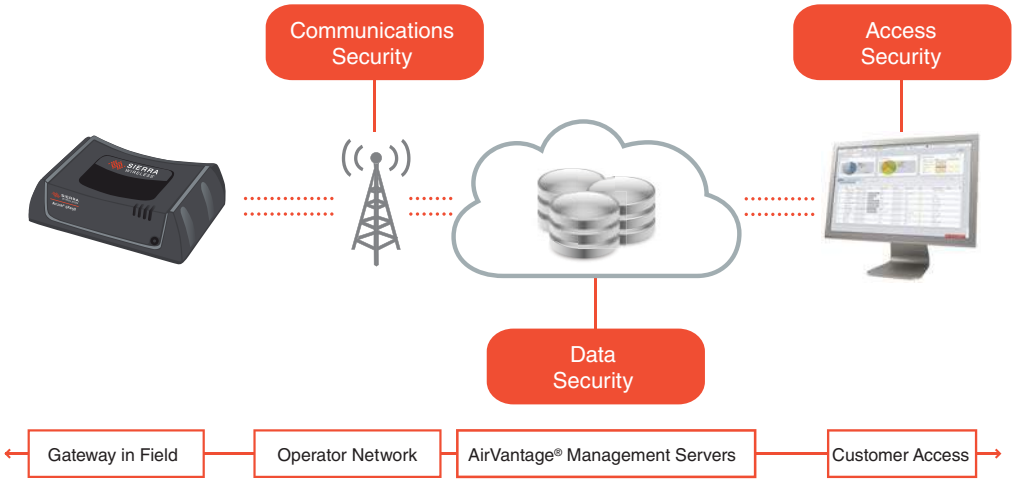
At Sierra Wireless, we are deeply committed to data security. As a leading provider of cloud-based device management, we know our company's future depends on keeping our client's data safe. We take the necessary precautions at every point in the process to maintain the integrity of our applications, our networks, and the data they carry, and we regularly invest in the security of our cloud infrastructure.

In our many years of providing AirLink® Management Service (ALMS), we have compiled a list of the questions our customers most frequently ask about security. These questions can be used to evaluate any cloud provider's offerings – and also serve to highlight the robustness of the ALMS offering.

CLOUD SECURITY: TOP AREAS OF CONCERN

Cloud services are used for a variety of purposes but, at their core, provide vital communications between an organization and its remote assets, branch offices, and remote workers, and support applications that leverage the infrastructure. Security should be a primary concern in any network architecture, but with a cloud-based service for device management, there are three aspects in particular to focus on: communications, data, and access.

Security Considerations



Communications security
This refers to the methods used to interact with devices. There needs to be a secure process for initiating communication with the network, receiving data from devices, and sending commands or updates from the cloud.

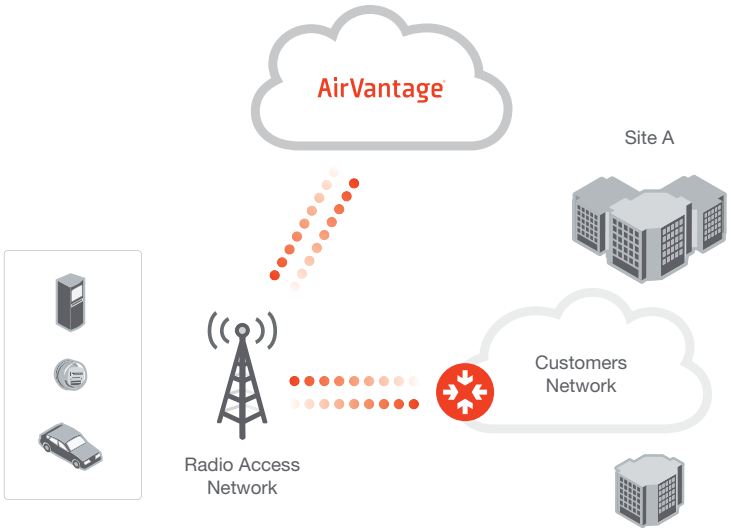
Data security
This is how data is stored, kept private, and protected from harm. Issues to review include redundancy, the hardness of the datacenter, and the measures taken to verify and test network security.

Access security
This includes who can access the service, what they can and can't do once they're logged in, and the features that help administrators analyze and control what's happening on the network.

COMMUNICATIONS SECURITY

Does my device data travel on the same network as user data?

No. Device data uses its own pathway to the radio access network. The flow of data for gateway management remains entirely separate from data on your network. Your traffic to the public internet (websites, emails), encrypted VPN communications over wireless, and internal applications are all isolated from ALMS and never flow through the ALMS servers. This approach of using a dedicated channel for managing network devices is known as "out-of-band" management, and is the preferred method for maintaining data integrity.

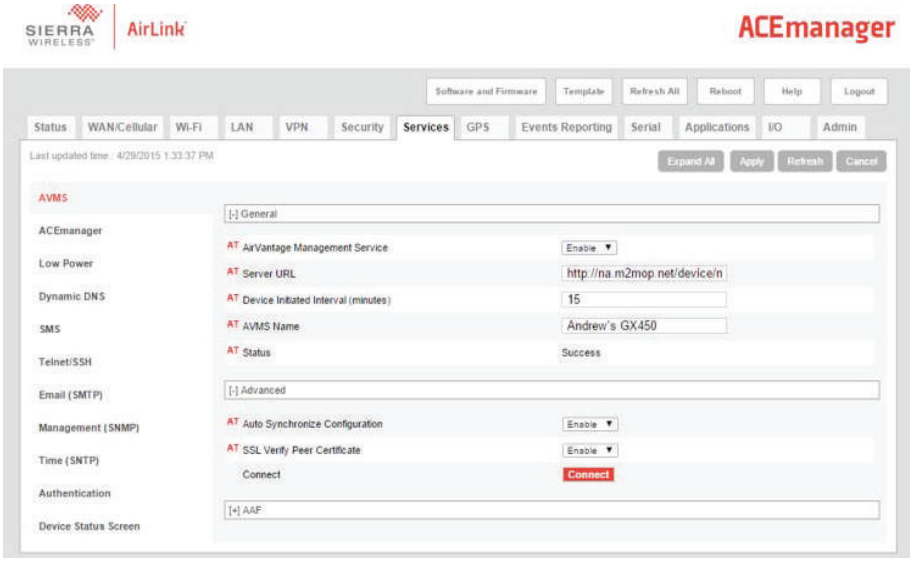


Management data is isolated from business data

Is device data encrypted?

Yes. Data flowing from an AirLink GS/LS/ES device to ALMS can be encrypted using HTTPS, the technique used by internet browsers and web servers to transmit sensitive information. (Note that data encryption is not supported on older devices, including AirLink Raven X/ST/XE, PPX, and MP.)

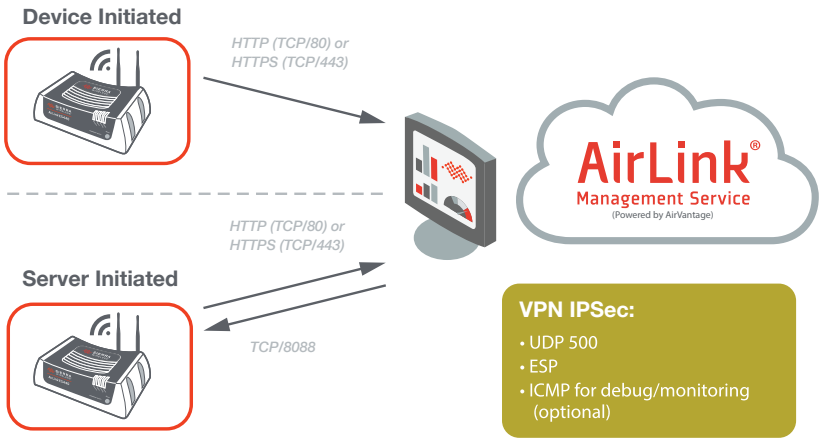
Within ALMS, administrators use AceManager, our browser-based configuration and management utility, to change the server URL to an HTTPS format, enable SSL for data encryption, and verify the SSL certificate.



AceManager interface for setting data encryption

How do devices communicate with the network?

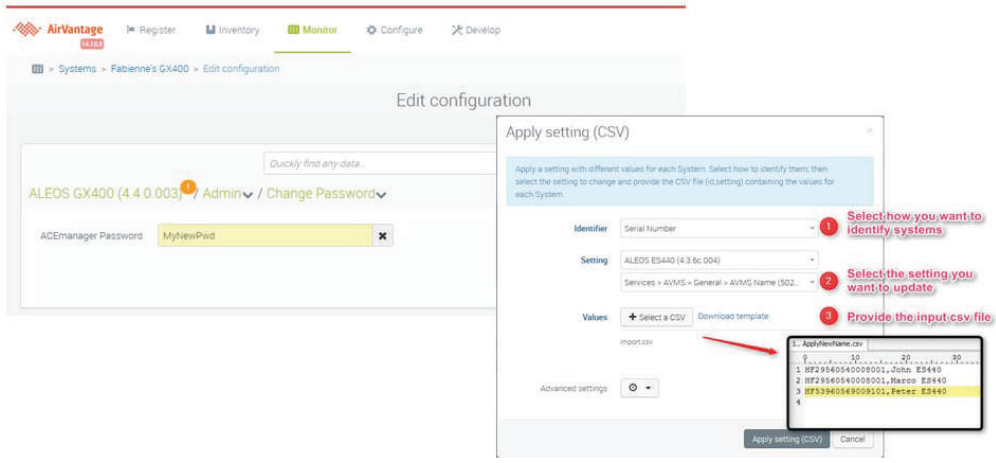
ALMS uses a technology similar to that used by large enterprise networking companies to manage their cloud operations. Device communications are initiated by the device, according to a configurable heartbeat policy. The device requests information from the management server, and the server responds with a list of queued tasks. This is a proven approach for maintaining data security, on either a public or a private network, because each device in the network can be managed remotely without being exposed to the network. The tasks associated with remote management are executed without opening your network, and the approach doesn't require the involvement of a static or public IP address, or even a dynamic DNS service. ALMS is fully compatible with private APN network architectures.



Information for Customer Firewall Configuration

Are unauthorized devices prevented from accessing the network?

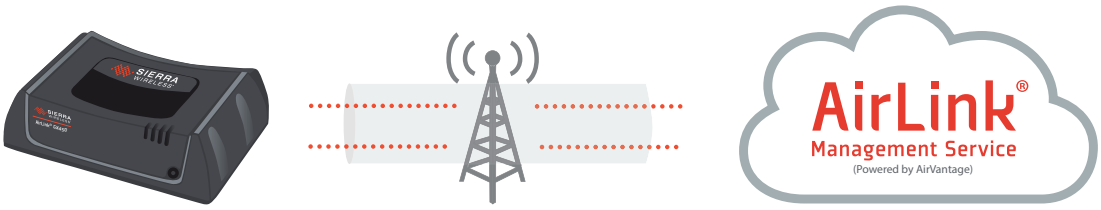
Yes. Each AirLink device has to register with ALMS before communications can take place. Registration is controlled using a unique identifier. Each identifier can only be registered once, and unauthorized devices cannot connect to ALMS. The integrity of device communications is confirmed using a checksum mechanism that prevents the data flow from being corrupted. With AirLink GX/LS/ES devices, data remains confidential, because all data entering and exiting the cloud can be encrypted. Device passwords can also be assigned or changed in bulk, for faster processing. (Note that encryption is not supported in older devices, including AirLink Raven X/XT/XE, PPX, and MP.) Settings with different values can be assigned to each system, and the password is write only, so it's not visible in the device configuration.



Configuring device authentication

I use a private operator network. Can I extend the network to include secure services for device management?

Yes. Sierra Wireless offers a special service, called AirVantage VPN Service, which encrypts management traffic to and from ALMS and delivers it using an IPsec tunnel.
This managed service is configured and monitored by AirVantage operations. The standard configuration uses an IPsec/PPTP-based VPN and is compatible with existing enterprise networking equipment. You retain complete control over how devices access the internet, and how the applications associated with each device operate.



AirVantage VPN Service uses an IPsec tunnel

Sierra Wireless
ALMS Security Q&A

DATA SECURITY

Who operates the service?

The service is operated and maintained by a dedicated team of Sierra Wireless employees. The health of ALMS is monitored constantly (24/7/365). As a customer of ALMS, you have continuous online access to network status (http://status.airvantage.net), and the site is supported by email alerts. Real-time network activity and overall system health are constantly monitored from our central network operations centers (NOCs). On AWS, the machines (VM) used for ALMS are dedicated to Sierra Wireless, and continuously monitored by Sierra Wireless team.

Where is my data stored?

ALMS is built on Amazon Web Services infrastructure. ALMS is deployed across 3 availability zones within the AWS region of Oregon in the United States of America. Each availability zone is designed as an independent failure zone. This means that availability zones are physically separated within the region and are located in lower risk areas. They are each fed via different grids from independent utilities to further reduce single points of failure. ALMS data are backup daily to reduce the risk of data loss, these backups are stored and stay in the United States of America.

Are the datacenters secure?

Yes. The AWS cloud infrastructure is housed in AWS's highly secure data centers, which utilize state-of-the art electronic surveillance and multi-factor access control systems. Data centers are staffed 24x7 by trained security guards, and access is authorized strictly on a least privileged basis. All personnel must be screened when leaving areas that contain customer data. Environmental systems in the data centers are designed to minimize the impact of disruptions to operations. And multiple geographic Availability Zones in one region allow ALMS to remain resilient in the face of most failure modes, including natural disasters or system failures.

How are the networks in these datacenters secured?

Availability zones are all redundantly connected to multiple tier-1 transit providers.

The AWS infrastructure is protected by extensive network and security monitoring systems. These systems provide important security measures, such as basic distributed denial of service (DDoS) protection and password brute-force detection on AWS accounts. In addition, AWS infrastructure components are continuously scanned and tested. While some organizations perform vulnerability scanning on their resources once a quarter or once a month, AWS scan multiple times a day.

On top of AWS infrastructure, dedicated firewalls and strict rules (IP and ports) are used to isolate each network layer. Any access to the web client is encrypted through HTTPS.

What certifications have these datacenters received?

AWS has achieved compliance with an extensive list of global security standards, including ISO 27001, SOC, the PCI Data Security Standard, the Australian Signals Directorate (ASD) Information Security Manual, and the Singapore Multi-Tier Cloud Security Standard (MTCS SS 584). AWS has been granted by two separate FedRAMP Agency ATOs: one for the AWS GovCloud (US) Region, and the other covering the AWS US East/West regions. AWS is also one of the only public cloud service providers to have been granted a provisional authorization for DoD CSM Levels 1-5.

Do these datacenters have policies and procedures in place for disaster response?

Yes. multiple geographic Availability Zones (3) in the United States allow ALMS to remain resilient in the face of most failure modes, including natural disasters or system failures.

Sierra Wireless team has recovery procedures that ensure downtimes of less than 24 hours. Daily backups of all data reduce the impact of any downtime or lost data.

Is this a multi-tenant service?

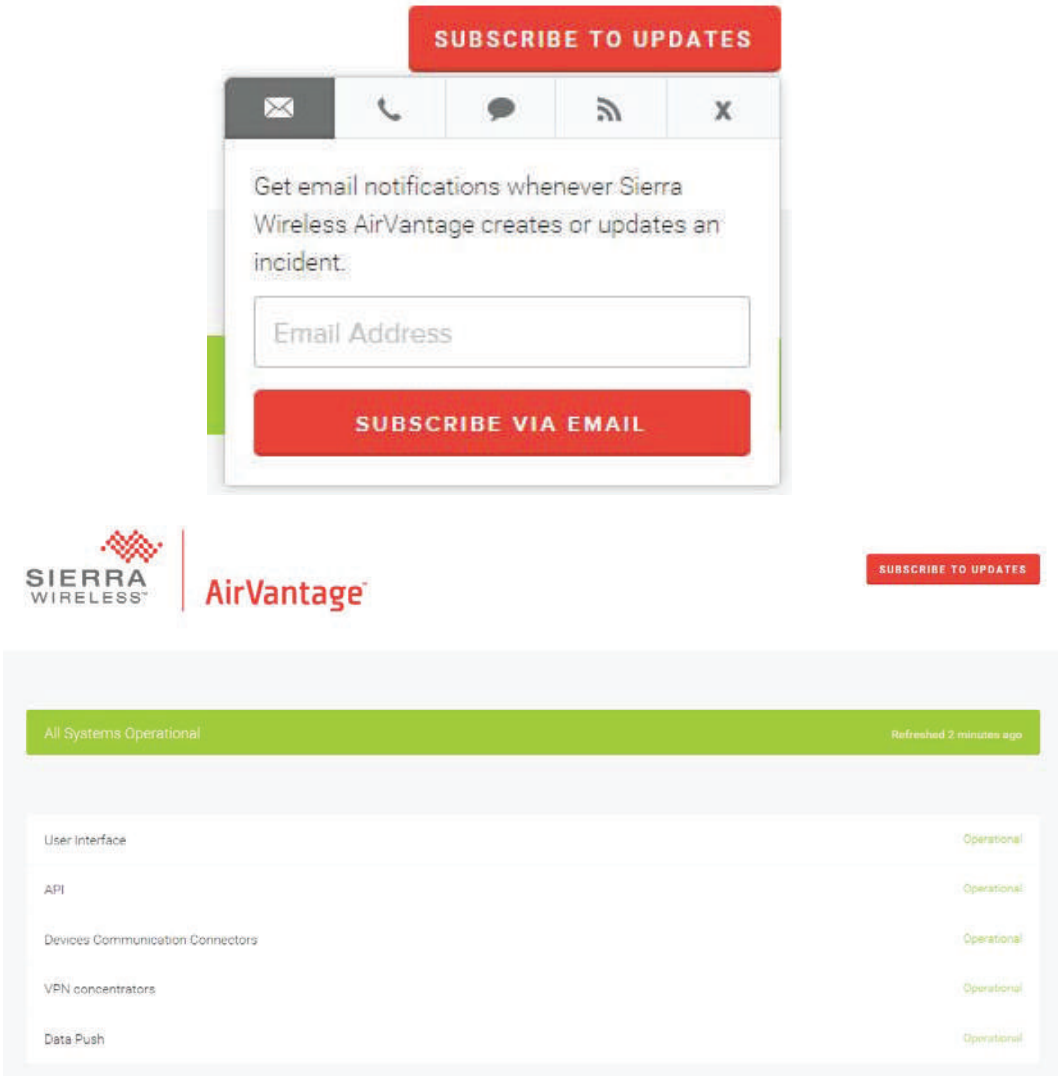
Yes. The ALMS software architecture is a multi-tenant environment, so a single instance serves multiple customers or tenants. All data is stored in a single database, but the storage code has been designed to ensure full isolation of tenant data. The system has successfully passed third-party security audit tests that confirm this.

What is the Service Level Agreement (SLA) for this service?

ALMS is backed by a 99.9% uptime SLA.

What is the procedure when something unexpected happens?

Administrators can configure alerts so they are notified immediately if an issue needs attention.

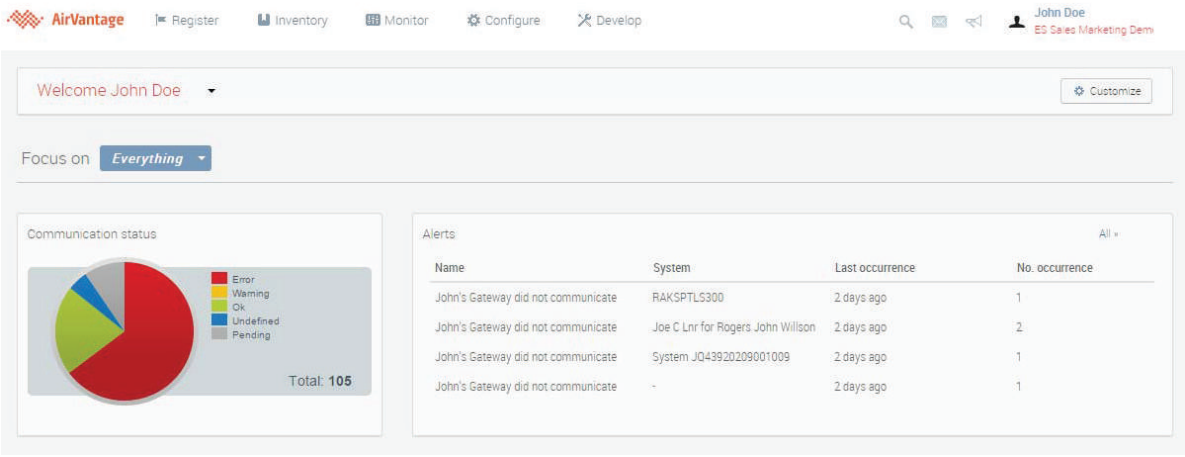


Signup page to receive alerts on AirVantage operational issues

What happens if a gateway loses connectivity?

Alerts can be configured so administrators are notified immediately if connectivity is lost or a gateway doesn't communicate as expected. The administrator can then log in to view communications failures in a report, complete with status updates, time of last occurrence, and a total number of occurrences since inception. Having online access to this kind of detailed, real-time information gives your IT team an instant understanding of what's happening, and reduces resolution time. The system also enables troubleshooting at remote locations, so administrators can manage distant locations without leaving the central office.

It's important to note that while gateway connectivity can temporarily be lost, the fact that data communications are isolated from other communications means that temporary failures in gateway connectivity are very unlikely to impact the rest of the organization, including the corporate website or email.



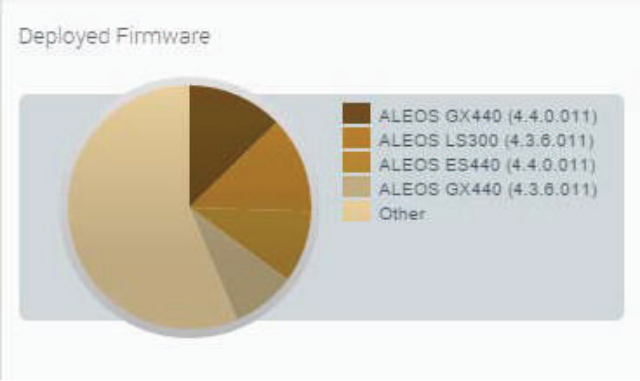
Alerts and reports on gateway communication status

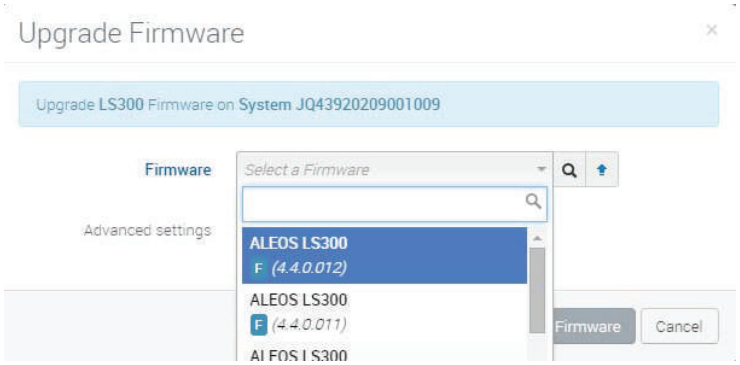
How can I tell what's happening on my network?

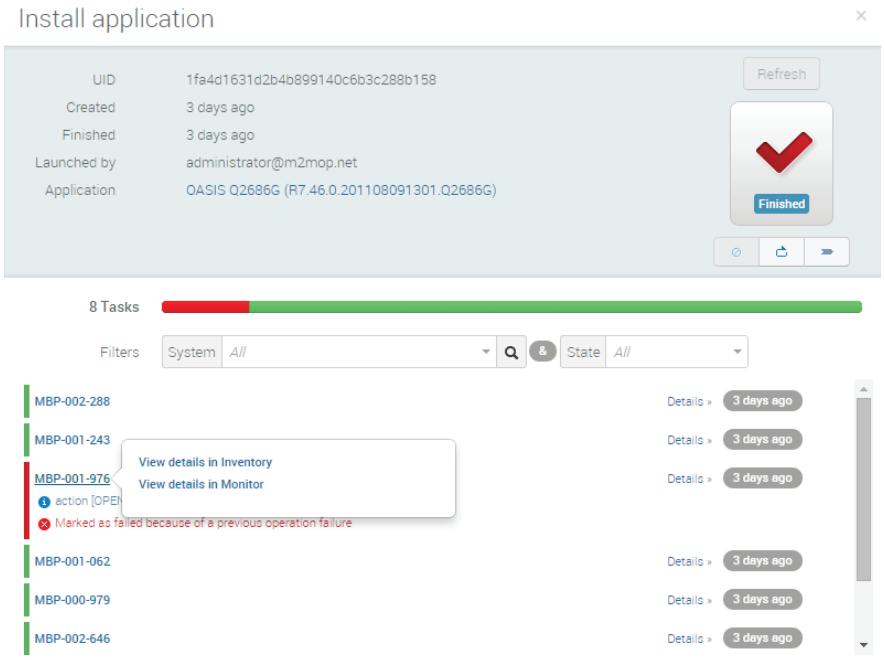
ALMS uses a cloud-based architecture that is designed to capture key operating parameters from AirLink gateways and report these to IT managers and administrators. The benefits are centralized visibility and control. Your IT department has a complete view of remote communications equipment – operating statistics, physical location, and other valuable information. Being able to "see" the communications infrastructure remotely means your administrators don't have to be onsite to address communications issues. You can check the health of the site any time by logging on to http://status.airvantage.net. You can also be alerted by email if there is an outage or if maintenance is required.

How are firmware updates managed?

Firmware updates are received automatically and can be deployed, over the air, with a single click. The ALMS interface includes a dashboard that provides an at-a-glance overview of which versions are running on each gateway in the field. ALMS can be used to view and track each firmware deployment, to verify that each gateway is using the right version.







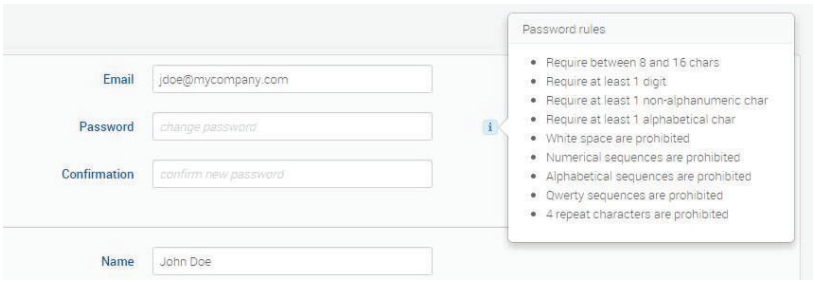
Report on firmware versions and upgrade entire fleet

ACCESS SECURITY

What authentication methods do you use to ensure that only authorized people have access to my network?

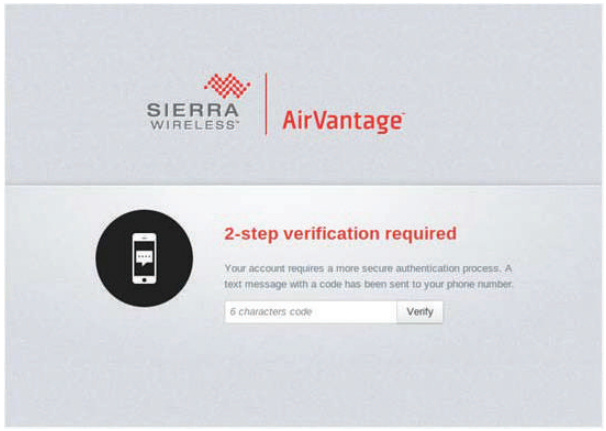
ALMS offers a number of authentication features that ensure users are who they say they are, and that they access applications, view data, or perform functions based on clearly defined roles. These features help maximize the security of your deployment.

- Strong password policy – Strict rules ensure users choose passwords that are highly secure.



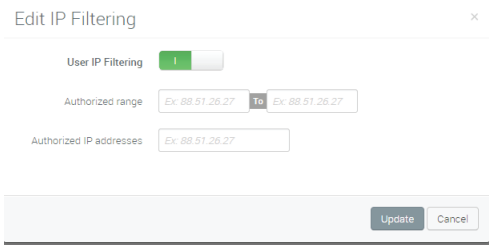
Strict rules for passwords increase logon security

- Optional two-factor authentication – With applications that benefit from added security, a text message with a one-time passcode can be sent to the user's phone each time they request a login. The user enters the temporary 6-character code to verify authentication. This process uses SMS messaging, which is both cost-effective and convenient.



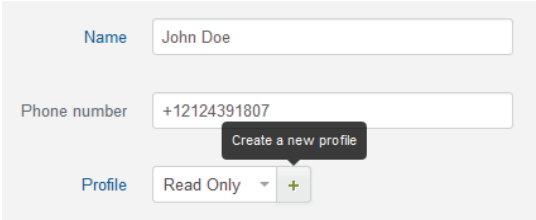
Temporary access code adds another level of login security

- Restrict logins by IP address – By using IP filtering to accept only those logins that come from a specific IP address or a range of addresses, administrators can verify access based on geographical location.



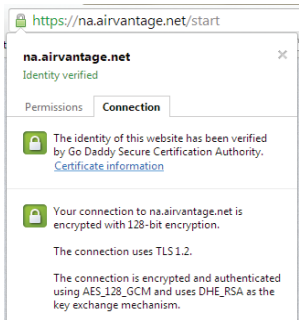
Logins can be restricted by IP address

- Role-based administration – This feature lets you use profiles to limit what users can do when they log in, so they only have access to the functions and data relevant to their work. A role is assigned to each account, and only administrators can create new users. Users can be assigned to a specific group of tasks, and can be provided with read-only access to reports. The system can also manage guest access and restrict the use of diagnostic tools. All these steps can help minimize the chances of accidental data loss or malicious acts. They also help restrict any problems or errors to isolated parts of the network.



User profiles increase security while protecting data

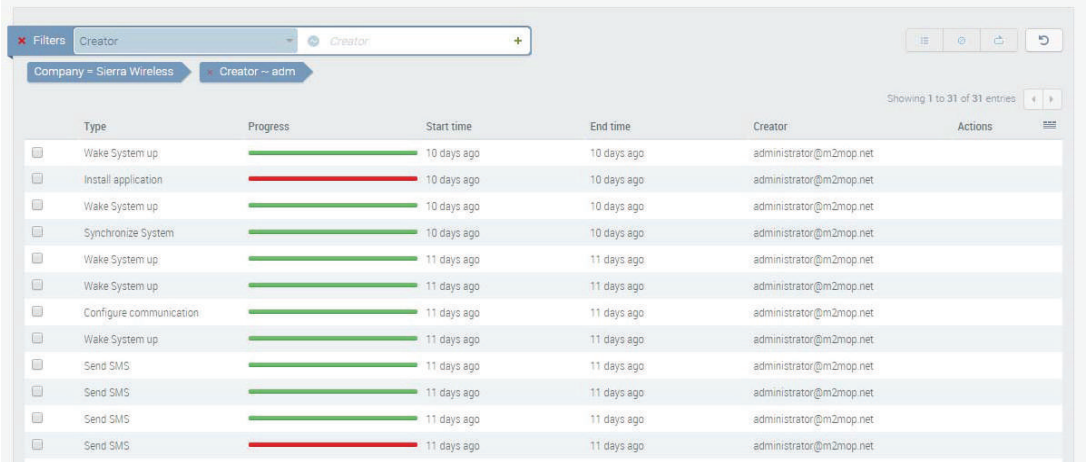
- HTTPS access – Access can be configured so that the user interface can only be reached via HTTPS, to ensure confidentiality of all administrator configurations performed with AirVantage. Any information read or changed remains confidential.



Protected AirVantage access via HTTPS

Can I monitor user activity?

Yes. User sessions are recorded and available for review. The ALMS audit log captures all operations associated with a user, tracking the time of access and the duration of each activity.



User activity logs provide traceability

CONCLUSION

Like other device-management services, ALMS operates in the cloud. The service involves the use of sensitive client data, so it's important to consider all the security features of the service and discuss them with the Sierra Wireless sales team.

The questions in this document reflect top-of-mind concerns about security and can be used to evaluate any provider of device-management services. As the answers to these questions show, Sierra Wireless understands that security is one of the most important aspects of a cloud-based service. ALMS is built for security and effectively protects communications, access, and data. To learn more, please visit www.sierrawireless.com/ALMS

About Sierra Wireless

Sierra Wireless is building the Internet of Things with intelligent wireless solutions that enable organizations to innovate in the connected world. We offer the industry's most comprehensive portfolio of 2G, 3G and 4G embedded modules and gateways, seamlessly integrated with our secure cloud and connectivity services. OEMs and enterprises worldwide trust our innovative solutions to get their connected products and services to market faster. Sierra Wireless has more than 900 employees globally and operates R&D centers in North America, Europe and Asia.

For further company and product information, please visit www.sierrawireless.com.

SIERRA WIRELESS® | AirLink®