REACH SYSTEMS

The Reach Access Control System

The Reach Access Control System (ACS) is a keyless entry solution that is delivered as a web-hosted service. The system connects intelligent IP Controllers (Panels), via the open Internet to deliver a low cost, secure, enterprise class access control system, ideally suited to meet the needs of organizations with geographically dispersed locations.

The Reach ACS provides a convenient and cost-effective solution for organizations that want the benefits of comprehensive multi-site access control, without the up-front investment in computer hardware and software, or the ongoing cost for their IT staff to maintain it. With the Reach ACS, organizations can take control of access to their facilities, making them more secure, while reducing IT costs.

Key Features

Convenient, Web-based interface that allows remote management

Reach ACS utilizes standard Internet communications protocols, and can be deployed using the facility's existing Wi-Fi or Ethernet infrastructure. User enrollment and system administration are performed through a browser-based interface to ReachNet™ via the Internet. Users have the ability to customize and remotely monitor access to their facility, remotely unlock doors, receive custom reports and notifications of when their facility is being accessed, or perform any other system function through the web browser interface.

Hosted and Highly Secure

ReachNet is hosted at a high-security data center. Located in guarded server rooms, Reach Systems guarantees the highest level of physical and data security for customers' access control system data. The facility is environmentally controlled and closely monitored with closed-circuit video and alarm monitoring, and redundant power feeds to ensure continuous operation during power failures. The facility also uses state-of-the-art fire suppression and laser smoke detection systems.

Scalable

ReachNet is built on an Oracle database that is massively scalable. At the smallest scale, ReachNet can be deployed to manage an access control system comprised of a single door at a single location. From there, you can grow to hundreds of locations and thousands of doors yet the Reach ACS remains cost effective because it does not require any on-site servers or software.

Easy to Install, Cost-Effective to Maintain

Since ReachNet is hosted remotely, there is no up front investment in computer hardware and software. Because of this architecture, you'll never need your IT department to reconfigure a server, back up your access control database, or upgrade an operating system. This hosted model provides a cost-effective solution for organizations that want the benefits of comprehensive access control management software without the overhead costs of a traditional ACS solution. A primary benefit of a remote hosted solution is all users can access the full functionality of the ACS software application including continual upgrades with no annual software maintenance charges.

Robust with High Availability

Reach ACS is designed for fault-tolerant operation. Even if the network fails, each access point continues to operate and all access events are recorded by the Reach IP Controller's local database and uploaded to the ReachNet server once network communications have been reestablished, preserving the integrity of all audits.

Reach maintains multiple, redundant servers in order to guarantee that customers' critical access control system capabilities are always accessible. Automated daily backups of system data guarantee the integrity and availability of all system data through almost any interruption or failure. Reach guarantees 99.9% uptime.

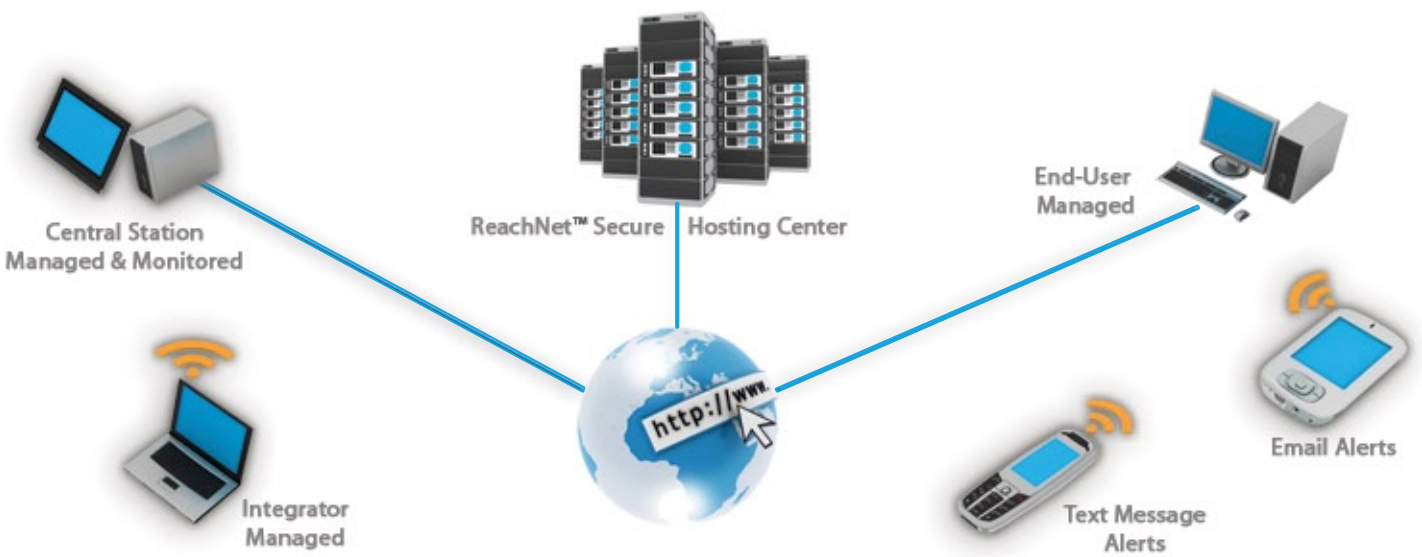
Secure Communications

While on a LAN connected to the internet, the Reach IP Controller only requires outbound Internet Access. Data and communications security is critical to maintaining the integrity of the Reach ACS. All communications to and from the ReachNet server are protected by 256-bit AES encryption, and through the use of the Secure Sockets Layer (SSL) protocol. SSL provides endpoint authentication and communications privacy over the Internet using cryptography, allowing client/server applications like ReachNet to communicate in a way that prevents eavesdropping, tampering, and message forgery.

Real-Time Operations

When an access credential is presented at the door, the IP Controller makes the decision locally, in real time, whether to let the user into the facility. Each event at an access point triggers a communication to the ReachNet server to report the event. In this way, administrators can monitor all facilities in real-time, gaining situational awareness of user activity throughout the organization.

System Architecture



ReachNet™ Features

ReachNet is the system management application through which users manage the Reach ACS. ReachNet resides in a secure data center and communicates with IP Controllers over the Internet. It is comprised of a database, a software module that communicates with the IP Controllers, and web applications that implement the browser interface to the ReachNet database. For reliability, ReachNet is built on an enterprise class Oracle database and utilizes open source software and operating systems wherever possible. ReachNet is designed to be highly scalable and because there is no on-site software to install, it can be deployed cost effectively for a single door access system or for an enterprise-wide system that spans the globe.

All user interaction with ReachNet takes place through a standard web browser, so users may log into the system over the Internet from anywhere in the world and perform any function for which they are authorized.

Tracking & Monitoring from a Central Station

ReachNet communicates real-time access exceptions to popular central station automation programs so that monitored access can be offered alongside traditional alarm and video monitoring. The central station operator gains full situational awareness of alerts/exceptions and reduces the number of false alarms caused by user error.

Notifications

Any event, created by a user at a door, an administrator on ReachNet or a system/network interruption can trigger a notification. Notifications can be customized for each user application and can be sent via email or text message.

Reporting

All system data and access events are recorded and stored in the ReachNet database and can be accessed to generate an endless variety of reports. The system includes a set of default queries to create common reports like event logs for access points, employee access logs, summary of employee permissions and others. In addition, users can create custom reports configuring simple “who”, “what”, “where” and “when” search filters to create instant, professional reports. Reports can be printed or downloaded as an Excel spreadsheet. The reporting feature is extremely powerful and able to generate an overview report of all activity at a facility, or drill down to show the access activity of one employee or one access point within a specific date and time range.

Managed Access Control

The master administrator can grant privileges for each administrator (or group of administrators) that control access to specific portions of the ReachNet software platform corresponding to their job function. For example, the department responsible for data entry could be granted access to only the software screens which pertain to adding users and modifying their access permissions. ReachNet is organized into separate "Views" for central stations, integrators and end-users.

All views provide the means to:

- Create, edit and manage administrators within the view.
- Define administrator privileges and access to the functionality in the respective view
- Monitor administrator activity
- Generate reports on administrator activity
- Set up notifications based on administrator activity

Currently implemented Views include:

End User View

The end-user view is for the owner and user of the access control system. end-user view provides the means to:

- Create, edit and manage the physical components of the access control system
- Create, edit and manage users of the access control system
- Provide access permissions to users
- Create schedules for permissions, reports and notifications
- Organize users, doors, buildings and permissions
- Create, edit and manage user credentials including access cards
- Configure IP controller peripherals
- Monitor IP controller and its peripherals' activity
- Generate reports on IP controller and its peripherals' activity
- Set up notifications based on IP controller and its peripherals' activity
- Set up event/alarm notifications to a CSM provider
- Remotely control IP controllers and their peripherals

Integrator View

The Integrator view is for the security professional that installs the system and provides ongoing support for the end user. This view provides Integrators a portal through which they can easily provision IP Controllers, design and setup systems and provide ongoing support to all of their end-users.
Integrator view provides the means to:

- Create, edit and manage end-user accounts
- Manage and configure IP Controllers
- Monitor end-user system activity
- Generate reports on end-user system activity
- Set up notifications based on end-user system activity

Central Station View

The Central Station view is for the Central Station service provider that monitors alarms from end-users and may provide support to end-users as subcontracted by an Integrator. This view provides the central station, a portal through which they can easily provide ongoing support to end-users and Integrators. ReachNet allows users to customize their access control system and designate any access event as an exception that will be relayed to a central station monitoring facility.

For more information:
Call: 510.452.9532 | Fax: 510.452.9292 | Email: sales@reachsystems.com
1330 Broadway, Suite 1201, Oakland, CA 94612
Visit us online at: www.reachsystems.com