Lightcloud Security
& Vulnerability Management

Security Overview

Lightcloud®

R C® LIGHTING

Lightcloud Takes Security Seriously

We take our users' security and privacy concerns seriously and strive to be transparent about our security infrastructure and practices. We secure our devices and data at every level of communication, from the site to the cloud, with 5 layers of security.

c UL® UL2900-01 LISTED

THE FIRST NETWORKED LIGHTING CONTROL SYSTEM LISTED FOR CYBER SECURITY!

5 Layers of Security

Isolation

All Lightcloud data communication is isolated from other networks. Lightcloud isn't affected by compromises to computer networks or dependent on utilizing existing IT infrastructure. Only Lightcloud devices are supported by the Lightcloud network — isolating it from interference and manipulation.

Encryption

Lightcloud uses end-to-end encryption (E2EE) — data transmission is always encrypted. If data were to be accessed, it wouldn't be readable. That encryption remains whether it's between devices, cellular, or accessed via the web. Your data is always secure.

Restriction

Access is restricted by site, passwords, two-factor authentication, and user-level permissions. Every network uses its own keys, so a compromise would be isolated to a single location. Password best practices and two-factor authentication ensure individual users' passwords are secure and used only by the intended user. User-level permissions ensure users only have access to the controls they need.

Prevention

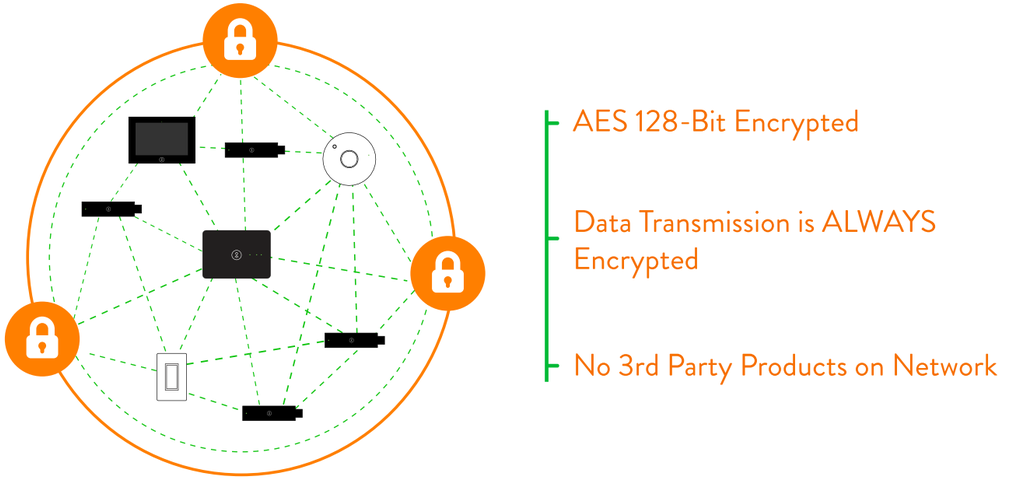
Lightcloud updates go through a rigorous evaluation period in an isolated environment before being released to devices. Evaluations include internal and external audits and penetration tests. This keeps Lightcloud security constantly ahead of any would-be intruders.

Verification

Working with external agencies to evaluate our security validates our efforts to be the most secure lighting controls system available. Our internal security team is constantly improving our system to exceed security guidelines, keeping us several steps ahead.

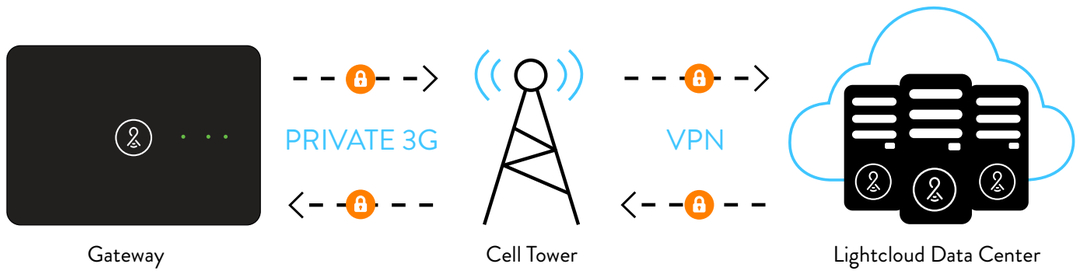
Call Us Anytime: 1 (844) - LIGHTCLOUD

On-Site Security: Device Communication



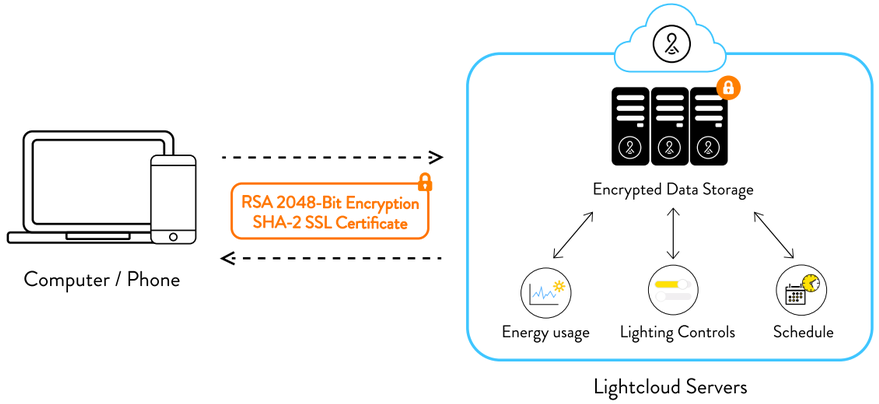
Lightcloud is a networked lighting control system with Devices communicating over a secure wireless mesh network. At the 802.15.4 wireless level, we provide an encrypted and secure joining process that includes unique network keys for every installation and AES 128-bit encrypted network communications. At no time does any data travel unencrypted. Additionally, only products manufactured by RC can communicate over the Lightcloud network.

3G Uplink: Private Cellular to Cloud



The Gateway communicates to the cloud-based services via dedicated, private 128-bit and 256-bit encrypted 3G cellular connections. Our secure connection operates completely independently from your IT infrastructure. The Gateway provides the communications between the 802.15.4 network and the 3G wireless network. In addition to standard 3G encryption, all data over the cell network travels on a private allocation of cellular addressing over an encrypted VPN (virtual private network) between the Gateways and our private data center.

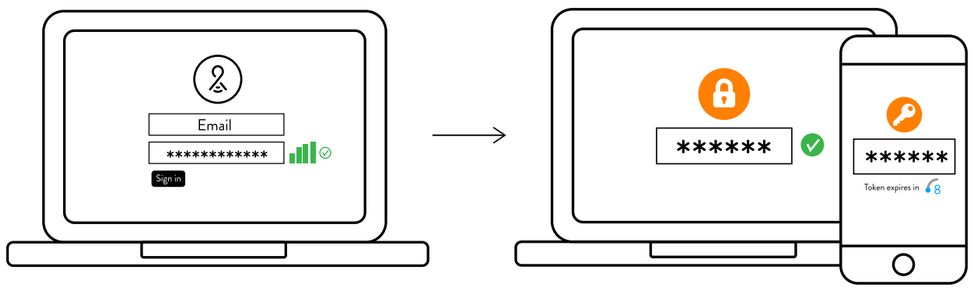
Cloud Infrastructure: Communication and Storage



We communicate entirely via SSL TLS — including client communications with servers that interface with our backend servers, which protects communications by using both server authentication and data encryption. Our application endpoints use industry-leading RSA 2048-bit encryption and have DigiCert SHA-2 SSL Certificates. Our servers employ a robust physical security program with multiple certifications. The cloud storage method also guarantees information won't be lost, by creating redundancies on servers around the world.

If a Lightcloud Network were compromised, no sensitive user data would be accessible. User data on Lightcloud is limited to email addresses and lighting controls, so sensitive information is safe.

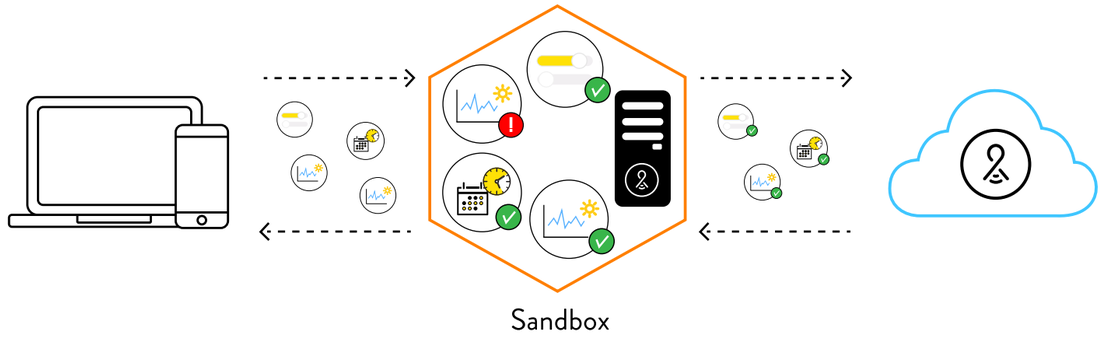
Access & Control: User-Level Security



Strong Passwords — Two-Factor Authentication

Industry-standard password management protocols are employed, including requirements for length and strength. Strong passwords are important and can be layered with two-factor authentication (2FA) for extra protection. This extra layer of protection can be especially important for administrative users such as systems management and support. Finally, user restrictions ensure access is granted for specific controls for each user. Whenever phones and computers are used to control Lightcloud, each adjustment is logged by user, so if a user's account is ever compromised, that user can immediately be removed or their password changed.

Testing & Vulnerability Management: Monitoring & Development



System functionality and design changes are verified in an isolated test "sandbox" environment and subjected to functional and security testing prior to deployment to active production systems. By testing in an isolated environment without live site data, we ensure no data can be compromised while testing. Once security and functionality is verified, changes are rolled out in stages.

Security Audits

Security is an ever-moving target, so we use both internal and 3rd parties to perform quarterly penetration tests and security audits to verify that we are meeting the strict guidelines we have established. Security audits look at the system's hardware/devices, network/server, and the user interfaces/software. Even with physical access to our hardware, none of our security partners have been able to compromise our system at any level. Our security partners are security experts trusted by Fortune 500 Global Companies including GE, Intel, Microsoft, and Samsung.

Verification: 3rd-Party Certification

We've designed a very secure ecosystem with layered protection, and two independent agencies — SSL Labs and UL — recognize our security superiority.

THE FIRST c UL UL2900-01 LISTED NETWORKED LIGHTING CONTROL SYSTEM!

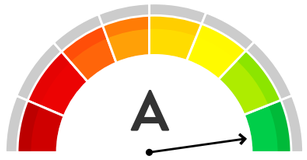
UL created the 2900-01 standard of software cybersecurity for network-connectible products and was published as an ANSI (American National Standards Institute) standard. UL evaluated and tested our devices for vulnerabilities, software weaknesses and malware, including risk management and controls in the architecture and design of the product.

UL tests performed:

- Scanned for malware on the binaries
- Scanned for vulnerabilities from the NIST National Vulnerability Database (NVD)
- Scanned for weaknesses in the source code and binaries
- Subjected to malformed traffic data
- Evaluated security protocols for access control and authentication, remote connections, software integrity, cryptography, security logs, and decommissioning
- Ran penetration tests to circumvent controls and security, engage the product in denial of service, access and authentic on the product via unauthorized means, attempt to exploit vulnerabilities acceptable in the risk analysis, elevated privilege on the product, man in the middle attacks

After careful evaluation, UL found our Devices and software exceeded or met all of their requirements, and listed our system as the first UL 2900-01 listed networked lighting control system.

SSL Labs verified and approved our SHA-2 SSL Certificate, inspected our encrypted network communication protocol based on protocol, key exchange, and cipher strength, and determined our security to be of the highest rating. We strive to adopt the latest most secure security protocols and procedures to keep customer data and sites safe.



Applications: Trusted Everywhere

Lightcloud is trusted by airports, civic centers, hospitals, hotels, manufacturers, municipal buildings, retailers, sheriff's offices, stadiums, and many other security-sensitive applications. Lightcloud is securely controlling lights all over the country and is ready for your application.

For more information on how Lightcloud can fit into your site, give us a call at **1 (844) - LIGHTCLOUD**

Glossary

AES 128-Bit Encryption

AES is a security standard adopted worldwide and by the US Government. AES is also approved as a cipher for top-secret information at the NSA (National Security Agency). For 128-bit encryption, data is placed in an array, then there are 10 rounds of processing information (substitute, transpose, and mixing of text). 128-Bit encryption has a block and key length of 128 bits.

Virtual Private Network (VPN)

A VPN is a secure, encrypted tunnel that is only accessible by authorized users. VPNs allow information to be safely transmitted over otherwise insecure networks by encrypting the data. If a network is penetrated, the data can't be read and is displayed as meaningless text.

SSL TLS

Secure Sockets Layer and Transport Layer Security are cryptographic protocols for secure, private communication over a network from the server to the browser. The symmetric encryption keys are created for each communication and are unique to each connection. The connection can't be interrupted by an attacker in the middle of the connection or viewed by eavesdroppers. The identities of both the server and the user via the access point is known to the connection. Each message sent has an integrity check to ensure data is transmitted securely and properly.

2-Factor Authentication (2FA)

2FA is an extra layer of security for your Lightcloud login that ensures that you're the only person who can access your account, even if someone knows your password. Each time you log in on a new device, a unique code will be texted to you. This unique code is required along with your password to log in to your user account. 2FA is generally reserved for account administrators or highly security-sensitive locations.

User Restrictions

User restrictions limit access to specific lighting controls and management. System administrators can be given complete control over the system. Other users can be given access to all of the scenes and zones or user-specific controls. By restricting access to only the lights users need to access, it's simpler for the users and more secure.

Sandbox

An isolated testing environment that has no connection to a "live" system is a sandbox. If a sandboxed environment is compromised, it has no effect on the system and no user data can be compromised. By testing in a sandbox, vulnerability and stability can be verified before releasing to customers.

Penetration Audits

Lightcloud Devices, networks, and user interfaces are tested internally and by 3rd-party security experts to look for potential security oversights.

Private 3G

A private allocation of AT&T and Verizon third-generation networks dedicated to Lightcloud. Data is encrypted and transmitted via a VPN to the highly secure Lightcloud Cloud.

Interested?

lightcloud.ca

1 (844) LIGHTCLOUD