Simple

Scalable

Daintree® Networked

Cybersecurity Overview

Flexible

Current

Overview

Daintree Networked is a Lighting Control system designed for commercial, industrial, retail and attached parking applications. It enables remote monitoring, control, and asset management of a single site or portfolio of buildings through the web-enabled Daintree Controls Software ("DCS") application. This document describes the controls and practices employed to protect the cybersecurity of Daintree Networked lighting controllers and sensors ("devices"), gateways (Wireless Area Controllers or "WACs"), and the Daintree Controls Software application.

Document Scope

This document applies only to systems hosted by Current and in-premise WACs and devices that are deployed using recommended configurations.

General Approach

Current employs a wide range of security controls to protect the DCS application, data, and the managed WACs and Devices. Current employs a "defense in depth" approach wherein multiple levels of security are used such that a breach of any one security control does not compromise the entire system. In addition, Current employs a "secure software development lifecycle" approach wherein design-for-security is considered throughout the entire software development process and not only once the software is deployed to the hosted environment.

Revision

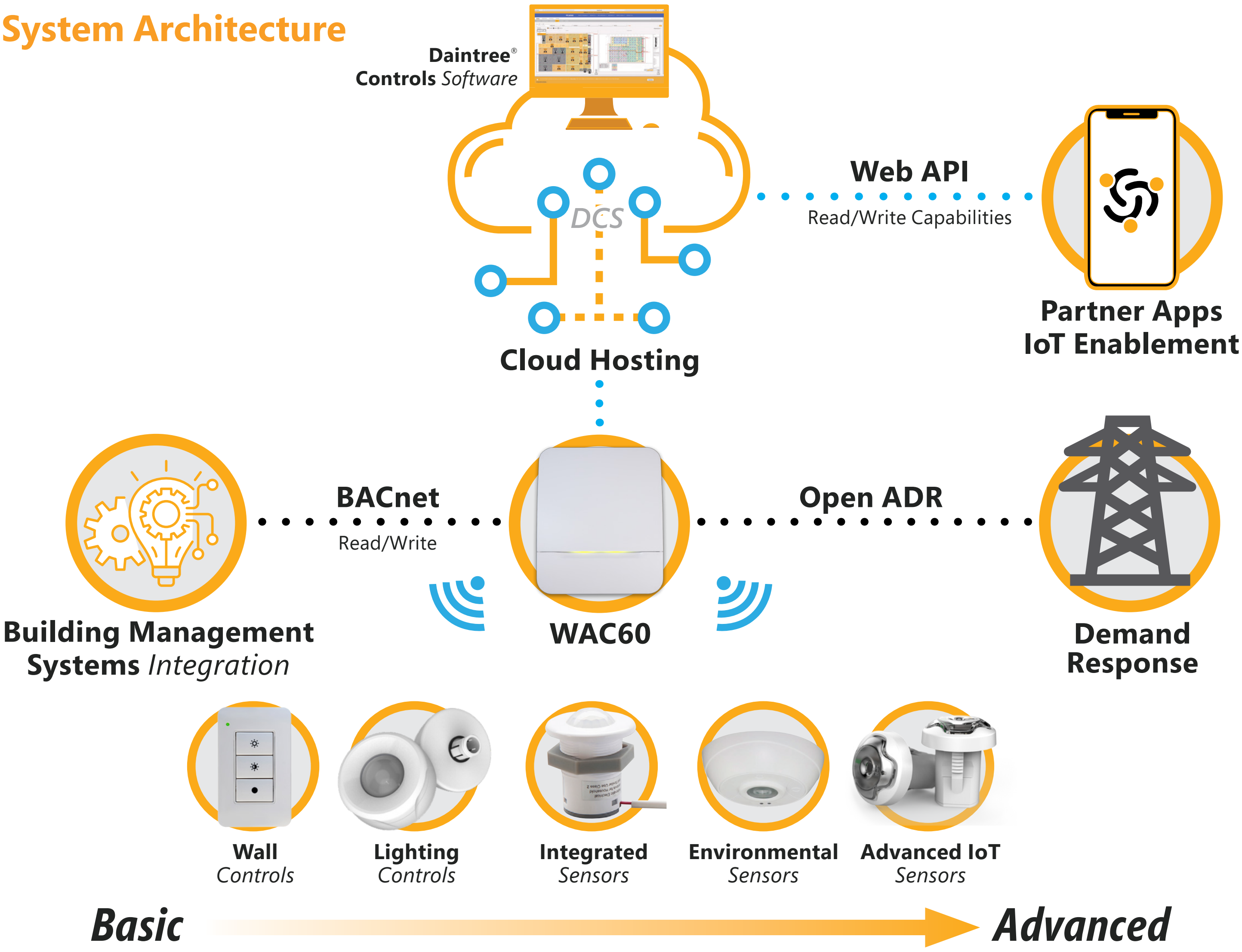
This document was last updated and published on 02/01/24.

Contents

The information contained in this document is Confidential and is shared under the terms of the Daintree End User License Agreement (EULA). This document is not for further distribution.

Daintree® Networked - CYBERSECURITY OVERVIEW

System Architecture



Security Controls – Wireless Area Controller

WAC-to-Cloud Communication

In the Daintree Networked solution, the WAC is the only device on-site that has connectivity to the Internet. All other devices on-site (wireless lighting controllers, sensors, etc.) communicate with the ZigBee protocol, and cannot be accessed from the Internet. Internet connectivity can be provided via the corporate network or a cellular modem.

The WAC uses best practices for TCP/UDP port management. Specifically, the WAC only requires the following outbound TCP/UDP ports:

WAC	Ports
443	Secure WebSocket & HTTPS connections
53	DNS queries (if no local DNS server)
123	Network Time Protocol (if no local NTP server)

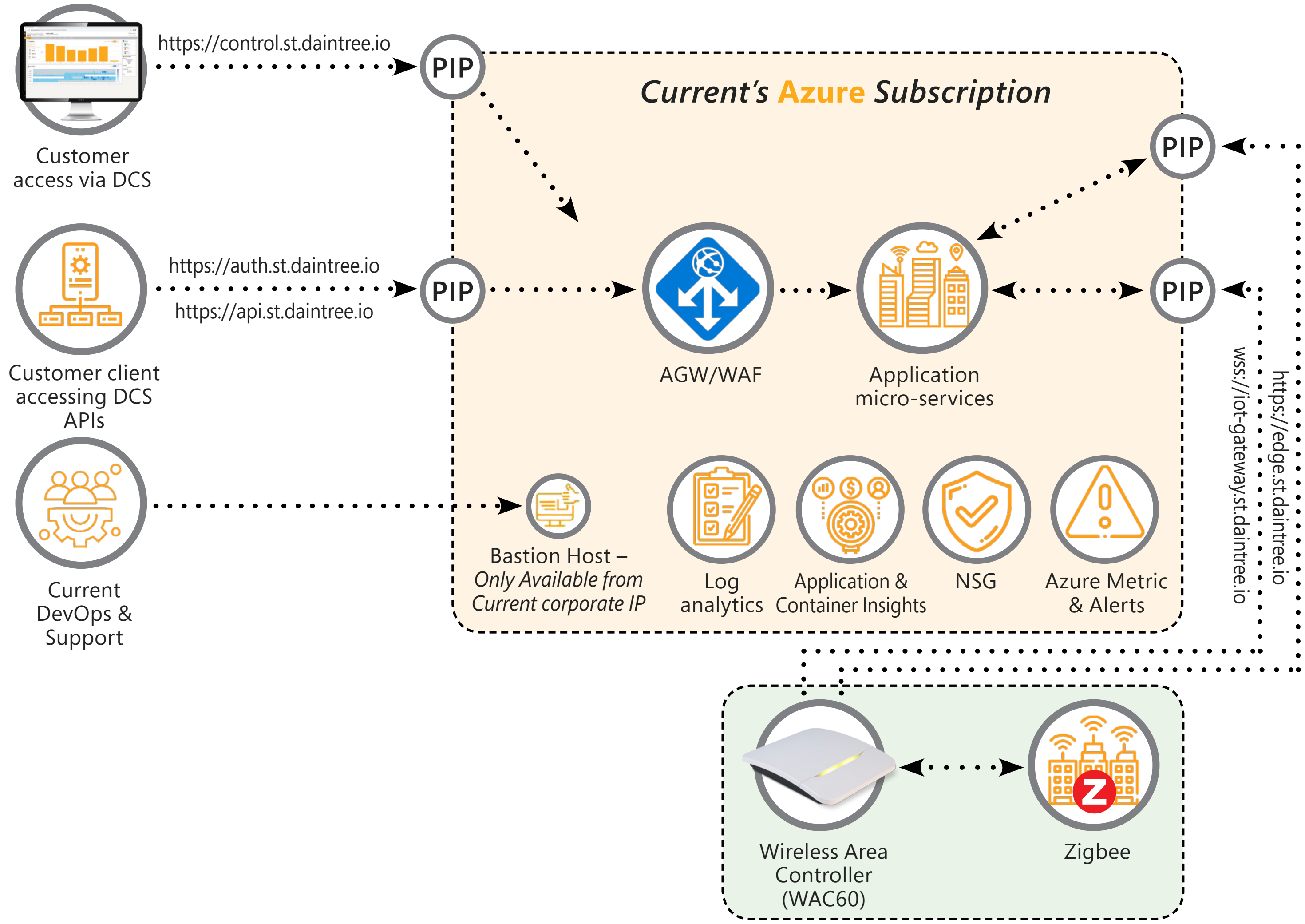
It is advised to not lock the WAC outbound access at the corporate firewall to a specific IP address as in some circumstances the IP addresses used may change and as this could break connectivity. The WAC will communicate with the following hosts:

Hosts	
edge.st.daintree.io	WAC enrolment, firmware upgrade and diagnostics
iot-gateway.st.daintree.io	Time-series data, configuration and control
time.google.com time1.google.com time2.google.com time3.google.com time4.google.com	Google's NTP time servers are used if DHCP does not provide NTP server address.

After physical installation and initial setup, the WAC and cloud software establish trust with X.509 certificate-based mutual TLS 1.2 authentication. Authentication occurs from client to server, as well as server to client. Thereafter, TLS 1.2 encryption with the recipient's public key is applied to all messages sent between the WAC and the server.

The WAC supports being deployed in corporate environments that make us of HTTPS proxies.

Security Controls Architecture


https://control.st.daintree.io
PIP
Customer access via DCS
Current's Azure Subscription
PIP
https://auth.st.daintree.io
https://api.st.daintree.io
PIP
PIP
Customer client accessing DCS APIs
AGW/WAF
Application micro-services
wss://iot-gateway.st.daintree.io
https://edge.st.daintree.io
Current DevOps & Support
Bastion Host – Only Available from Current corporate IP
Log analytics
Application & Container Insights
NSG
Azure Metric & Alerts
Wireless Area Controller (WAC60)
Zigbee

WAC-Onsite Communication

Within the local building's IP network, the WAC uses the following TCP/IP protocols:

Protocol	Port	TCP/UPP	Description
SSH	22	TCP	SSH terminal login for remote management of the WAC. Occasionally used by on-site technical support.
HTTPS	443	TCP	Access to WAC's web management interface. Used for initial IP configuration.
DNS	53	UDP	DNS
DHCP	68	UDP	DHCP
NTP	123	UDP	NTP
SECURE-MQTT	8883	TCP	Only enabled when inter-WAC communication is used in the building, e.g. switch pressed on one WAC turning lights on another WAC on (TLS certificate-based encryption).
BACnet	47808	UDP	Only enabled when BACnet is used. User can choose to use different port numbers for BACnet (default of 47808).

Wireless-side Security

The on-site wireless network is ZigBee, a global standard for Internet of Things (IoT) application. Used in a wide range of applications by hundreds of companies, ZigBee has been deployed in connected lighting, utility and retail applications, and the Smart Home.

The ZigBee standard currently being used in the Daintree Networked system is ZigBee Pro. ZigBee Pro defines the security standard to ensure interoperability between products from different vendors. Within this standard, there is a single trust center which manages access and trust. In the Daintree Networked system, the trust center resides in the WAC.

Messages exchanged between all wireless devices are encrypted using the network key with AES-128 with CCM, which is a NIST (National Institute of Standards Technology) approved cryptographic standard used to classify information up to the SECRET level.

Network Isolation

One of the strongest forms of security is isolation. Networks that are isolated from each other prevent compromises in one network from affecting other networks.

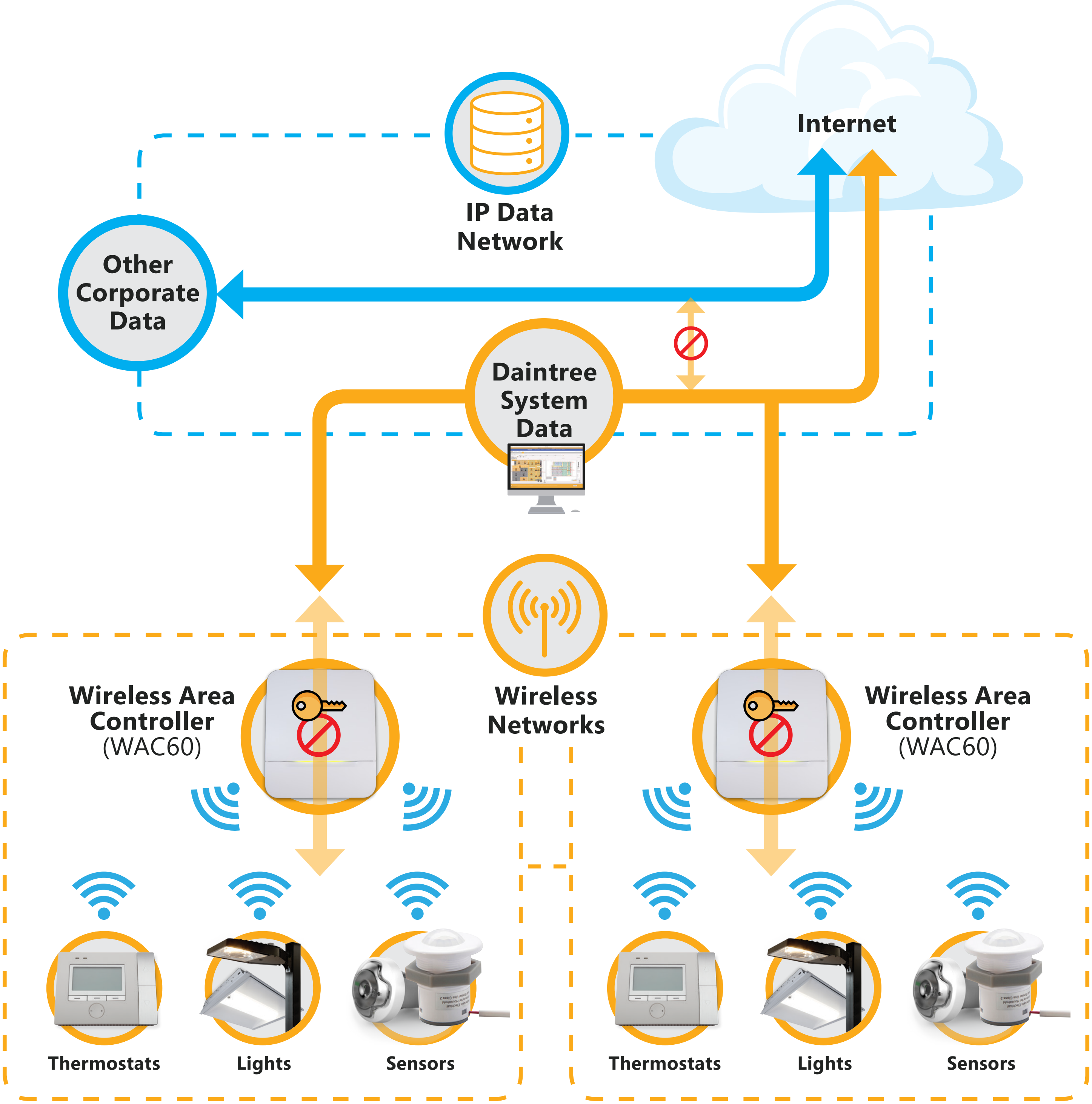
Each WAC manages a separate ZigBee network. Devices on one ZigBee network cannot directly communicate with devices on another network. Furthermore, each WAC independently manages its own and its network's security credentials. This effectively isolates these wireless networks from each other.

Furthermore, when a device gains access to the ZigBee network, that device cannot gain access to the IP network connected to the WAC. This effectively isolates the ZigBee network from the IP network.

A common practice is to isolate the data network used to move Daintree data (to/from the cloud) from the rest of the corporate network. In many corporate networks VLANs are used to support this.

Daintree® Networked - CYBERSECURITY OVERVIEW

Network Isolation Architecture



Security Controls – Hosting Environment

Data Center-Level Controls

The DCS-hosted environment resides in the Microsoft Azure public cloud. The data center is in Azure's East US region. Physical access security and other data center controls are provided by the hosting vendor. See the following link for additional information:
https://docs.microsoft.com/en-us/azure/security/fundamentals/infrastructure

Environment-Level Controls

Current maintains a rigorous separation between hosted production environments and pre-production and development environments. Computing resources supporting the production environment are not shared with pre-production/ development user, nor do they have access to the same network segments.

Network-Level Controls

The DSC infrastructure is protected at the network level by several mechanisms:

- A network level firewall (Azure NSG) is used to restrict communications between subnets and the public internet.
- A WAF configured with the OWASP 3.1 ruleset is configured to prevent insecure access at the application level.
- Access to internal database/messaging servers is restricted and accessible only via a jump host.
- Infrastructure support interfaces are protected by allow-listing only Current hosts. Public access to endpoints is limited to those required to for the application function. Support or diagnostic endpoints are only accessible via the employee login process.
- SSL is enabled for all infrastructure servers. WACs are trusted by the infrastructure by using peer authentication. TLS version 1.2 or above is required by all servers.

Host-Based Controls

Each host is provisioned via infrastructure automation tools. This ensures correct configuration of the host in compliance with Current policies and allows for full recovery in the event of a resource failure.

The infrastructure provisioning agent ensures that each host is configured with host-based network firewalls that close unneeded network ports and limit open ports only to the required protocol, source, and destination patterns. The provisioning agent also ensures that the host is running the latest available software patches for all installed software. Finally, the provisioning agent ensures that each host is configured with an anti-malware agent, monitoring agent, and security log aggregation agent.

Hosts and cloud services are configured to encrypt data at rest.

Availability and Disaster Recovery

Infrastructure is deployed in a redundant manner across multiple fault and update domains within Azure's East US region.

Databases are backed up at least daily and backups are stored for 90 days in a secure US-based multi-region storage. Disaster recovery plans are tested on at least an annual basis.

Security Controls – DCS Application

Web Application

The DCS web application is provided to clients only over HTTPS. Unencrypted sessions are not accepted. User sessions expire automatically after 60 minutes of inactivity, after which time the user is required to re-authenticate to continue to access the system.Environment-Level Controls

REST APIs

The DCS application can have API client accounts created to access the product's REST APIs. All REST APIs use OAUTH2 and client tokens have a validity of 12 hours.

Account Management & Federation

By default, DCS offers built-in User Administration functionality. At the customer's discretion, the system can optionally be integrated with the customer's preferred federated Identity Provider ("single sign-on") using industry-standard SAML2 exchanges. When using the built-in User Administration functionality, DCS requires user passwords to meet minimum password complexity requirements and prevents password reuse when changing passwords.

Role-Based Access Control

The DCS web application uses a role-based access control system. Each user is granted privileges based on the role assigned to his or her account. The available privileges are:

- Enterprise Admin – Can manage user accounts and make enterprise-wide configuration changes
- Commission – Can commission and fault find sites
- Facility Manager – Can view reports, current status and modify lighting control schedules

In addition to the above user roles there are two Current internal user roles System Admin and Support that are used by Current to manage and support the product.

Data Classification

The primary data stored by the DCS system includes data collected by Wireless Area Controllers (energy metering, light/sensor states and diagnostics), as well as user configurations (schedules and control parameters) and activity logs. DCS does not store any financial, payment, or healthcare/medical data.

DCS follows all privacy regulations to protect PII. In some regions, user account information stored by DCS (name and email address) may be classified as personally identifiable information. Requests to delete this information can be made by sending an email to current.privacy@currentlighting.com. For more information, refer to the company's privacy policy (www.LED.com).

Security Practices

In addition to the technical security controls described above, Current's staff employs many security practices and procedures as part of the operation of the system. Although internal policy documents are not shared with external parties, the following is a summary of practices employed.

Employee Access

Administrator access to the hosted environment is centrally controlled through the automated infrastructure provisioning process. Access to hosted resources is only granted on an as-needed, least-privileges approach and revoked after change of responsibilities or employment status. Granted access is regularly audited for policy compliance.

Access to hosted resources is tied into Current's corporate identity management solution, requires two factor authentication and only allowed when made from approved IP addresses.

Logging & Monitoring

As mentioned above, each host is automatically provisioned with a monitoring agent and configured with a set of task-specific monitoring rules. These monitoring checks ensure that the host is correctly configured and performing its intended function correctly. Monitoring checks are performed locally on the host via the monitoring agent as well as remotely by the monitoring service. The Current operations team responding to monitoring alerts is located in multiple time zones globally. In addition, each host is provisioned with a log aggregation agent that collects security event logging in a centralized repository for dashboarding, monitoring, and analysis.

Incident Response

Current has an Incident Response Program. As part of the program, dedicated playbooks are used for specific events. The program documents outline the IRP structure with roles and responsibilities. Steps within the playbook include assembling teams, triage, maintaining evidence, alerting insurance, involving authorities where appropriate, limiting spread/damage, clean-up, regulation compliance, notifications, and conducting lessons learned/improvements.

Secure Software Development Lifecycle

Current's "secure software development lifecycle" approach uses design-for-security throughout the entire software development process, not only once the software is deployed to the hosted environment. Automated tools are used to continuously identify and assess license- and vulnerability- risks associated with open source and third-party libraries used by the application.

Vulnerability Reporting

Current accepts security vulnerability reports from the public and security researchers. Vulnerabilities can be reported by emailing security@currentlighting.com.

Current - GLI Brands
25825 Science Park
Beachwood, OH 44122

LED.com/daintree