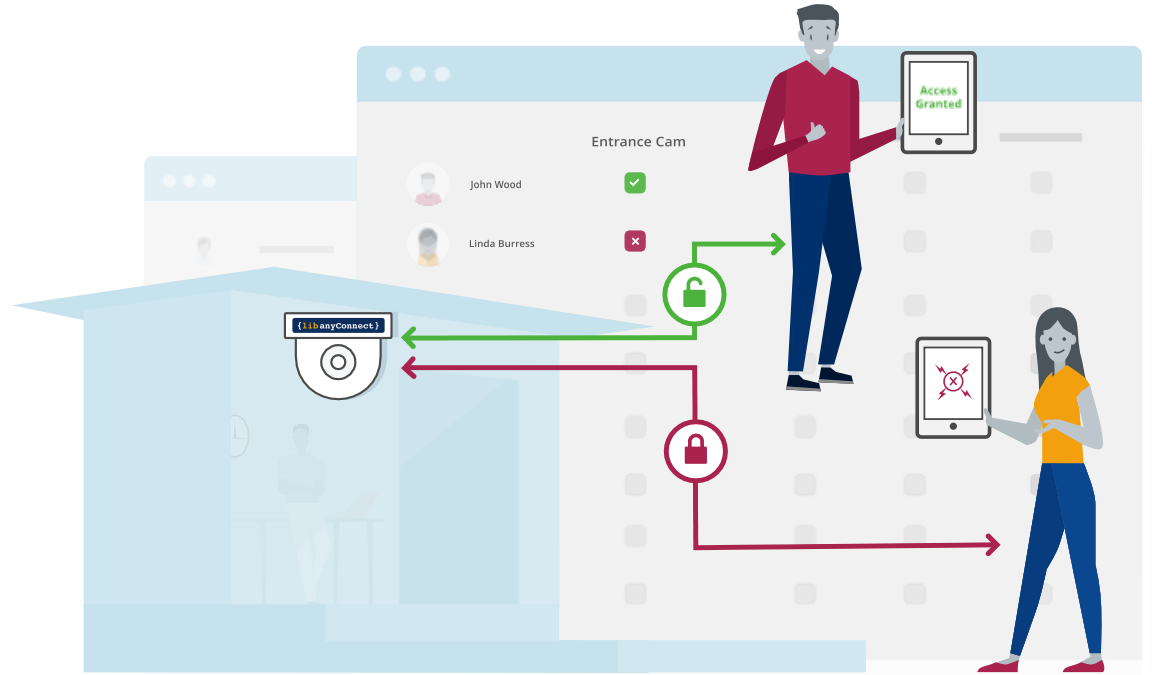


Access Control

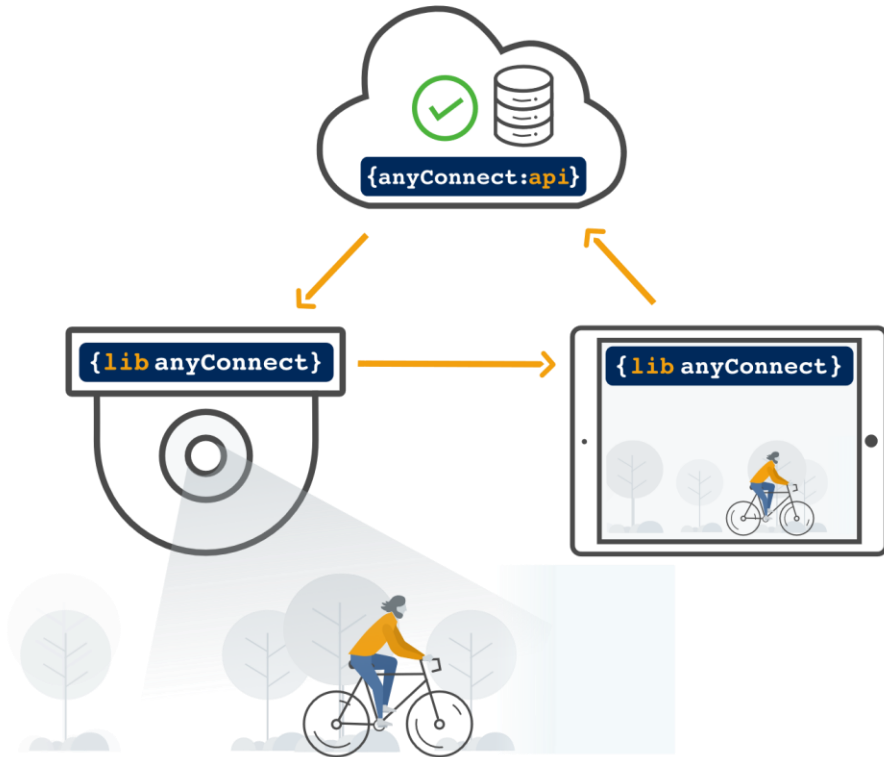
Version 1.1 | As seen on [Access Control](#)

What is Access Control?

Access control is a set of permissions for a connected camera (or any IoT Device) that specify which users are granted access and the operations they are permitted to perform. Each entry in an Access Control List (ACL) specifies a camera, a user, and an associated access level.



AnyConnect Access Control



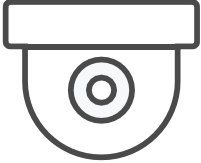
AnyConnect Access Control grants access to only the right users over [public networks](#) ([Wi-Fi](#), [LTE](#), [5G](#), etc.) It offers different access levels, simplifying access control management. AnyConnect Access Control is secure and enables you to be [GDPR](#)-compliant.


Access Control Challenges

Reliable access control must be resilient across public networks and mobile devices. This presents many challenges to reliable access control:


App and camera updates

updating...






Gregory Galan






Linda Burress



Irene Ross

Front Camera



Cross-region support



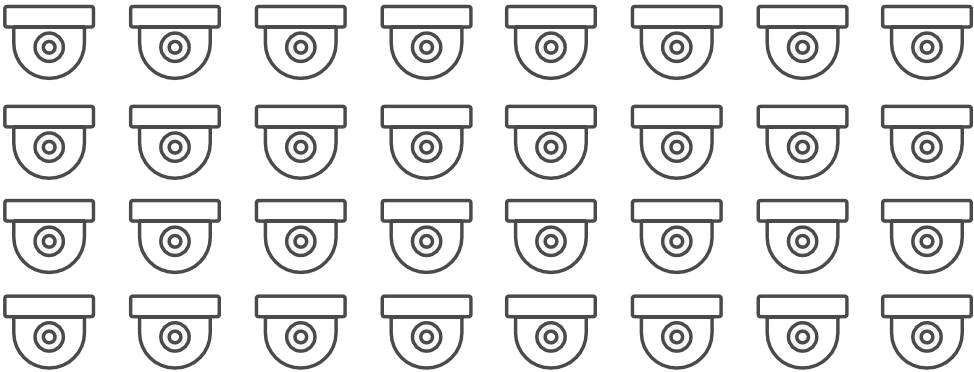
Network and state transitions



Data protection and privacy

COPPA **GDPR** **PIPEDA** **PIPA** **CaLOPPA** **APPI**

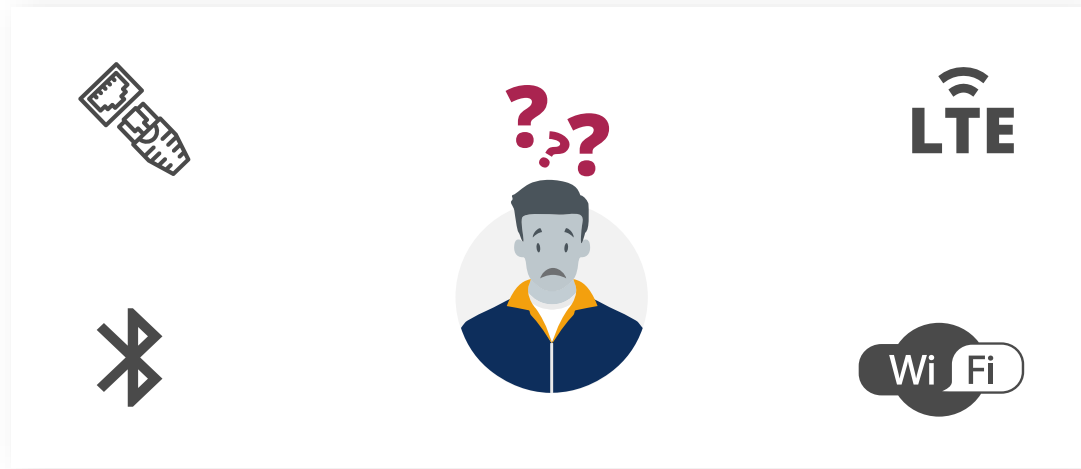
Scale



Security

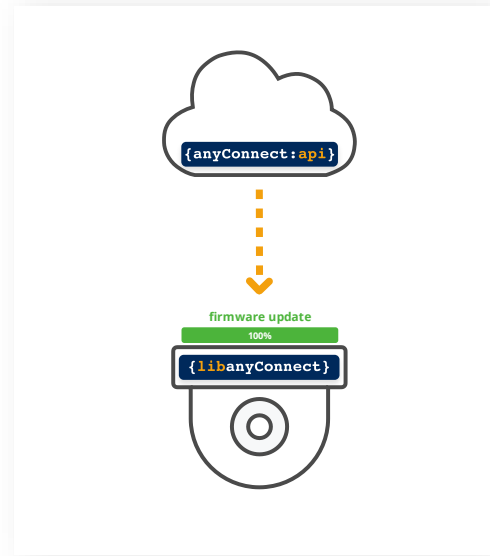


Wired and wireless networks

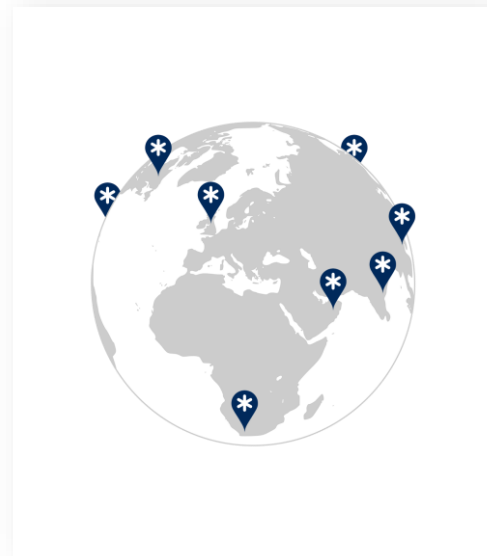


AnyConnect Access Control Benefits

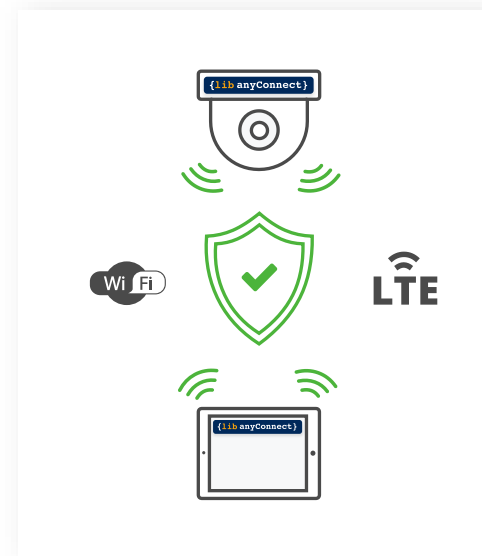
AnyConnect Access Control enables reliable camera (and other connected device) access control while maintaining security and compliance with data protection and privacy regulations. AnyConnect Access Control delivers:



Cloud-based access control is resilient to network (e.g. [Wi-Fi](#), [LTE](#) & [5G](#)) and state (i.e. online / offline) transitions.



AnyConnect cloud services originate and operate from separate geographic regions to support cameras and users worldwide.



Cloud-based access control is resilient to network (e.g. [Wi-Fi](#) to 4G) and state (i.e. online / offline) transitions.

- ✓ **COPPA**
- ✓ **GDPR**
- ✓ **APPI**
- ✓ **CaLOPPA**
- ✓ **PIPEDA**
- ✓ **PIPA**

Data protection and privacy compliance, including [GDPR](#) and other regulations.



Scalability, capable of controlling access to thousands of devices with a few clicks.



Security for data and connected devices.






Wired and wireless network support, including 4G, Bluetooth / BLE, Ethernet, and WiFi AP / WiFi Direct.

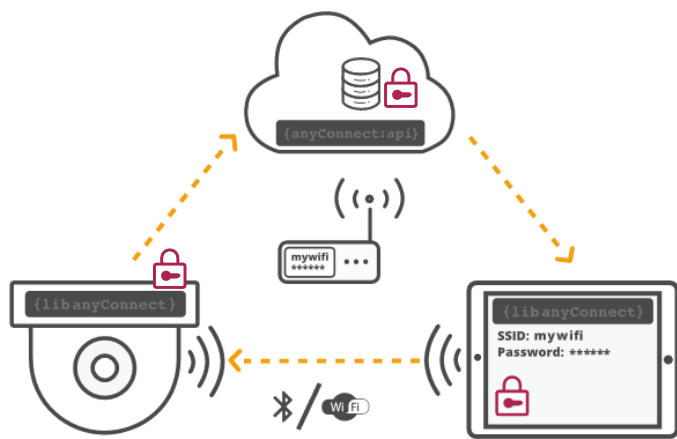
How AnyConnect Access Control Works

AnyConnect Access Control enables you to create new IoT business models such as Camera as a Service (CaaS) and Security as a Service (SECaaS or SaaS), where you might sell camera access to users.

1. Access Levels

AnyConnect Access Control supports 3 access levels:

| | View | Grant / Revoke Viewer Permissions | Grant / Revoke Admin Permissions |
|--|------|---|--|
|  Owner | ✓ | ✓ | ✓ |
|  Admin | ✓ | ✓ | ✗ |
|  Viewer | ✓ | ✗ | ✗ |



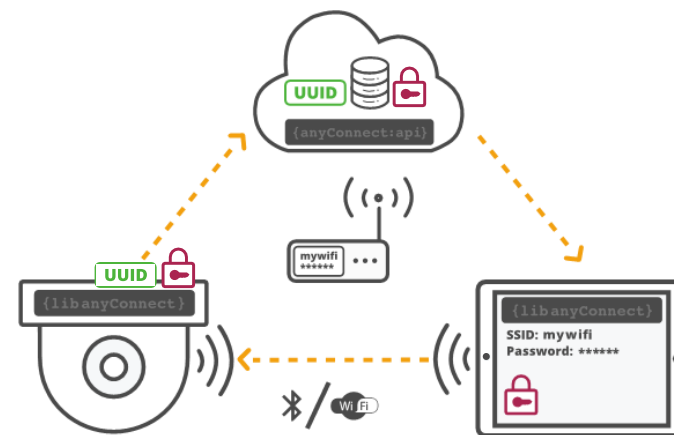
2. Pairing









Once a camera has been onboarded, a user can (via an App) request a “pairing key” from AnyConnect’s cloud service, and send this pairing key to the camera (e.g. via Bluetooth / BLE (Bluetooth Low Energy) or Wi-Fi AP / Wi-Fi Direct).

Upon receiving a pairing key, the camera forwards it to AnyConnect’s cloud service. Once AnyConnect’s cloud service validates the pairing key, the Camera and the App’s User and the Camera are “paired”, and AnyConnect’s Access Control service has created an ACL entry.

3. Access Control Service

Upon receiving a pairing key, the camera forwards it to AnyConnect’s cloud service. Once AnyConnect’s cloud service validates the pairing key, the Camera and the App’s User and the Camera are “paired”, and AnyConnect’s Access Control service has created an ACL entry.



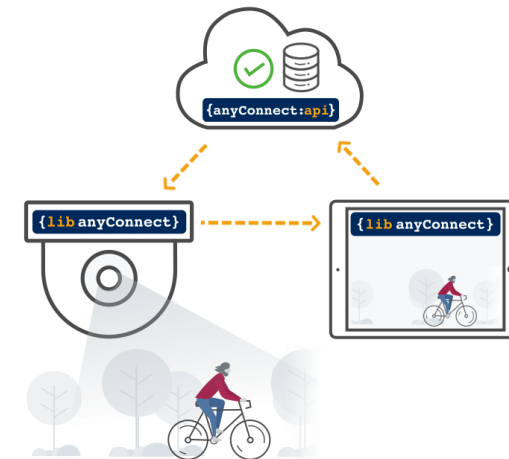
| Camera | User | Permissions |
|----------|---|--|
| Camera 1 |  Gregory Galan |  Owner |
| Camera 1 |  Linda Burress |  Admin |
| Camera 1 |  Irene Ross |  Viewer |
| Camera 1 |  John Wood |  Viewer |

5. Controlling Access

When a User requests to access a camera, for example to [stream live](#) or [recorded](#) video, AnyConnect's cloud service checks for a corresponding Access Control entry before granting or denying access.

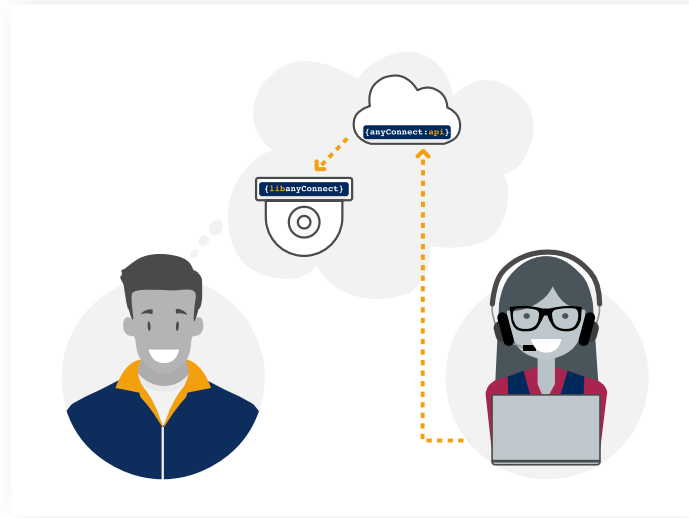
4. Granting and Revoking Access

Provided that they have sufficient access rights, an owner or admin user may grant access to and revoke access from other Users. A typical [Access Control List](#) may look like this:



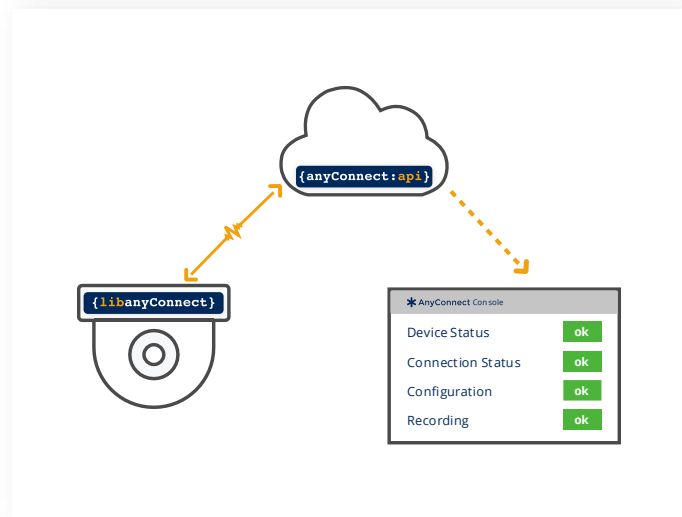
Additional Benefits of AnyConnect Access Control

AnyConnect Access Control enables you to create new IoT business models such as Camera as a Service (CaaS) and Security as a Service (SECaaS or SaaS), where you might sell camera access to users.



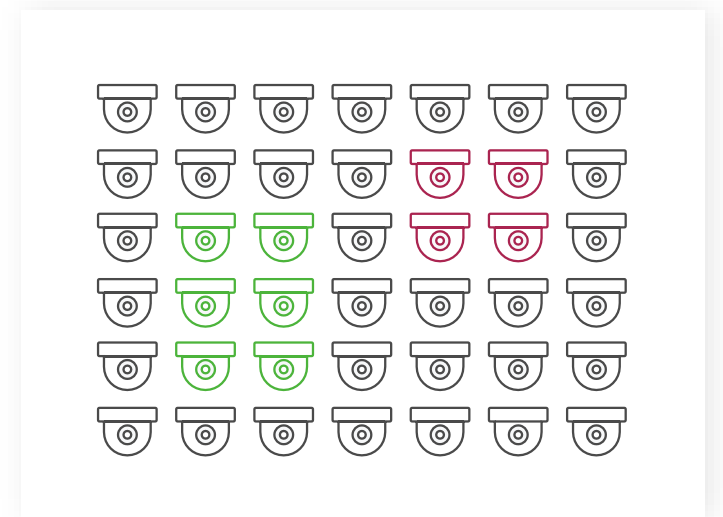
Remote customer and user support

Detect and remotely troubleshoot issues.



Device heartbeat

Manage the health of your connected devices by monitoring health and executing actions such as reboots, factory resets, and security updates.



Deployment management

Organize and manage your connected devices by groups, by applying access policies and firmware updates.

Get started with AnyConnect.

Ready to get started? Contact us

Talk to an expert