Overview of Ayla's Access Policy Control Manager

The Internet of Things evolution has enabled consumers and OEMs to interact with their connected devices in unprecedented ways.

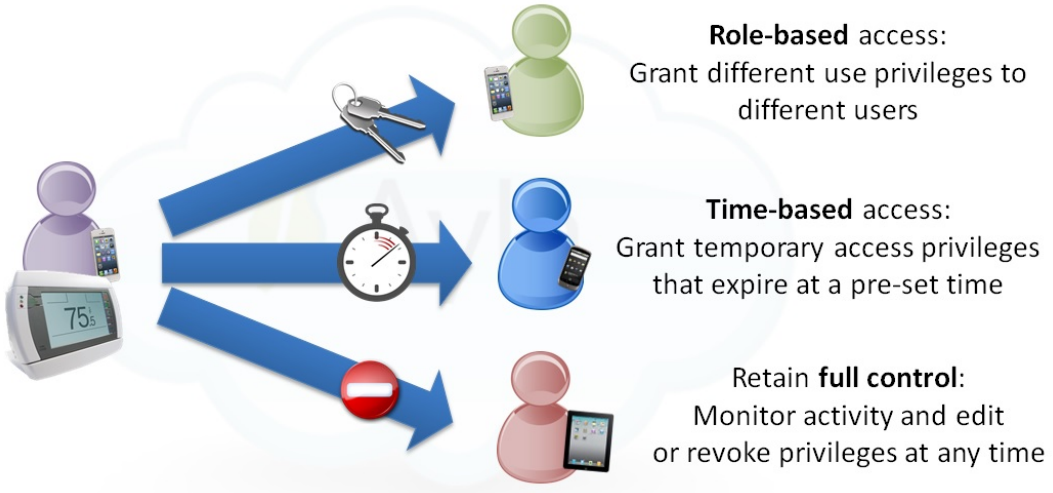
Consumers who buy connected devices expect to be able to control their devices in a secure manner. They need to be able to share their devices with their friends and family, while still maintaining control over how and when their devices are accessed.

For manufacturers developing connected devices, obtaining data from their devices offers a wealth of information. Typical use cases include analytics, auditing and troubleshooting. The manufacturer administrator of the IoT platform needs to have control over the company's users access to support and development portals. There is a strong need to have different levels of access based on their role in the company.

For legal, privacy and safety reasons, it is essential for access control policies to be enforced while users interact with their devices. This tech note presents an overview of Ayla's Access Policy Control Manager that can be used to define and enforce such policies.

Basic Tenet: A role is associated with a set of privileges on resources. Each user in the system is assigned a role. The role determines the privileges the user has on a resource. The salient features of the system are:

- Addresses both enterprise and consumer concerns
- Flexible, granular controls based on roles
- Supports a hierarchy of roles



Usage and Scenarios

Roles based on Organizational Structure

In a company, organizations are structured using various criteria such as product responsibility, location etc. In many instances, employees are granted privileges based on the organization they belong to. For example, an employee in the HVAC division of a company may be given access to oversee all connected thermostats, but not other wirelessly enabled products such as smoke and CO detectors belonging to the safety division.

Using Ayla's Access Policy Control Manager, a manufacturer admin can create a role for Thermostat Admins who have "superuser" like access to all the thermostat models that the company has in the field. The admin can also create a Thermostat Technician role with privileges to only view part of the data that a Thermostat Admin can view.

This flexibility allows for policies to be defined that follow a company's organizational structure.

Roles based on Sales Channel

Dealer Distribution

Many products sold through commercial channels are distributed through dealers. Examples are installations in commercial buildings, hospitals, or residences. The dealer typically performs the installation and has a maintenance contract with the customer. With this distribution model, there are many considerations. The dealer should have enough access to a device after its installation that would allow for its monitoring. However, the customer may want to limit how much of the data the dealer can access due to privacy or other considerations.

Retail Distribution

In this model, products are purchased by customers directly from retailers. The customer may own a mix of devices from the same manufacturer, some purchased through a dealer and some from a retailer. In this case, the customer would want to access all owned devices from a single application.

Ayla's Access Policy Control Manager supports a hierarchical model where the customer can access all owned devices, a dealer can only access allowed information on serviced devices, and the manufacturer can access all devices.

Device Sharing

There are use cases that warrant sharing of a device among many users. An example is any device in a home being used by multiple family members. In this situation, the primary owner of the device shares it with the other family members or with a guest. In a more commercial setting, a hotel could have connected locks installed with access granted to hotel guests for a period of time. Temporary or permanent privileges can be granted using the Ayla policy manager and can be revoked at any time by the owner.

Roadmap

Ayla's Access Policy Control Manager offers feature-rich access control services to cover the most common use cases for connected devices in enterprise, commercial and residential settings. Looking ahead, more enhancements are planned including an expanded role management user interface on the operational portal of the Ayla Agile IoT Platform. The goal is further expand this industry leading functionality as a self-service dashboard for manufacturers to administer their custom roles.