Avigilon ACM & Ambient.ai Signals User Guide

Nicolas Brochu, Ben Goeing / Ambient.ai Integrations Group

Document Version 1.0

Contents

Foreword

The purpose of this document is to describe the solutions features and provide instruction on how to use it.

Version History

Version	Date	Author	Object
1.0	2023-08-02	Nicolas Brochu, Ben Goeing	Original document

Table 1 - Version History

Abbreviations

Term	Definition
ACA	Ambient.ai Contextualized Alerts
ACS	Ambient.ai Cloud Services
CMA	Cloud Managed Appliance
EUS	Event Update Service
ACG	Ambient.ai Context Graph™
ERS	Event Retrieval Service
PACS	Physical Access Control System

Table 2 - Abbreviations

Introduction

The **Ambient.ai Signals Intelligence Integration** v2.0 connects the Ambient.ai Platform and Context Graph™ with Avigilon ACM. The Ambient.ai integration will ingest all events and forward them to the AI Context Graph. If a camera is attached to the reader in Ambient, a note will be added to the alarm to inform operators that the contextualization is in progress. The AI will analyze the video surrounding the event. This is primarily enabled for **Forced Door, Door Held Open and Invalid Card** events. **Valid Card** events are also used as additional context to improve contextualization. If no suspicious activity is detected, the AI Context Graph will instruct the integration to contact the Avigilon ACM to add a note as to why the event is not suspicious and to acknowledge the event to support operators in their monitoring work If a suspicious activity is detected, the integration will contact the Avigilon ACM using again the ACM REST API to add a note about why the alarm needs the operators intervention. As a result, customers can expect better prioritization and response times to critical alarms, while experiencing an overall alarm volume reduction through the deprioritization of alarms that are less relevant from a security perspective

The end-user will use this integration through the Avigilon ACM Alarms Monitor and the Events Monitorl. There is a separate Ambient.ai User Interface hosted in the cloud with complementary functionalities such as statistics about the types of alarms received and top alarm producing readers.

Contacting Ambient.ai

For support contact the following departments:

- Technical Support: integrations@ambient.ai
- General Support: support@ambient.ai

Additional contact information:

- Company Name: Ambient AI Inc.
- Company Address: 2010 N First St, Suite 405, San Jose CA 95131
- Company Website: https://ambient.ai/

What is the Ambient.ai Signals Intelligence Integration?

The integration uses Avigilon ACM REST API and an XML Collaboration. It communicates Avigilon ACM to exchange data as follows:

- It listens to an XML Collaboration that sends PACS events in XML format to a UDP port on the Ambient.ai Cloud Managed Appliance.
- It adds a note to inform operators that contextualization is in progress using the Avigilon ACM REST API.
- It adds a note when an alarm needs the operator's intervention.
- When the alarm does not need an operator's intervention, it adds a note about why and it acknowledges the alarm using the ACM REST API.

Only alarms coming from a reader or a door which has been associated with a video stream aimed at the door will be updated by the integration. These alarms are monitored by Ambient.ai. Other alarms will not be changed by Ambient.ai.

Threat signatures detection must also be enabled on the streams associated with the readers for any alarm to be put in progress and later acknowledged.

The stream must be healthy as the AI uses it to contextualize the alarm and determine if it is actionable or not.

The supported PACS events are Forced Door, Door Held Open and Invalid Card. Valid Card events are also used as additional context for Ambient.ai contextual threat signatures such as Tailgating detection. No PII information

related to card events is recorded by the integration. The integration can receive other events if the customer configures the Collaboration in Avigilon ACM to send more events. A customer may want to do this for a custom or a new threat detection.

How to use the Ambient.ai integration?

Ambient.ai will operate the services required for the integration. In the next figure, we can see the Avigilon ACM system, the Ambient.ai Cloud Managed Appliance and the Ambient.ai Cloud.

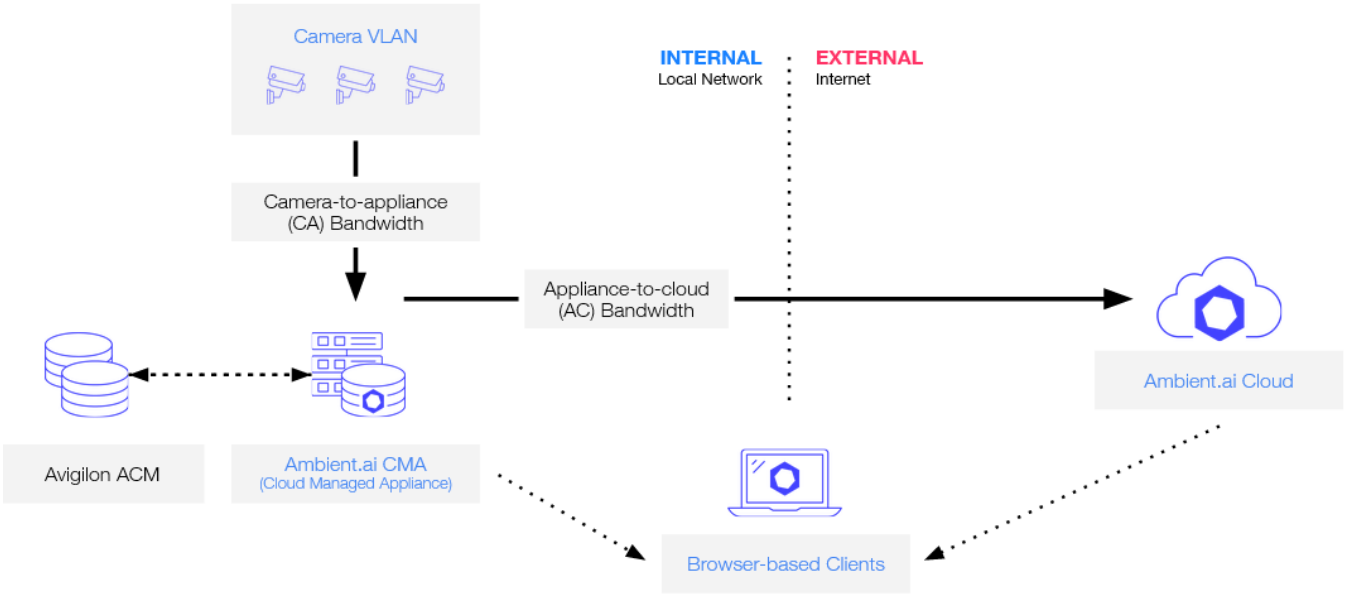

Figure 1 - Topology Diagram

Only the Cloud Managed Appliance installed in the local network can communicate with the Avigilon ACM system. Ambient.ai will provision the CMA and ship it to the customer. The customer can then install the physical server on the local network.

The Ambient.ai team will guide the customer in allowing communication between the CMA and the internet. This is required for the cloud to access the CMA.The Ambient.ai Cloud will only communicate with the CMA.

The integration requires that the CMA be able to communicate with the Avigilon ACM REST API endpoint. Typically, the ACM REST API endpoint is running on **port 443 of an Avigilon ACM appliance**. The **hostname or IP** and the port need to be communicated to Ambient.ai. **Firewalls and network routing** need to allow communication between the CMA and the Avigilon ACM.

All communications are in **HTTPS**. It is recommended that the end-user provide **the certificates of the root and intermediate Certificate Authorities that signed the certificate of the Avigilon ACM REST API endpoint**. Ambient.ai will trust these certificates in its CMA services to ensure the communication is secure.

The CMA will connect to the Avigilon ACM REST API endpoint. **A hostname, a port (usually 443)** and an **Avigilon ACM User** are required. The user must be named **Ambient.ai**. Since it needs to be able to add notes to ACM PACS alarms and acknowledge them if they don't require operator intervention, the user must be a member of the **Super Admin role**. See the next images for a UI reference on how to configure the Ambient.ai user in ACM.

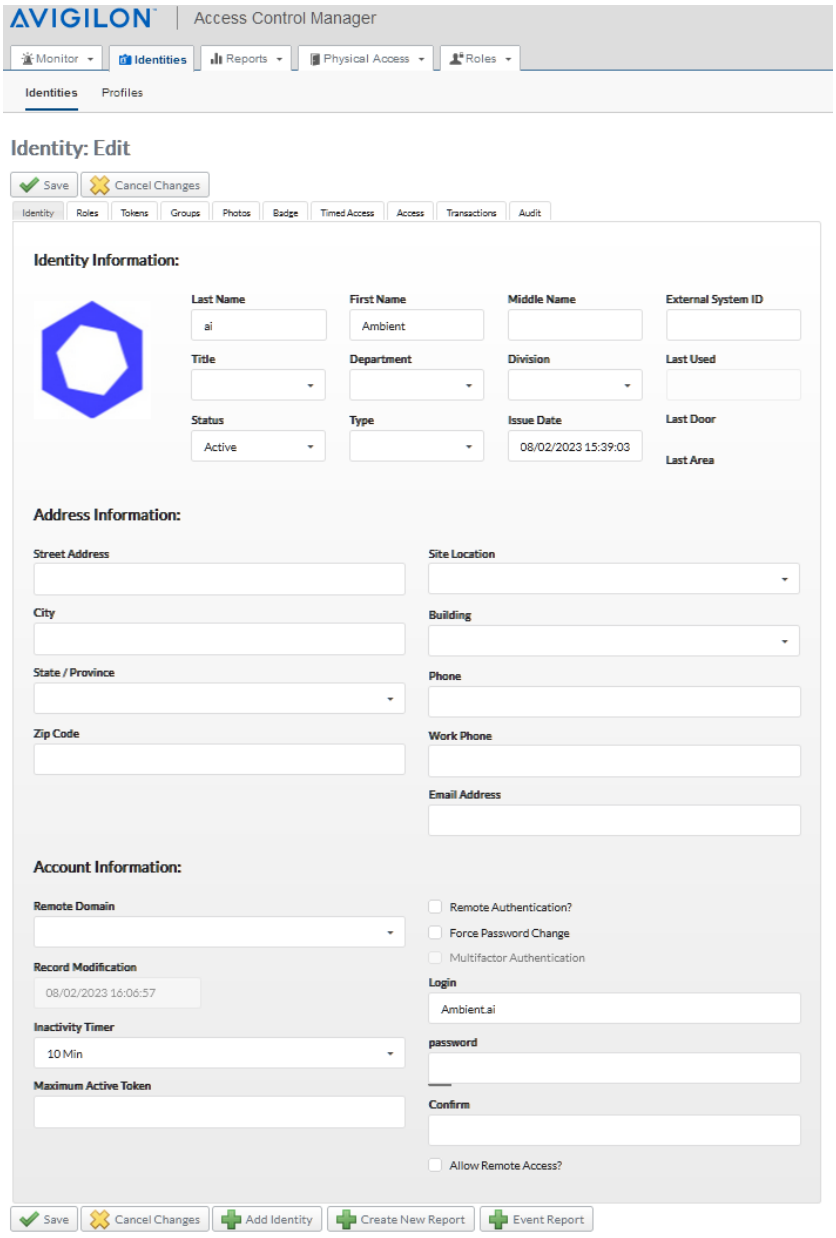

Image 1 - Avigilon ACM Ambient.ai User Identity Information

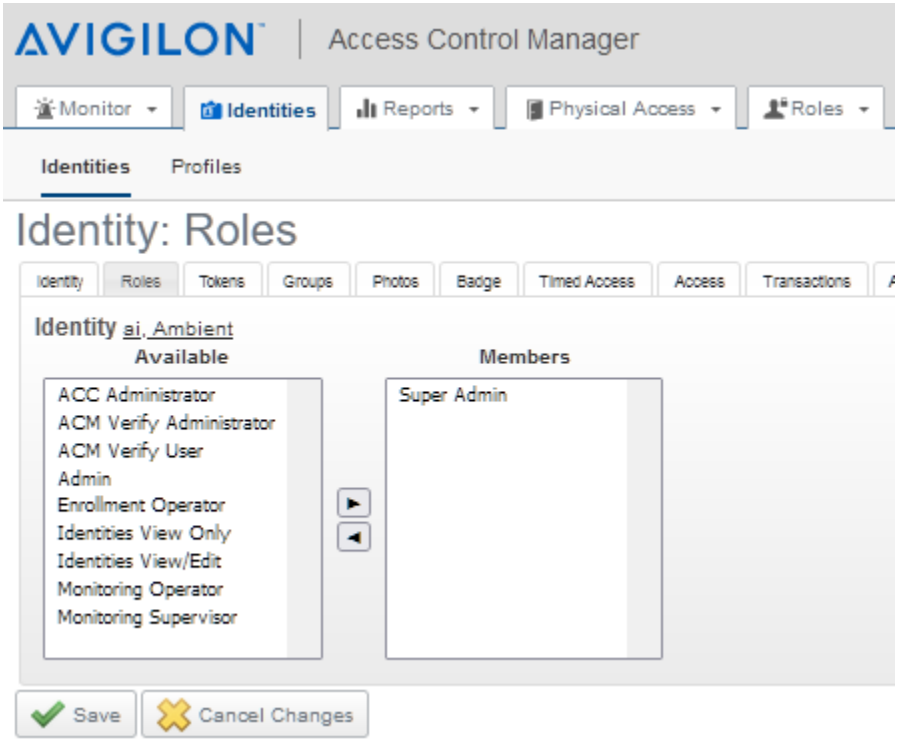

Image 2 - Avigilon ACM Ambient.ai User Identity Roles

An **Avigilon ACM Event Generic XML Collaboration** must be configured on the Avigilon ACM by the customer. **One CMA IP address** must be chosen. **A UDP port (usually 65123)** will need to be communicated to Ambient.ai.

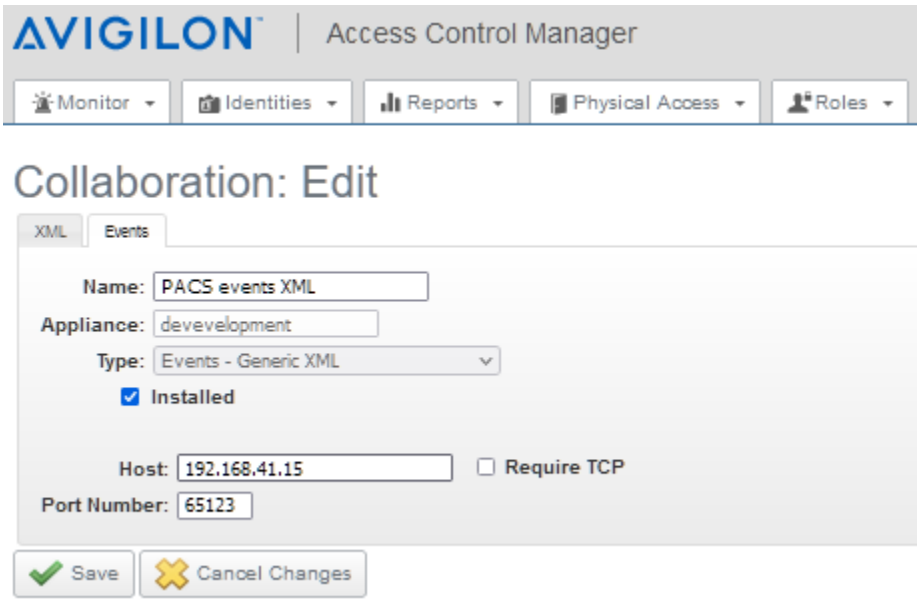

Image 3 - Avigilon ACM Collaboration Part 1

Also select the PACS events to send to the CMA and make sure to check the “Installed” checkbox and to set the schedule to “24 hours active”.

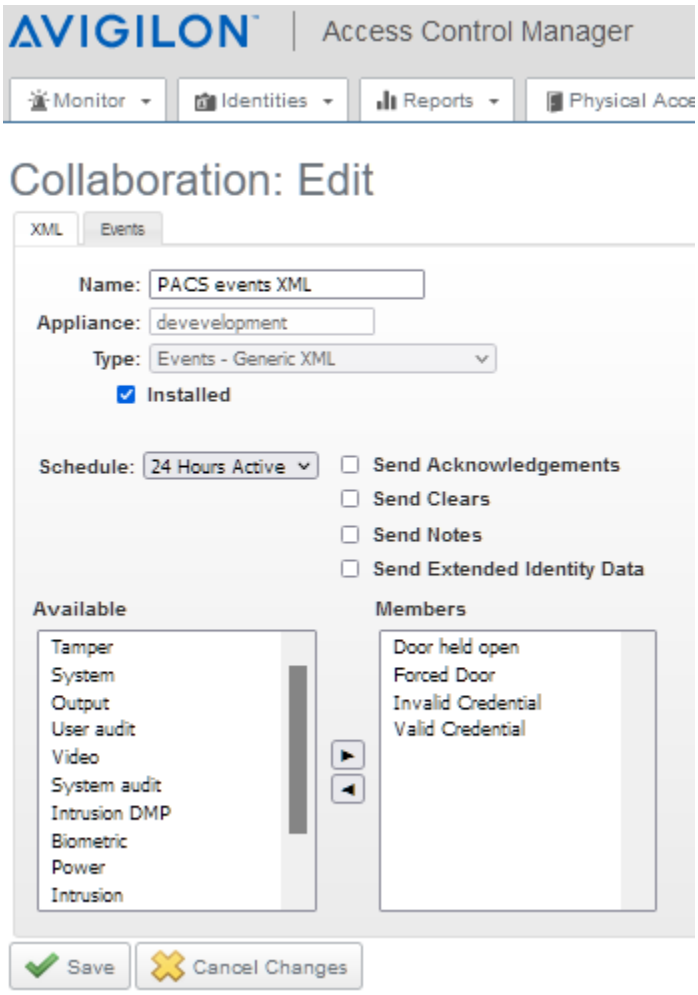

Image 4 - Avigilon ACM Collaboration Part 2

Once the Avigilon ACM is configured, the Ambient.ai Implementation Team will determine which threat signatures to enable on which video streams and will also assign readers to streams in its services.

Example use-case with Door Forced Open

Let's take the example of a customer that wants to be alerted only when someone enters through a door forced open.

Prerequisites

1. Ambient.ai has asserted that the door is within the view of a camera and that the image is of good quality for the AI to contextualize what is happening.
2. The Ambient.ai CMA was configured and receives events from the Avigilon ACM.
3. The reader of this door was linked to the video stream in Ambient.ai services by the Ambient.ai team.
4. Ambient.ai has discussed with the customer and the threat signature "Unauthorized Person Entering After Door Forced Open" is of interest.

5. The "Unauthorized Person Entering After Door Forced Open" is enabled and the video stream is healthy.

Actionable Event

1. The Ambient.ai system receives a Forced Door event from Avigilon ACM.
2. A note is added to the alarm in Avigilon ACM by the integration.The note informs operators that contextualization is in progress.
3. The AI contextualizes the alarm by analyzing the video stream showing the door.
4. The door opens and the AI detects a person coming through the door.
5. The integration adds a note to the alarm to let the operator know that this alarm requires an intervention.

Unactionable Event

1. The Ambient.ai system receives a Forced Door event from Avigilon ACM.
2. A note is added to the alarm in Avigilon ACM by the integration.The note informs operators that contextualization is in progress.
3. The AI contextualizes the alarm by analyzing the video stream showing the door.
4. The door stays closed and no one enters through the door.
5. The AI does not detect any threat because no person is present.
6. The integration adds a note that this alarm does not require an intervention and acknowledges it in the Avigilon ACM. The note has the reason “no person is present”.
7. Later, the operator can open the original alarm or event in Avigilon ACM Alarm Monitor and can review the AI’s decision through the PACS alarm history.

Image 5 - Avigilon ACM Alarm Monitor with Notes and Acknowledgment