BOSCH
Invented for life

BVMS - Configure AMS connection

Author: Verhaeg Mario (BT-SC/PAS4-MKP)
Date: 06-Nov-2018 08:03

1 Document information

Project	BVMS 9.0
Reference	198715
Version	2
Last modified	06 November 2018

1.1 Version history

Version	Date	Author	Comment
2	2018-06-11	Verhaeg Mario (BT-SC/PAS4-MKP)	

2 Introduction

This document describes how a BVMS system can be connected to the Bosch Access Management System.

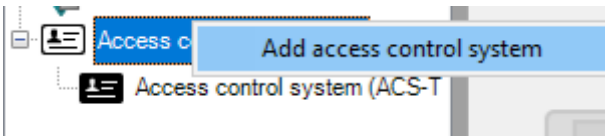
3 Import certificate

In order to secure the connection between the Access Management System and BVMS, a (client) certificate needs to be exported from the Access Management System to BVMS. This process is described in the section "HTTPS Certificate for Client" of the Access Management System documentation.

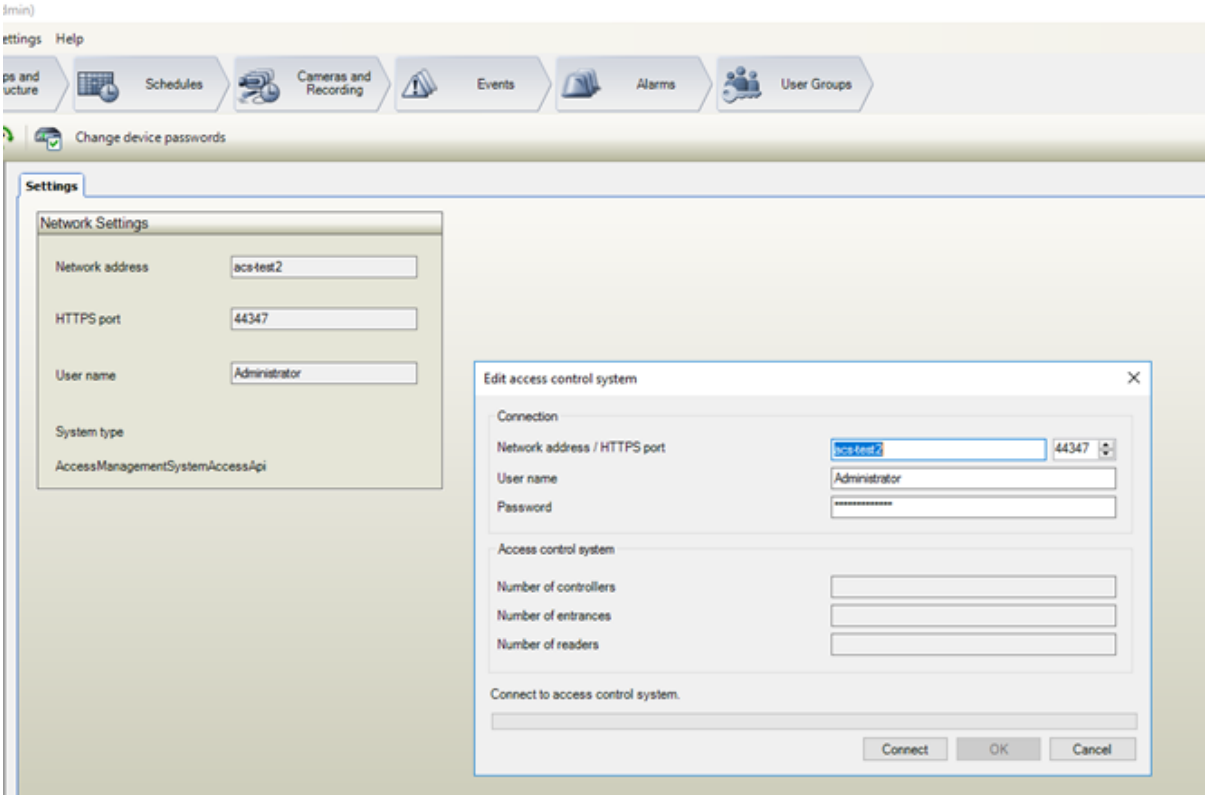
If the certificate is not added, the systems will not be able to exchange information with each other.

4 Adding system

The access control system node in the BVMS configuration client can be found under *other devices*. An access control system can be added by right clicking on the node.

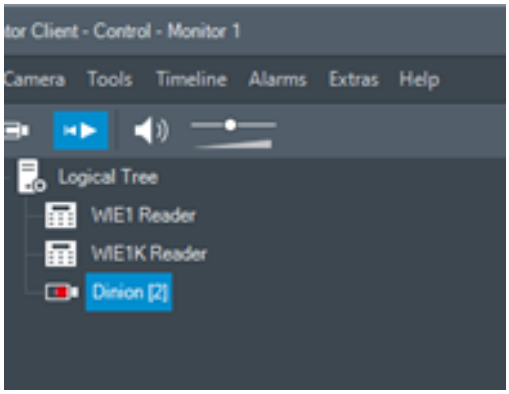


Fill in the details that are requested in the dialogue that popped-up, including the network address / HTTPS port, username and password.



Test the connection by clicking the *connect* button. The BVMS configuration client will try to connect to the Access Management System and retrieve the relevant information, for example: the number of controllers, the number of entrances and the number of readers. Click *OK* to add the Access Management System, based on the information displayed, to the BVMS configuration.

In order for the operator to see alarms coming in from the access control readers, the readers need to be added to the logical tree in the *Maps and logical structure* page of the BVMS configuration client. Based on the logical tree, the user permissions should also be configured.



Once configured correctly, the operator should be able to see the configured readers in the logical tree of the BVMS operator client.

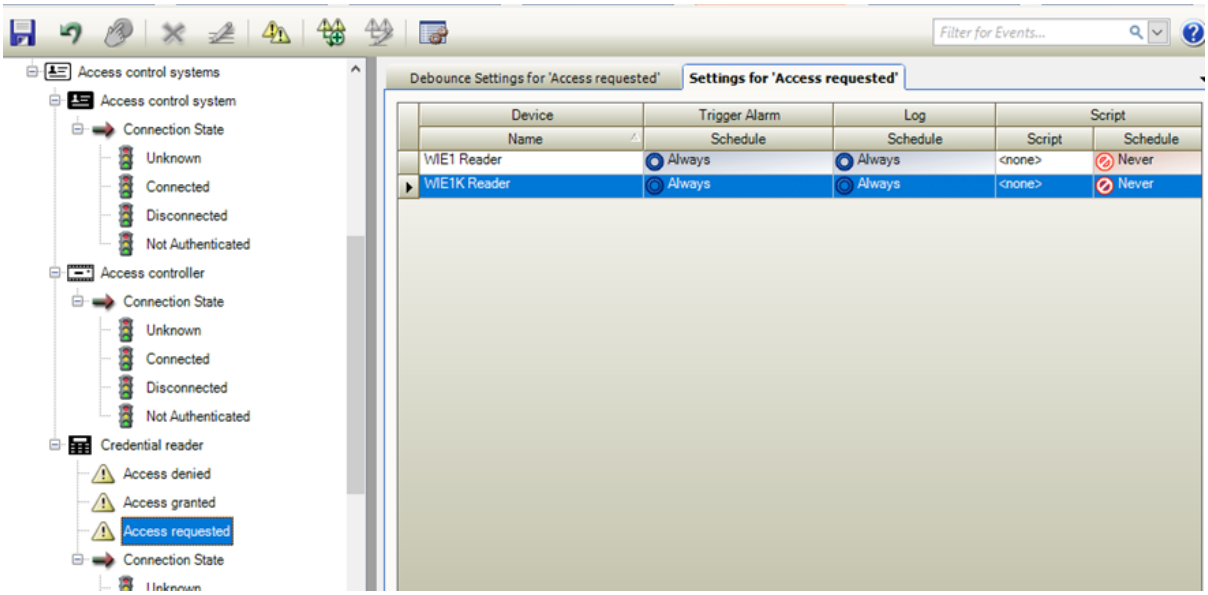
5 Event configuration

The first integration between the Access Management System and BVMS covers three use-cases:

1. Video verification: the operator is able to manually grant or deny access based on a request to enter an area or building.
2. People following: based on the information that the Access Management System sends to BVMS an operator can easily follow the last known location from a person based on recorded footage.
3. Entrance check: based on the information that the Access Management System sends to BVMS an operator can easily check all access control grant and deny events on a specific entrance.

5.1 Video verification / Access requested

In order to configure the video verification the reader needs to be configured for *additional verification*. Once this is done, the Access Management System will send the *Access requested* event to BVMS. This is a special event, which is able to control the behaviour of the Access Management System by allowing an operator to manually grant or deny access to a person.



In the BVMS event configuration, ensure that the readers that should trigger an *Access requested* event are always triggering an alarm. Then, the normal alarm configuration functionality can be used to assign a camera (live or instant playback) or additional information to this specific alarm.

> It is recommended to set the highest priority (1) for the *access request* related alarms. This will ensure the alarms will automatically pop-up and receive the necessary attention of the operator. Additionally it could be considered to assign these alarms to specific operator user group, which is tasked to handle these alarms with priority.

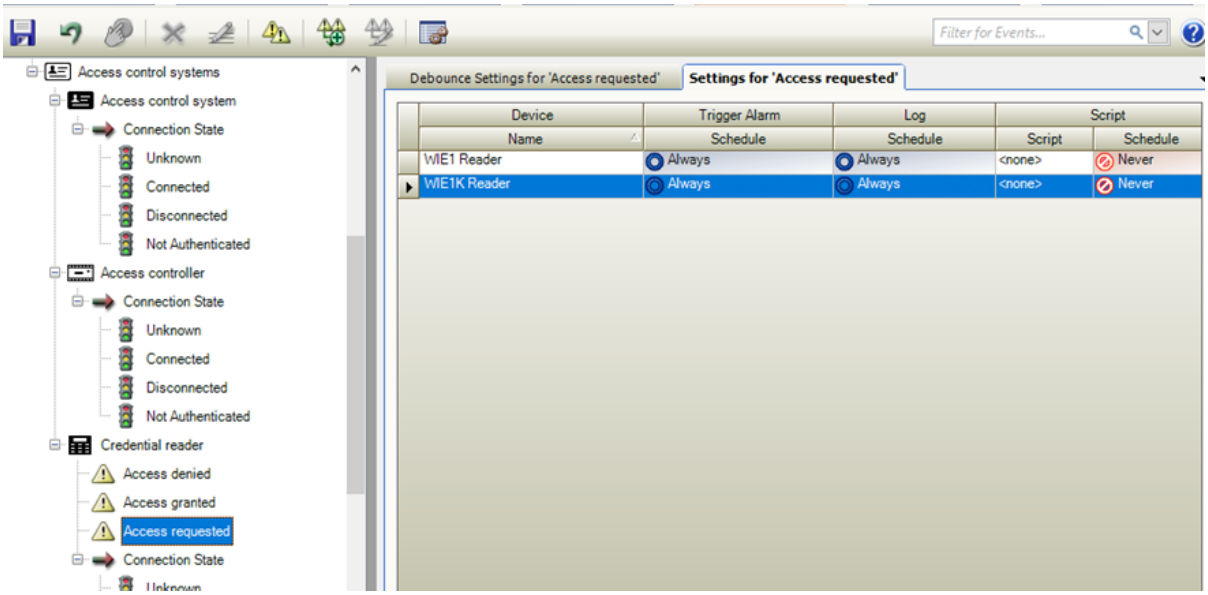
5.2 People following and entrance check

In order to allow an operator to easily search for persons and/or entrance related events in BVMS, all access control related information should be stored within the BVMS context.

5.2.1 Event logging

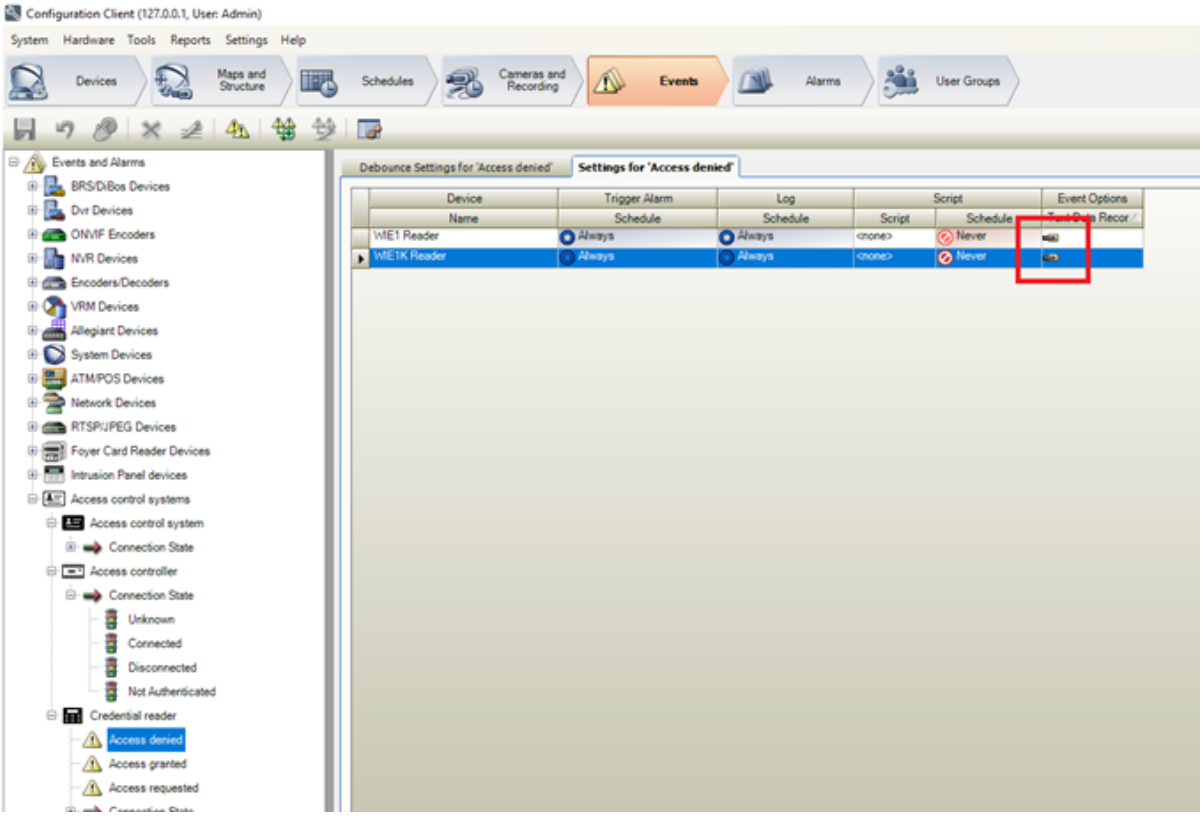
For this, all *Access requested, Access denied, and Access granted* events should be logged.

Please consider the maximum event load of the BVMS management server, which is listed in the datasheet.



5.2.2 Event recording

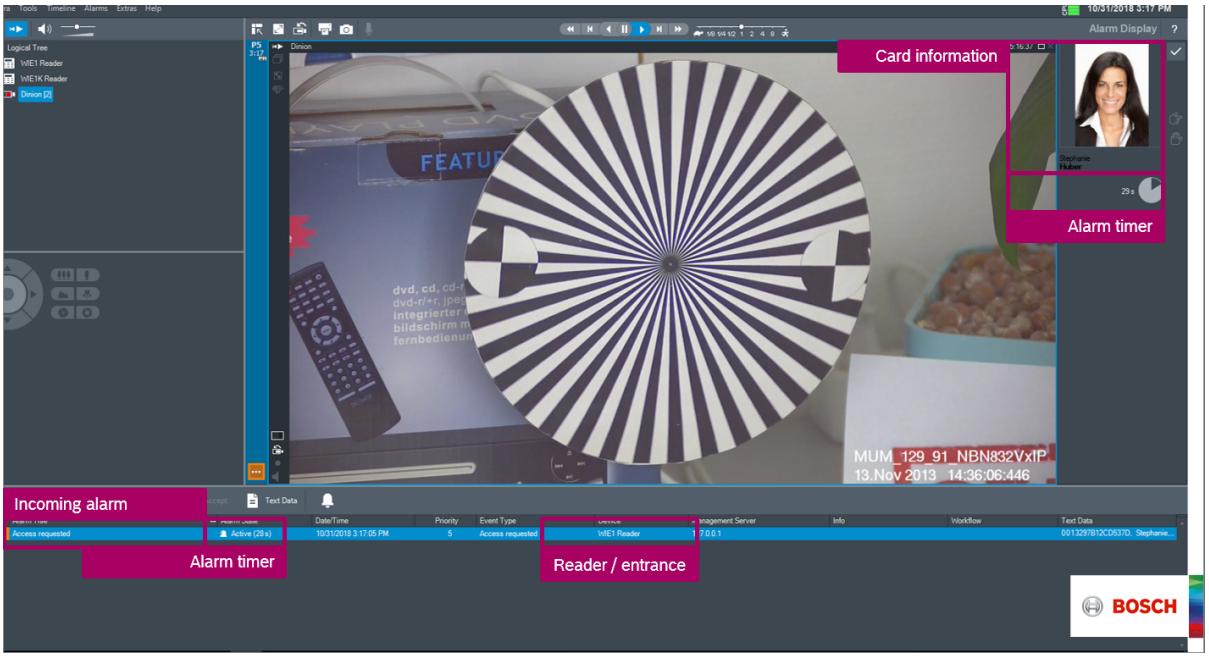
On top, these events should be recorded as additional data with the corresponding camera as well. Configure the *text data recording* for each event and relate it to the appropriate camera.



6 Result

6.1 Video verification

When an alarm comes in, the operator needs to accept the alarm first (depending on the alarm priority, it will automatically pop-up or it will pop-up after it has been accepted). In the meantime an alarm-timer is running which will show how much time the operator has to manually grant or deny access. Once the timer has run out, the system will automatically deny access for this specific request. The grant and deny access buttons can be found right next to the bottom of the cardholder photo.



6.2 Person following and entrance checking

The video event search mechanisms can be used to search for a specific (or multiple) persons or to check a specific entrance. Filter based on device for entrance checking or filter based on text data for finding a specific person.