

# Access and Time Biometric Terminals Parameters Guide

---

[Main Page](#)

[Modules](#)

[Classes](#)

[Access and Time Biometric Terminals Parameters Guide](#) >

**ReadMe**

## **Introduction**

---

This guide consists of an entire list of parameters that are used to configure the features of Biometric Terminals.

## **Copyright**

---

Copyright © 2017-2023, IDEMIA, All rights reserved.

Information in this document is subject to change without notice and does not represent a commitment on the part of IDEMIA.  
No part of this document may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying or recording, for any purpose without the express written permission of IDEMIA.

The software described in this document is supplied under a license agreement or nondisclosure agreement.

It is against the law to copy the software on any medium except as specifically allowed in the agreement.

This manual makes reference to names and products that are trademarks of their respective owners.

MorphoWave® is registered trademarks of IDEMIA, IDEMIA group.

Made in France.

## Revision History

### MorphoAccess® SIGMA Family Parameters Guide Revision History

<b>Firmware 1.0.10</b>	Dec, 2013	First official revision.
<b>Firmware 1.1.4</b>	May, 2014	Correction on sc.auto_key_update Change transaction_log.action_num_erase_log range
<b>Firmware 1.2.4</b>	Oct, 2014	<p>Added new keys:</p> <ul style="list-style-type: none"> <li>• misc.language_config_display</li> <li>• misc.user_id_edit</li> <li>• bio_security_settingsffd_security_level</li> <li>• auth_param.bio_policy_on_security_level_none</li> <li>• controller_feedback.pre_check_panel_state</li> <li>• sc.encode_timeout</li> <li>• ucc.users_photo_policy</li> <li>• sc.verify_csn_start</li> <li>• sc.verify_csn_length</li> <li>• sc.enroll_csn_start</li> <li>• sc.enroll_csn_length</li> </ul> <p>Updated keys:</p> <ul style="list-style-type: none"> <li>• sc.auto_key_update</li> <li>• sc.enroll_user_id</li> <li>• sc.verify_user_id</li> </ul> <p>Updated description:</p> <ul style="list-style-type: none"> <li>• controller_feedback.feedback_lines</li> <li>• remote_msg_conf.feedback_interface</li> <li>• ucc.users_photo_policy</li> </ul>
<b>Firmware 1.3.2</b>	Feb, 2015	<p>Note added in NTP server section</p> <p>Added new keys:</p> <ul style="list-style-type: none"> <li>• rtc.triggers_block_state</li> <li>• sc.HID_card_number_format</li> </ul> <p>Updated keys:</p> <ul style="list-style-type: none"> <li>• sc.enroll_user_id</li> <li>• sc.verify_user_id</li> </ul> <p>Updated description:</p>

		<ul style="list-style-type: none"> <li>ucc.face_auth_rule</li> <li>wiegand.prox_port_input_format</li> </ul>
<b>Firmware 1.3.3</b>	Mar, 2015	<p>Updated keys:</p> <ul style="list-style-type: none"> <li>sc.read_profile</li> </ul>
<b>Firmware 1.3.4</b>	Apr, 2015	<p>Updated description:</p> <ul style="list-style-type: none"> <li>sc.encode_profile</li> <li>sc_tlv_mifare_plus.start_block</li> </ul>
<b>Firmware 1.3.5</b>	May, 2015	<p>Added new keys:</p> <ul style="list-style-type: none"> <li>wiegand_protocol.output_byte_order</li> <li>sc_tlv_iclass.num_block</li> </ul> <p>Updated keys:</p> <ul style="list-style-type: none"> <li>time_and_attendance.tna_extended_mode</li> <li>sc.verify_user_id</li> </ul> <p>Updated description:</p> <ul style="list-style-type: none"> <li>sc_tlv_iclass.page_offset</li> <li>sc_l1_iclass.book_number</li> </ul>
<b>Firmware 1.3.7</b>	June, 2015	<p>Updated key:</p> <ul style="list-style-type: none"> <li>sc_l1_iclass.page_offset</li> </ul>
<b>Firmware 1.4.0</b>	Jul, 2015	<p>Added new keys:</p> <ul style="list-style-type: none"> <li>LCD_configuration.PIN_keypad_type</li> </ul>
<b>Firmware 1.5.0</b>	Aug, 2015	<p>Added new keys:</p> <ul style="list-style-type: none"> <li>misc.distant_session_timeout</li> <li>sc_tlv_mifare_plus.start_block</li> <li>sc_tlv_mifare_plus.num_block</li> <li>sc_tlv_mifare_plus.key_policy</li> <li>error_log_sensor.enabled</li> <li>error_log_sensor.modules</li> <li>time_and_attendance.jobcode_by_key</li> </ul> <p>Updated key:</p> <ul style="list-style-type: none"> <li>first_boot.storage_type</li> </ul>

		Updated description: <ul style="list-style-type: none"><li>sc.read_profile</li></ul>
<b>Firmware 1.5.1</b>	Jan, 2016	Updated keys: <ul style="list-style-type: none"><li>first_boot.storage_type</li></ul>
<b>Firmware 1.5.3</b>	April, 2016	Updated keys: <ul style="list-style-type: none"><li>sc.auto_key_update</li></ul>
<b>Firmware 1.6.0</b>	April, 2016	Added new keys related to distant command communication in client mode: <ul style="list-style-type: none"><li>comm_channels_state.TCP_client</li><li>TCP_client.host_ip</li><li>TCP_client.host_port</li><li>TCP_client.connection_period</li><li>TCP_client.connection_timeout</li><li>TCP_client.connection_retry</li></ul>
<b>Firmware 2.0.0</b>	Aug, 2015	Added new keys: <ul style="list-style-type: none"><li>comm_channels_state.USB_script</li><li>auth_param.timed_anti_passback_same_user_timeout</li><li>ucc.enable_timed_anti_passback</li></ul>
<b>Firmware 2.0.4</b>	Sep, 2015	Added MorphoAccess® SIGMA Lite Product Support
<b>Firmware 2.0.5</b>	Oct, 2015	Updated Firmware Version
<b>Firmware 2.1.1</b>	Dec, 2015	Updated Firmware Version
<b>Firmware 2.2.1</b>	Mar, 2016	Updated Documentation for Learning Phase
<b>Firmware 3.0.0</b>	May, 2016	Added New Keys: <b>SIGMA:</b> <ul style="list-style-type: none"><li>comm_channels_state.USB_script</li><li>auth_param.timed_anti_passback_same_user_timeout</li><li>ucc.enable_timed_anti_passback</li></ul> <b>SIGMA Lite / SIGMA Lite+:</b> <ul style="list-style-type: none"><li>error_log_sensor.enabled</li></ul>

		<ul style="list-style-type: none"> <li>• error_log_sensor.modules</li> <li>• misc.distant_session_timeout</li> <li>• comm_channels_state.TCP_client</li> <li>• TCP_client.host_ip</li> <li>• TCP_client.host_port</li> <li>• TCP_client.connection_period</li> <li>• TCP_client.connection_timeout</li> <li>• TCP_client.connection_retry</li> </ul> <p>Updated keys:</p> <ul style="list-style-type: none"> <li>• sc.hashing_enable</li> <li>• misc.multifinger_timeout</li> </ul>
<b>Firmware 3.1.0</b>	Aug, 2016	<p>Updated key:</p> <ul style="list-style-type: none"> <li>• error_log.debug_level</li> </ul> <p>Added New keys:</p> <ul style="list-style-type: none"> <li>• wiegand.site_code_propagation</li> <li>• wiegand.input_bits_detection_timeout</li> <li>• remote_msg_conf.serial_feedback_msg_display_timeout</li> <li>• remote_msg_serial_conf.format</li> </ul>
<b>Firmware 3.2.0</b>	Sep, 2016	<p>Added New keys:</p> <ul style="list-style-type: none"> <li>• MMI_state.finger_trigger_activate</li> <li>• LCD_configuration.icon_set</li> </ul>
<b>Firmware 3.3.2</b>	Jan, 2017	<p>Updated key:</p> <ul style="list-style-type: none"> <li>• sc_tlv_mifare.start_block</li> </ul>
<b>Firmware 3.4.0</b>	May, 2017	<p>Added New keys:</p> <ul style="list-style-type: none"> <li>• OSDP.channel</li> <li>• OSDP.device_serial_address</li> <li>• auth_param.template_type</li> <li>• sc_tlv_seos.adf_oid</li> <li>• sc_tlv_seos.first_do_tag</li> </ul>
<b>Firmware 3.5.0</b>	Jun, 2017	<p>Updated key:</p> <ul style="list-style-type: none"> <li>• comm_channels_state.USB_script</li> </ul>

		<p>Added New keys:</p> <ul style="list-style-type: none"> <li>LCD_configuration.ID_keypad_type</li> </ul>
<b>Firmware 4.0.0</b>	Jan, 2017	<p>Added MorphoAccess® SIGMA Extreme Product Support Added new keys:</p> <ul style="list-style-type: none"> <li>LCD_configuration.brightness_autoadaptive</li> <li>fake_finger.photo_taking</li> <li>tamper.photo_taking</li> <li>LCD_configuration.brightness_high</li> <li>LCD_configuration.brightness_low</li> <li>Light_sensor.threshold</li> <li>Light_sensor.hysteresis</li> <li>Light_sensor.adaptation_time</li> </ul>
<b>Firmware 4.1.0</b>	Mar, 2017	<p>Removed keys:</p> <ul style="list-style-type: none"> <li>LCD_configuration.brightness_autoadaptive</li> <li>LCD_configuration.brightness_high</li> <li>LCD_configuration.brightness_low</li> <li>MMI_state.finger_trigger_activate</li> <li>Light_sensor.threshold</li> <li>Light_sensor.hysteresis</li> <li>Light_sensor.adaptation_time</li> <li>fake_finger.photo_taking</li> <li>tamper.photo_taking</li> </ul>
<b>Firmware 4.1.2</b>	May, 2017	<p>Updated key:</p> <ul style="list-style-type: none"> <li>sc_tlv_mifare.start_block</li> </ul>
<b>Firmware 4.1.4</b>	August, 2017	<p>Added keys:</p> <ul style="list-style-type: none"> <li>LCD_configuration.brightness_autoadaptive</li> <li>LCD_configuration.brightness_high</li> <li>LCD_configuration.brightness_low</li> <li>Light_sensor.threshold</li> <li>Light_sensor.hysteresis</li> <li>Light_sensor.adaptation_time</li> </ul> <p>Updated description:</p> <ul style="list-style-type: none"> <li>LCD_configuration.brightness_autoadaptive</li> </ul> <p>Updated default value of keys:</p>

		<ul style="list-style-type: none"> <li>• Light_sensor.threshold</li> <li>• Light_sensor.hysteresis</li> <li>• Light_sensor.adaptation_time</li> </ul>
<b>Firmware 4.3.0</b>	Nov, 2017	<p>Updated key:</p> <ul style="list-style-type: none"> <li>• sc.support_l1_cards</li> <li>• LCD_configuration.enable_azerty_kbd</li> </ul> <p>Added keys:</p> <ul style="list-style-type: none"> <li>• misc.customized_workflow</li> </ul>
<b>Firmware 4.5.0</b>	May, 2018	<p>Added keys:</p> <ul style="list-style-type: none"> <li>• OSDP.secure_connection</li> <li>• sc_tlv_mifare_plus.start_block</li> <li>• sc_tlv_mifare_plus.num_block</li> <li>• sc_tlv_mifare_plus.key_policy</li> <li>• transaction_log.format</li> <li>• remote_msg_conf.format</li> </ul> <p>Updated key:</p> <ul style="list-style-type: none"> <li>• sc.verify_user_id</li> </ul>
<b>Firmware 4.6.0</b>	Apr, 2019	<p>Updated key:</p> <ul style="list-style-type: none"> <li>• sc.support_l1_cards</li> <li>• gpio.sdac_door_unlock_dur</li> <li>• misc.distant_session_timeout</li> <li>• time_and_attendance.tna_message_timeout</li> <li>• remote_msg_conf.feedback_interface</li> <li>• comm_channels_state.serial</li> </ul> <p>Added keys:</p> <ul style="list-style-type: none"> <li>• LCD_configuration.touch_sound</li> <li>• TCP_client.SSL_conn_state</li> <li>• TCP_client.profile_id</li> <li>• sc.encrypted_data</li> <li>• font.size</li> <li>• bio_security_settings.authentication_matching_threshold</li> <li>• comm_channels_state.upgrade_firmware</li> </ul> <p>Updated description:</p> <ul style="list-style-type: none"> <li>• sc.HID_card_number_format</li> <li>• sc.enroll_csn_start</li> </ul>

		<ul style="list-style-type: none"> <li>sc.enroll_csn_length</li> <li>sc.read_profile</li> <li>controller_feedback.feedback_lines</li> <li>time_and_attendance.tna_user_control</li> <li>time_and_attendance.key_select_timeout</li> <li>time_and_attendance.active_key_timeout</li> </ul>
<b>Firmware 4.7.1</b>	June, 2019	<p>Added MorphoAccess® VP Product Support</p> <p>Updated keys:</p> <ul style="list-style-type: none"> <li>gpio.gpo2_default_state</li> <li>gpio.gpi_table_gpi_2</li> <li>gpio.gpo_2_duration</li> </ul>
<b>Firmware 4.8.2</b>	February, 2020	<p>Updated key:</p> <ul style="list-style-type: none"> <li>time_and_attendance.tna_message_timeout</li> <li>gpio.gpi_table_gpi_0</li> <li>gpio.gpi_table_gpi_1</li> <li>gpio.gpi_table_gpi_2</li> </ul>
<b>Firmware 4.8.7</b>	June, 2020	<p>Updated key:</p> <ul style="list-style-type: none"> <li>success_message.display_information</li> <li>time_and_attendance.tna_message_timeout</li> <li>dynamic_message.mode</li> </ul> <p>Updated Description:</p> <ul style="list-style-type: none"> <li>bio_security_settings.ffd_security_level</li> <li>OSDP.ignore_mmi description</li> <li>sc.enroll_user_id</li> <li>contact_info.hotline_mail</li> </ul> <p>Added Keys:</p> <ul style="list-style-type: none"> <li>comm_channels_state.disable_IP</li> </ul>
<b>Firmware 4.9.2</b>	March, 2021	Removed MorphoAccess VP Product Support
<b>Firmware 4.12.0</b>	August, 2022	<p>Change default values of following parameters:</p> <ul style="list-style-type: none"> <li>in_channel.SSL_conn_mode</li> <li>TCP_client.SSL_conn_state</li> <li>comm_channels_state.web_server</li> <li>comm_channels_state.USB_script</li> <li>comm_channels_state.USB_thrift</li> </ul>

		<ul style="list-style-type: none"> <li>• comm_channels_state.TCP</li> <li>• sc.read_profile</li> </ul> <p>Updated keys:</p> <ul style="list-style-type: none"> <li>• misc.LCD_login_option</li> <li>• SSL_profile_0.protocol_version</li> <li>• SSL_profile_1.protocol_version</li> <li>• SSL_profile_0.cipher_list</li> <li>• SSL_profile_1.cipher_list</li> <li>• auth_param.timed_anti_passback_same_user_timeout</li> <li>• controller_feedback.panel_timeout</li> </ul> <p>Added keys:</p> <ul style="list-style-type: none"> <li>• comm_channels_state.cr_file_commit_or_cancel_timeout</li> </ul>
<b>Firmware 4.13.0</b>	August, 2022	Added Keys: <ul style="list-style-type: none"> <li>• LCD_configuration.keypad_layout</li> <li>• wiegand.pin_burst_mode</li> </ul>
<b>Firmware 4.13.1</b>	August, 2022	Added Key: <ul style="list-style-type: none"> <li>• sc_tlv_desfire.aid_list</li> </ul>
<b>Firmware 4.15.4</b>	August, 2023	Updated Keys: <ul style="list-style-type: none"> <li>• USB_script</li> <li>• verify_user_id</li> </ul>

## MorphoWave® Compact Parameters Guide Revision History And VisionPass Parameters Guide Revision History

<b>MWC Firmware 1.0.2</b>	April, 2018	<p>Added MorphoWave® Compact Product Support</p> <p>Added new keys:</p> <ul style="list-style-type: none"><li>• tamper.suspension_duration</li><li>• LCD_configuration.ID_keypad_type</li><li>• auth_param.template_type</li><li>• OSDP.channel</li><li>• OSDP.secure_connection</li><li>• OSDP.device_serial_address</li></ul> <p>Updated keys:</p> <ul style="list-style-type: none"><li>• tamper.state</li><li>• tamper.photo_taking</li><li>• gpio.sdac_relay_default_state</li><li>• wiegand.event_duress_finger</li><li>• contact_info.hotline_mail</li><li>• contact_info.hotline_number</li><li>• auth_param.bio_policy_on_security_level_none</li><li>• enroll.acquisition_threshold</li><li>• sc_l1_desfire.fid</li><li>• sc_l1_desfire.aid</li><li>• sc_l1_iclass.page_offset</li><li>• sc_l1_iclass.page_layout</li><li>• sc_l1_iclass.book_number</li><li>• sc_l1_mifare.kb_number</li><li>• sc_l1_mifare.key_policy</li><li>• sc_tlv_mifare_plus.start_block</li><li>• sc_tlv_mifare_plus.num_block</li><li>• sc_tlv_mifare_plus.key_policy</li><li>• sc.read_profile</li><li>• sc.encode_profile</li><li>• sc.hashing_enable</li><li>• sc.support_l1_cards</li><li>• LCD_configuration.idle_video_timeout</li><li>• LCD_configuration.brightness_autoadaptive</li><li>• face_detection.timeout</li><li>• ucc.allow_duress_finger</li><li>• ucc.allow_duress_finger_TL1</li><li>• ucc.allow_duress_finger_TL2</li><li>• ucc.allow_duress_finger_TL3</li><li>• ucc.users_photo_policy</li><li>• ucc.face_auth_rule</li><li>• ucc.face_auth_rule_TL1</li></ul>
-----------------------------------	-------------	--

		<ul style="list-style-type: none"> <li>ucc.face_auth_rule_TL2</li> <li>ucc.face_auth_rule_TL3</li> <li>fake_finger.photo_taking</li> <li>MMI_state.finger_trigger_activate</li> <li>sc_tlv_mifare.start_block</li> </ul>
<b>MWC Firmware 1.1.0</b>	August, 2018	<p>Added keys:</p> <ul style="list-style-type: none"> <li>transaction_log.format</li> </ul> <p>Updated keys:</p> <ul style="list-style-type: none"> <li>comm_channels_state.web_server</li> </ul>
<b>MWC Firmware 1.2.0</b>	December, 2018	<p>Added key:</p> <ul style="list-style-type: none"> <li>comm_channels_state.USB_script</li> <li>TCP_client.SSL_conn_state</li> <li>TCP_client.profile_id</li> </ul>
<b>MWC Firmware 1.4.0</b>	February, 2019	<p>Updated key:</p> <ul style="list-style-type: none"> <li>ucc.trigger_event</li> </ul>
<b>MWC Firmware 1.5.0</b>	September, 2019	<p>Added key:</p> <ul style="list-style-type: none"> <li>font.size</li> <li>bio_security_settings.authentication_matching_threshold</li> <li>LCD_configuration.touch_sound</li> </ul> <p>Updated keys:</p> <ul style="list-style-type: none"> <li>dynamic_message.mode</li> </ul> <p>Updated description:</p> <ul style="list-style-type: none"> <li>time_and_attendance.tna_message_timeout</li> <li>tamper.suspension_duration</li> </ul>
<b>MWC Firmware 1.5.2</b>	November, 2019	<p>Updated description:</p> <ul style="list-style-type: none"> <li>tamper.suspension_duration</li> </ul>
<b>VisionPass Firmware 2.0.0</b>	Apr, 2020	<p>Added VisionPass Product Support</p> <p>Deprecated keys in comparison to MWC:</p>

		<ul style="list-style-type: none"> <li>• misc.multifinger_timeout</li> <li>• ucc.finger_bio_auth_rule</li> <li>• ucc.finger_bio_auth_rule_TL1</li> <li>• ucc.finger_bio_auth_rule_TL2</li> <li>• ucc.finger_bio_auth_rule_TL3</li> </ul> <p>Added new keys in comparison to MWC:</p> <ul style="list-style-type: none"> <li>• misc.multiusers_timeout</li> <li>• ucc.biometric_auth_rule</li> <li>• ucc.biometric_auth_rule_TL1</li> <li>• ucc.biometric_auth_rule_TL2</li> <li>• ucc.biometric_auth_rule_TL3</li> <li>• bio_security_settings.intentional_bio_capture</li> <li>• LCD_configuration.play_video_during_active_mode</li> <li>• MMI_state.user_guidance</li> </ul> <p>Updated keys in comparison to MWC:</p> <ul style="list-style-type: none"> <li>• auth_param.additional_bio_check_nb_attempt</li> <li>• auth_param.additional_bio_check_timeout</li> <li>• auth_param.template_type</li> <li>• identify_param.matching_strategy</li> <li>• enroll.acquisition_threshold</li> <li>• bio_security_settings.matching_threshold</li> <li>• bio_security_settings.authentication_matching_threshold</li> <li>• bio_security_settings.ffd_security_level</li> <li>• error_log_sensor.modules</li> <li>• LCD_configuration.low_power_disable_sensor</li> <li>• LCD_configuration.icon_set</li> <li>• LCD_configuration.standby_mode</li> <li>• sc_tlv_desfire.aid</li> <li>• sc_tlv_mifare.num_block</li> <li>• tamper.photo_taking</li> <li>• terminal_information.desc_name</li> <li>• time_and_attendance.tna_mandatory_mode</li> <li>• time_and_attendance.tna_user_control</li> <li>• time_and_attendance.active_key_timeout</li> <li>• ucc.trigger_event</li> </ul>
<b>Firmware</b> <b>2.4.1</b>	October, 2020	<p>Seos is added to MWC / ViP</p> <p>Updated keys:</p> <ul style="list-style-type: none"> <li>• sc.read_profile</li> <li>• sc.enroll_user_id</li> <li>• sc_tlv_iclass.num_block</li> <li>• success_message.display_information</li> </ul>

		<p>Added Keys:</p> <ul style="list-style-type: none"> <li>• comm_channels_state.disable_IP</li> </ul>
<b>Firmware 2.4.4</b>	December, 2020	<p>PIV/TWIC is supported to MWC / ViP Updated keys:</p> <ul style="list-style-type: none"> <li>• sc.read_profile</li> <li>• sc.verify_user_id</li> </ul> <p>Wiegand format added:</p> <ul style="list-style-type: none"> <li>• wiegand_fmt_TWIC_75</li> <li>• wiegand_fmt_TWIC_200</li> </ul>
<b>Firmware 2.5.0</b>	February, 2021	<p>Image storage in transaction logs is added to ViP Updated keys:</p> <ul style="list-style-type: none"> <li>• ucc.face_auth_rule</li> <li>• controller_feedback.feedback_lines</li> <li>• controller_feedback.panel_mode</li> <li>• controller_feedback.pre_check_panel_state</li> <li>• controller_feedback.granted_pulse_width</li> <li>• controller_feedback.granted_pulse_interval</li> <li>• controller_feedback.denied_pulse_width</li> <li>• controller_feedback.denied_pulse_interval</li> <li>• controller_feedback.PIN_pulse_width</li> <li>• controller_feedback.PIN_pulse_interval</li> <li>• LCD_configuration.idle_screen_status</li> </ul> <p>Added Keys:</p> <ul style="list-style-type: none"> <li>• ucc.mask_auth_rule</li> </ul>
<b>Firmware 2.5.1</b>	March, 2021	<p>Removed MorphoAccess VP Product Support Updated keys:</p> <ul style="list-style-type: none"> <li>• ucc.users_photo_policy</li> </ul> <p>Main page:</p> <ul style="list-style-type: none"> <li>• Updated website URL</li> </ul>
<b>Firmware 2.6.1</b>	May, 2021	<p>Updated keys: Added QR trigger event</p> <ul style="list-style-type: none"> <li>• ucc.trigger_event</li> </ul> <p>Added keys:</p>

		<ul style="list-style-type: none"> <li>• misc.auth_cmd_trigger_timeout</li> </ul> <p>Updated description:</p> <ul style="list-style-type: none"> <li>• ucc.user_record_reference</li> </ul>
<b>Firmware 2.7.1</b>	June, 2021	<p>Key renamed:</p> <ul style="list-style-type: none"> <li>• misc.auth_cmd_trigger_timeout to identify_param.auth_trigger_timeout</li> </ul> <p>Added Keys:</p> <ul style="list-style-type: none"> <li>• auth_param.qr_code_auth_timeout</li> </ul> <p>Updated description:</p> <ul style="list-style-type: none"> <li>• identify_param.auth_trigger_timeout</li> <li>• ucc.per_user_rules</li> <li>• ucc.face_auth_rule</li> <li>• ucc.face_auth_rule_TLx</li> <li>• Smart Card</li> </ul> <p>Updated keys:</p> <ul style="list-style-type: none"> <li>• misc.multiuser_timeout</li> <li>• contact_info.web</li> </ul>
<b>Firmware 2.8.0</b>	August, 2021	<p>Updated keys:</p> <ul style="list-style-type: none"> <li>• OSDP.ignore_MM</li> </ul> <p>Added keys:</p> <ul style="list-style-type: none"> <li>• OSDP.access_granted</li> <li>• OSDP.access_denied</li> </ul>
<b>Firmware 2.8.2</b>	September, 2021	<p>Updated keys:</p> <ul style="list-style-type: none"> <li>• sc.verify_user_id</li> </ul>
<b>Firmware 2.9.0</b>	July, 2022	<p>Change default values of following parameters:</p> <ul style="list-style-type: none"> <li>• in_channel.SSL_conn_mode</li> <li>• TCP_client.SSL_conn_state</li> </ul>

		<ul style="list-style-type: none"> <li>• comm_channels_state.web_server</li> <li>• comm_channels_state.USB_script</li> <li>• comm_channels_state.USB_thrift</li> <li>• comm_channels_state.TCP</li> <li>• sc.read_profile</li> </ul> <p>Updated keys:</p> <ul style="list-style-type: none"> <li>• misc.LCD_login_option</li> <li>• SSL_profile_0.protocol_version</li> <li>• SSL_profile_1.protocol_version</li> <li>• SSL_profile_0.cipher_list</li> <li>• SSL_profile_1.cipher_list</li> <li>• auth_param.timed_anti_passback_same_user_timeout</li> <li>• controller_feedback.panel_timeout</li> </ul> <p>Added keys:</p> <ul style="list-style-type: none"> <li>• comm_channels_state.cr_file_commit_or_cancel_timeout</li> </ul>
<b>Firmware 2.10.5</b>	August, 2022	<p>Added keys:</p> <ul style="list-style-type: none"> <li>• QR.hexa_value</li> <li>• sc_tlv_desfire.aid_list</li> </ul>
<b>Firmware 2.10.7</b>	November, 2022	<p>Added key:</p> <ul style="list-style-type: none"> <li>• error_log.osdp_debug_level</li> </ul> <p>Updated key:</p> <ul style="list-style-type: none"> <li>• OSDP.ignore_MMI</li> </ul>
<b>Firmware 2.10.10</b>	Feb, 2023	<p>Updated description for:</p> <ul style="list-style-type: none"> <li>• Introduction</li> <li>• Copyright</li> </ul> <p>Two subsections introduced:</p> <ul style="list-style-type: none"> <li>• Covered products</li> <li>• ReadMe</li> </ul>
<b>Firmware 2.11.1</b>	April, 2023	<p>Updated key:</p> <ul style="list-style-type: none"> <li>• sc.auto_key_update</li> </ul>
<b>Firmware</b>	August,	Updated keys:

<b>2.12.1</b>	2023	<ul style="list-style-type: none"> <li>• QR.hexa_value</li> </ul>
<b>Firmware 2.12.2</b>	September, 2023	<p>Updated keys:</p> <ul style="list-style-type: none"> <li>• ucc.trigger_event</li> </ul>
<b>Firmware 2.13.3</b>	December, 2023	<p>Updated keys:</p> <ul style="list-style-type: none"> <li>• allow_biopin_user_rule</li> </ul>
<b>Firmware 2.13.4</b>	January, 2024	<p>Added key :</p> <ul style="list-style-type: none"> <li>• OSDP.pin_over_osdp</li> </ul>

## MorphoWave® Simplified Parameters Guide Revision History

<b>MWSP Firmware 1.0.0</b>	Feb, 2022	<p>Added MorphoWave® Simplified Profile Product Support</p> <p>Unsupported keys in comparison to MWC:</p> <ul style="list-style-type: none"> <li>• all Keys about chapter “audio” except audio.volume</li> <li>• auth_param.additional_pin_check_nb_attempt</li> <li>• auth_param.additional_pin_check_timeout</li> <li>• comm_channels_state.upgrade_firmware</li> <li>• comm_channels_state.USB_thrift</li> <li>• controller_feedback.panel_mode</li> <li>• controller_feedback.PIN_pulse_width</li> <li>• controller_feedback.PIN_pulse_interval</li> <li>• controller_feedback.keypad_passthru_timeout</li> <li>• all Keys about chapter “Dynamic message and Font”</li> <li>• all Keys about chapter “Job Code”</li> <li>• all Keys about chapter “LCD configuration” except misc.user_id_edit &amp; misc.distant_session_timeout</li> <li>• all Keys about chapter “Time and Attendance”</li> <li>• ucc.allow.biopin_user_rule</li> <li>• ucc.allow.biopin_user_rule_TL1/TL2/TL3</li> <li>• ucc.pin_auth_rule</li> <li>• ucc.pin_auth_rule_TL1/TL2/TL3</li> <li>• success_message.display_information</li> <li>• reject_message.display_reason</li> <li>• auth_param.cr_auth_timeout</li> </ul> <p>Supported keys in comparison to MWC:</p> <ul style="list-style-type: none"> <li>• MMI_state.finger_trigger_activate</li> </ul> <p>Different default key value in comparison to MWC:</p> <ul style="list-style-type: none"> <li>• terminal_information.desc_name</li> <li>• comm_channels_state.USB_script</li> <li>• controller_feedback.feedback_lines</li> <li>• in_channel.SSL_conn_mode</li> <li>• comm_channels_state.TCP</li> </ul> <p>Different Key values in comparison to MWC</p> <ul style="list-style-type: none"> <li>• SSL_profile_0.protocol_version</li> <li>• SSL_profile_1.protocol_version</li> </ul>
<b>MWSP Firmware 1.1.0</b>	July, 2022	Change default values of following parameters: <ul style="list-style-type: none"> <li>• in_channel.SSL_conn_mode</li> </ul>

		<ul style="list-style-type: none"> <li>• TCP_client.SSL_conn_state</li> <li>• comm_channels_state.web_server</li> <li>• comm_channels_state.USB_script</li> <li>• comm_channels_state.USB_thrift</li> <li>• comm_channels_state.TCP</li> <li>• sc.read_profile</li> </ul> <p>Updated keys:</p> <ul style="list-style-type: none"> <li>• misc.LCD_login_option</li> <li>• SSL_profile_0.protocol_version</li> <li>• SSL_profile_1.protocol_version</li> <li>• SSL_profile_0.cipher_list</li> <li>• SSL_profile_1.cipher_list</li> <li>• auth_param.timed_anti_passback_same_user_timeout</li> <li>• controller_feedback.panel_timeout</li> </ul> <p>Added keys:</p> <ul style="list-style-type: none"> <li>• comm_channels_state.cr_file_commit_or_cancel_timeout</li> </ul>
MWSP Firmware 2.1.4	March, 2024	<p>Changed default values of following keys:</p> <ul style="list-style-type: none"> <li>• SSL_profile_0.cipher_list</li> <li>• SSL_profile_1.cipher_list</li> <li>• bio_security_settings.ffd_security_level</li> </ul> <p>Updated keys:</p> <ul style="list-style-type: none"> <li>• SSL_profile_0.protocol_version</li> <li>• SSL_profile_1.protocol_version</li> <li>• SSL_profile_0.cipher_list</li> <li>• SSL_profile_1.cipher_list</li> <li>• OSDP.ignore_MM</li> </ul> <p>Added keys:</p> <ul style="list-style-type: none"> <li>• comm_channels_state.legacy_certificate</li> <li>• QR.hexa_value</li> <li>• auth_param.qr_code_auth_timeout</li> <li>• sc.no_data</li> <li>• sc_tlv_desfire.aid_list</li> <li>• SSCP.channel</li> <li>• SSCP.device_serial_address</li> <li>• SSCP.intercharacter_timeout</li> <li>• SSCP.start_of_frame_timeout</li> <li>• tamper.action_reset_SSCP</li> </ul>

**MWSP  
Firmware  
2.1.5**

April,  
2024

Updated Description for the keys:

- controller\_feedback.feedback\_lines
- controller\_feedback.pre\_check\_panel\_state

## VisionPass SP Parameters Guide Revision History

<b>VisionPass SP Firmware 2.0.0</b>	Sep, 2023	<p>Added VisionPass SP® Product Support</p> <p>Unsupported keys in comparison to VisionPass:</p> <ul style="list-style-type: none"><li>• audio.permission_verify_success</li><li>• audio.permission_verify_fail</li><li>• audio.permission_message_attention</li><li>• comm_channels_state.upgrade_firmware</li><li>• comm_channels_state.USB_thrift</li><li>• controller_feedback.denied_pulse_width</li><li>• controller_feedback.granted_pulse_width</li><li>• controller_feedback.PIN_pulse_interval</li><li>• controller_feedback.PIN_pulse_width</li><li>• QR.hexa_value</li><li>• wiegand.prox_port_input_format</li><li>• LCD_configuration.play_video_during_active_mode</li><li>• auth_param.qr_code_auth_timeout</li><li>• auth_param.additional_bio_check_nb_attempt</li><li>• ucc.mask_auth_rule</li><li>• LCD_configuration.idle_video_timeout</li><li>• identify_param.auth_trigger_timeout</li><li>• controller_feedback.granted_pulse_width</li><li>• controller_feedback.denied_pulse_width</li></ul> <p>Different default key value in comparison to VisionPass:</p> <ul style="list-style-type: none"><li>• controller_feedback.feedback_lines</li><li>• sc.encode_profile</li><li>• terminal_information.desc_name</li><li>• auth_param.additional_bio_check_timeout</li><li>• bio_security_settings.ffd_security_level</li><li>• font.size</li><li>• MMI_state.user_guidance</li></ul> <p>Different Key values in comparison to VisionPass:</p> <ul style="list-style-type: none"><li>• SSL_profile_0.protocol_version</li><li>• SSL_profile_0.cipher_list</li><li>• SSL_profile_1.protocol_version</li><li>• SSL_profile_1.cipher_list</li><li>• sc.encode_profile</li><li>• sc.read_profile</li><li>• ucc.trigger_event</li><li>• ucc.trigger_event_TL1</li><li>• ucc.trigger_event_TL2</li><li>• ucc.trigger_event_TL3</li></ul>
-------------------------------------	-----------	---

		<p>Supported keys in comparison to VisionPass:</p> <ul style="list-style-type: none"> <li>• identify_param.detection_area</li> <li>• identify_param.acquisition_area</li> <li>• comm_channels_state.legacy_certificate</li> <li>• Display_text.horizontal_start</li> <li>• Display_text.vertical_start</li> <li>• Display_text.color</li> </ul>
<b>VisionPass SP Firmware 2.1.0</b>	Dec, 2023	<p>Added clarification and updated wording in the following sections:</p> <ul style="list-style-type: none"> <li>• auth_param.additional_pin_check_timeout</li> <li>• auth_param.additional_bio_check_timeout</li> <li>• auth_param.timed_anti_passback_same_user_timeout</li> <li>• QR.hexa_value</li> <li>• bio_security_settings.authentication_matching_threshold</li> <li>• bio_security_settings.intentional_bio_capture</li> <li>• comm_channels_state.TCP</li> <li>• in_channel.primary_port</li> <li>• in_channel.secondary_port</li> <li>• comm_channels_state.cr_file_commit_or_cancel_timeout</li> <li>• misc.receive_state_machine_timeout</li> <li>• ip_restraining.mode</li> <li>• controller_feedback.panel_mode</li> <li>• controller_feedback.feedback_lines</li> <li>• controller_feedback.panel_timeout</li> <li>• remote_msg_conf.feedback_interface</li> <li>• remote_msg_conf.serial_feedback_msg_display_timeout</li> <li>• jobcode.timeout</li> <li>• LCD_configuration.ID_keypad_type</li> <li>• misc.user_id_edit</li> <li>• remote_msg_ip_conf.mode</li> <li>• sc.zero_tag_read</li> <li>• sc_tlv_desfire.aid_list</li> <li>• sc.enroll_user_id</li> <li>• sc.verify_user_id</li> <li>• sc.HID_card_number_format</li> <li>• Time_override_mode.tor_mode</li> <li>• gpio.threat_level_mode</li> <li>• gpio.cmd_based_active_threat_level</li> <li>• gpio.threat_level_gpi_0</li> <li>• gpio.threat_level_gpi_1</li> <li>• gpio.threat_level_gpi_2</li> <li>• gpio.threat_level_gpi_3</li> <li>• time_and_attendance.tna_mode</li> <li>• transaction_log.format</li> <li>• ucc.trigger_event</li> </ul>

		<ul style="list-style-type: none"> <li>• ucc.per_user_rules</li> <li>• ucc.mask_auth_rule</li> <li>• ucc.pin_auth_rule</li> <li>• ucc.face_auth_rule</li> <li>• success_message.display_information</li> <li>• ucc.enable_timed_anti_passback</li> <li>• ucc.trigger_event</li> <li>• ucc.allow_biopin_user_rule</li> <li>• wiegand.site_code_checking</li> <li>• wiegand.site_code_propagation</li> <li>• wiegand.pin_burst_mode</li> <li>• Display_text.color</li> <li>• SSL_profile_0.cipher_list</li> <li>• SSL_profile_1.cipher_list</li> </ul> <p>Updated keys:</p> <ul style="list-style-type: none"> <li>• Display_text.vertical_start</li> <li>• comm_channels_state.USB_script</li> <li>• bio_security_settings.ffd_security_level</li> </ul> <p>Added keys:</p> <ul style="list-style-type: none"> <li>• LCD_configuration.lighting_level</li> <li>• motion_sensor.activation</li> </ul>
VisionPass SP Firmware 2.1.5	April, 2024	<p>Added new value in the key:</p> <ul style="list-style-type: none"> <li>• bio_security_settings.ffd_security_level</li> </ul> <p>Updated Description for the keys:</p> <ul style="list-style-type: none"> <li>• controller_feedback.feedback_lines</li> <li>• controller_feedback.pre_check_panel_state</li> </ul>

Copyright © 2024, IDEMIA, All rights reserved. Reproduction in whole or in part in any form or medium without the express written permission of IDEMIA is prohibited.

# Access and Time Biometric Terminals Parameters Guide

[Main Page](#) [Modules](#) [Classes](#)

[Access and Time Biometric Terminals Parameters Guide](#) >

## Covered products

This guide consists of an entire list of parameters that are used to configure the features of Biometric Terminals.

VisionPass includes following variants

- VisionPass MIFARE® DESFIRE® (MD)
- VisionPass MIFARE® DESFIRE® PROX® iCLASS® (MDPI)

Terminal Series	Terminal Name	Contactless smartcard reader		
		iCLASS® Seos®	MIFARE® DESFire®	Prox®
VisionPass	VisionPass MD		Y	
	VisionPass MDPI	Y	Y	Y

MorphoWave® Compact includes following variants

- MorphoWave® Compact MIFARE® DESFIRE® (MD)
- MorphoWave® Compact MIFARE® DESFIRE® PROX® iCLASS® (MDPI)

Terminal Series	Terminal Name	Contactless smartcard reader		
		iCLASS® Seos®	MIFARE® DESFire®	Prox®

MorphoWave® Compact	MorphoWave® Compact MD		Y	
	MorphoWave® Compact MDPI	Y	Y	Y

MorphoWave® SP includes following variants

- MorphoWave® Simplified Profile MIFARE® DESFIRE® (MD)
- MorphoWave® Simplified Profile MIFARE® DESFIRE® PROX® iCLASS® (MDPI)

Terminal Series	Terminal Name	Contactless smartcard reader		
		iCLASS® Seos®	MIFARE® DESFire®	Prox®
MorphoWave® Simplified Profile	MorphoWave® Simplified Profile MD		Y	
	MorphoWave® Simplified Profile MDPI	Y	Y	Y

MorphoAccess® SIGMA Family includes following products

- SIGMA Series
- SIGMA Lite Series
- SIGMA Extreme Series

Terminal Series	Terminal Name	Biometrics	Contactless smartcard reader			Outdoor
			iCLASS® Seos®	MIFARE® DESFire®	Prox®	
MorphoAccess® SIGMA Series	MorphoAccess® SIGMA	Y				

	MorphoAccess® SIGMA WR	Y			Y
	MorphoAccess® SIGMA iCLASS®	Y	Y		
	MorphoAccess® SIGMA iCLASS® WR	Y	Y		Y
	MorphoAccess® SIGMA Multi	Y		Y	
	MorphoAccess® SIGMA Multi WR	Y		Y	Y
	MorphoAccess® SIGMA Prox®	Y			Y
	MorphoAccess® SIGMA Prox® WR	Y			Y
MorphoAccess® SIGMA Lite	MorphoAccess® SIGMA Lite WR	Y			Y
	MorphoAccess® SIGMA Lite iCLASS® WR	Y	Y		Y
	MorphoAccess® SIGMA Lite Multi WR	Y		Y	Y
	MorphoAccess® SIGMA Lite Prox® WR	Y			Y

MorphoAccess® SIGMA Lite+ Series	MorphoAccess® SIGMA Lite+ WR	Y					Y
	MorphoAccess® SIGMA Lite+ iCLASS® WR	Y	Y				Y
	MorphoAccess® SIGMA Lite+ Multi WR	Y		Y			Y
	MorphoAccess® SIGMA Lite+ Prox® WR	Y			Y		Y
	MorphoAccess® SIGMA Extreme iCLASS®	Y	Y				Y
MorphoAccess® SIGMA Extreme Series	MorphoAccess® SIGMA Extreme FFD iCLASS®	Y	Y				Y
	MorphoAccess® SIGMA Extreme Multi	Y		Y			Y
	MorphoAccess® SIGMA Extreme FFD Multi	Y		Y			Y
	MorphoAccess® SIGMA Extreme Prox®	Y			Y		Y
	MorphoAccess® SIGMA Extreme FFD Prox®	Y			Y		Y

VisionPass SP includes following variants

- VisionPass SP MIFARE® DESFIRE® (MD)

- VisionPass SP MIFARE® DESFIRE® iCLASS® (MDI)

Terminal Series	Terminal Name	Contactless smartcard reader		
		iCLASS® Seos®	MIFARE® DESFire®	Prox®
VisionPass SP	VisionPass SP MD		Y	
	VisionPass SP MDI	Y	Y	

Note: In this document, all references to VisionPass MDPI terminals are applicable to VisionPass MDPI-M Terminals too.

Note: In this document, all references to MorphoWave® Compact MDPI terminals are applicable to MorphoWave® Compact MDPI-M Terminals too.

Note: In this document, all references to MorphoWave® Simplified Profile MDPI terminals are applicable to MorphoWave® Simplified Profile MDPI-M Terminals too.

Copyright © 2024, IDEMIA, All rights reserved. Reproduction in whole or in part in any form or medium without the express written permission of IDEMIA is prohibited.

# Access and Time Biometric Terminals Parameters Guide

[Main Page](#)

**Modules**

[Classes](#)

# Modules

---

Here is a list of all modules:

- [Audio](#)
- [Authentication and Identification](#)
- [Biometric Security Settings](#)
- [Communication](#)
- [Contact Details](#)
- [Controller Feedback](#)
- [Dynamic Message and Font](#)
- [Error Log](#)
- [GPIO \(General Purpose Input Output\)](#)
- [Job Code](#)
- [LCD Configuration](#)
- [MMI Configuration](#)
- [NTP Service](#)
- [OSDP Protocol](#)
- [RTC Validation](#)
- [Remote Message](#)
- [SDAC \(Single Door Access Control\)](#)
- [SSCP Protocol](#)
- [Sensors](#)
- [Smart Card](#)
- [TCP client](#)
- [TOR Mode](#)
- [Tamper](#)
- [Terminal Information](#)
- [Threat Level](#)
- [Time and Attendance](#)
- [Transaction Log](#)
- [User Control Configuration](#)
- [Wiegand/Clock and data](#)

Copyright © 2024, IDEMIA, All rights reserved. Reproduction in whole or in part in any form or medium without the express written permission of IDEMIA is prohibited.

---

Generated by doxygen 1.7.6.1.

# Access and Time Biometric Terminals Parameters Guide

[Main Page](#)

[Modules](#)

[Classes](#)

Defines

## Audio

---

## **Detailed Description**

The audio feature covers parameters required for global terminal volume and accessibility permission of audio directories.

---

## Define Documentation

### audio.volume

Parameter for terminal global audio volume.

## Values

- 0 - 100 (**50** - Default)

### **audio.permission\_verify\_success**

Parameter to enable/disable playing of audio when user control verification is successful.

## Values

### SIGMA / SIGMA Extreme / MWC / VisionPass

- 0 - Disable (**0** - Default)
- 1 - Enable

### SIGMA Lite / SIGMA Lite+ / MWSP / VisionPass SP

Not applicable

## **audio.permission\_verify\_fail**

Parameter to enable/disable playing of audio when user control verification is failed.

## Values

### SIGMA / SIGMA Extreme / MWC / VisionPass

- 0 - Disable (**0** - Default)
- 1 - Enable

### SIGMA Lite / SIGMA Lite+ / MWSP / VisionPass SP

Not applicable

## **audio.permission\_message\_attention**

Parameter to enable/disable playing of audio when user's attention is required.

## Values

### SIGMA / SIGMA Extreme / MWC / VisionPass

- 0 - Disable (*0 - Default*)
- 1 - Enable

### SIGMA Lite / SIGMA Lite+ / MWSP / VisionPass SP

Not applicable

Copyright © 2024, IDEMIA, All rights reserved. Reproduction in whole or in part in any form or medium without the express written permission of IDEMIA is prohibited.

# Access and Time Biometric Terminals Parameters Guide

[Main Page](#)

[Modules](#)

[Classes](#)

Defines

## Authentication and Identification

---

## **Detailed Description**

This section covers the Authentication and Identification related parameters including biometric check attempts and timeout, PIN check attempts and timeout, identification statistics and the overall synchronization duration.

---

## Define Documentation

### **auth\_param.additional\_pin\_check\_nb\_attempt**

Parameter to set number of attempts for entering PIN during user control.

If parameter is "2", terminal allows to enter PIN second time after a first incorrect PIN entry.

## Values

**SIGMA / SIGMA Lite+ / SIGMA Extreme / MWC / VisionPass / VisionPass SP**

- 1 - 2 (**2 - Default**)

**SIGMA Lite / MWSP**

Not applicable

## auth\_param.additional\_pin\_check\_timeout

Parameter to define PIN check timeout.

When PIN is required, if it is not entered within configured time (timeout) then user control verification fails.

## Values

**SIGMA / SIGMA Lite+ / SIGMA Extreme / MWC / VisionPass / VisionPass SP**

- 3 - 15 (**10** - Default)

**SIGMA Lite / MWSP**

Not applicable



**Note:**

Timeout in seconds

### **auth\_param.additional\_bio\_check\_nb\_attempt**

Parameter to set number of attempts for biometric operations during user control.

Set this parameter to '1' to offer only one biometric operation.

Set this parameter to '2', to perform second biometric operation after a first incorrect identification/authentication attempt.

Set this parameter to '3', to perform second biometric operation after a first incorrect identification/authentication attempt. The main difference with the previous configuration is that the first identification is done on the MFU list (Most Frequent Users) instead of the full users list.

## Values

### SIGMA / SIGMA Extreme

- 1 - 3 (**2 - Default**)

### SIGMA Lite / SIGMA Lite+ / MWC / MWSP

- 1 - 2 (**2 - Default**)

### VisionPass

- 1 - 2 (**1 - Default**)

### VisionPass SP

Not applicable

## auth\_param.additional\_bio\_check\_timeout

Parameter to define Biometric check timeout.

If biometric authentication is not performed within configured time (timeout) then user control verification fails.

## Values

**SIGMA / SIGMA Lite / SIGMA Lite+ / SIGMA Extreme / MWC / MWSP / VisionPass SP**

- 2 - 60 (**5** - Default)

## VisionPass

- 2 - 60 (**10** - Default)



**Note:**

Timeout in seconds

### auth\_param.timed\_anti\_passback\_same\_user\_timeout

Anti-passback timeout: the same user will not be granted access on the same terminal during this period of time.

## Values

- 1 - 3600 (**5** - Default)

### SIGMA Lite / SIGMA Lite+



**Since:**  
MorphoAccess® 2.0

### SIGMA / SIGMA Extreme



**Since:**  
MorphoAccess® 3.0.0



**Warning:**  
The users' history for managing time-out is cleared if the terminal undergoes a power cycle.



**Note:**  
Timeout in seconds

### See also:

[`ucc.enable\_timed\_anti\_passback`](#)

## [`auth\_param.template\_type`](#)

Parameter to specify biometric template type for biometric data received from the host system. This parameter is only applicable when biometric template type is not specified as part of distant command received from the host system.

## Values

**SIGMA Lite / SIGMA Lite+ / SIGMA / SIGMA Extreme / MWC / MWSP**

Default value: 0 (pkcompV2).

values	Template Type	SIGMA / SIGMA Extreme / SIGMA Lite / SIGMA Lite+ Support	MWC / MWSP Support
-1	TLV format	Yes	Yes
0	pkcompv2	Yes	Yes
1	pkmat	Yes	Yes
2	ansi378_2004	Yes	Yes
3	iso19794_2_fmc_cs	Yes	Yes
4	iso19794_2_fmc_ns	Yes	Yes

5	iso19794_2_fmr	Yes	Yes
6	iso19794_2_fmc_cs_aa	Yes	Yes
7	minex_a	Yes	No
8	din_v66400_cs	Yes	No
9	din_v66400_cs_aa	Yes	No
10	multimodal	Yes	Yes
11	bioscrypt	Yes	No
12	pklite	Yes	Yes



**Since:**  
MorphoAccess® 3.4.0

## VisionPass / VisionPass SP

Not applicable

### auth\_param.qr\_code\_auth\_timeout

Parameter to define time during which same QR code will not be authenticated.

## Values

### VisionPass / MWSP

- 1 - 10 (**3** - Default)



#### Note:

Timeout in seconds

### SIGMA / SIGMA Lite / SIGMA Lite+ / SIGMA Extreme / MWC / VisionPass SP

Not applicable

## identify\_param.stats\_sync\_duration

Parameter to set the time interval for MFU(Most Frequent User) statistic synchronization.

When MFU is enabled using "auth\_param.additional\_bio\_check\_nb\_attempt" and a user's access through the biometric control is successful in that case an user's statistics are updated. But they are not saved on every control.

This parameter defines the time interval for automated synchronization of statistics after each operation.

Statistics are used by the terminal to build the MFU list, so it has to be saved regularly.

## Values

### SIGMA / SIGMA Extreme

- 1 - 24 (**1** - Default)

### SIGMA Lite / SIGMA Lite+ / MWC / VisionPass / MWSP / VisionPass SP

Not applicable

#### See also:

[auth\\_param.additional\\_bio\\_check\\_nb\\_attempt](#)



#### Note:

Interval in hours

## [identify\\_param.matching\\_strategy](#)

Parameter to set biometric matching strategy.

## Values

### MWC / MWSP

- 0 - standard\_strategy: Standard matching strategy (**0 - Default**)
- 1 - advanced\_strategy: Advanced matching strategy
- 2 - fastest\_strategy: Fastest matching strategy

### SIGMA / SIGMA Lite / SIGMA Lite+ / SIGMA Extreme / VisionPass / VisionPass SP

Not applicable

## identify\_param.auth\_trigger\_timeout

When multiple triggers are activated, including biometric trigger, there is a delay before to display an access denied result due to biometric identification failed. This delay allows to the unenrolled user to present his QR code or contactless card for example. This key configures this delay.

## Values

### VisionPass

- 1 - 10 (**3** - Default)



#### Note:

Timeout is in seconds.

**SIGMA / SIGMA Lite / SIGMA Lite+ / SIGMA Extreme / MWC / MWSP / VisionPass SP**

Not applicable

## identify\_param.detection\_area

Parameter to set the maximum length to detect a user.

## Values

### VisionPass SP

- 100
- 150
- 200 (**200** - Default)



**Note:**

length is in centimeter.

**SIGMA / SIGMA Lite / SIGMA Lite+ / SIGMA Extreme / MWC / MWSP / VisionPass**

Not applicable

### identify\_param.acquisition\_area

Parameter to set the maximum length to launch the biometric recognition on the detected user.

## Values

### VisionPass SP

- 50
- 70
- 100 (**100** - Default)



**Note:**

length is in centimeter.

### SIGMA / SIGMA Lite / SIGMA Lite+ / SIGMA Extreme / MWC / MWSP / VisionPass

Not applicable

## enroll.acquisition\_threshold

Parameter to set biometric quality or matching threshold during user enrolment.

## Values

### SIGMA / SIGMA Lite / SIGMA Lite+ / SIGMA Extreme

Quality threshold:

- 20 - 100 (**60** - Default)

### MWC / MWSP

Matching threshold:

- 0 - Standard quality threshold (**0** - Default)
- 1 - Secure quality threshold
- 2 - Very secure quality threshold

### VisionPass / VisionPass SP

Not applicable

## QR.hexa\_value

Parameter to configure terminal to interpret QR code data as hexadecimal value rather than a decimal value.

When enabled, the hexadecimal data read from the QR code is first converted into decimal value before being used as User ID.

## Values

### VisionPass / MWC / MWSP

- 0 - The data read from QR code will be interpreted as decimal value (**0 - Default**)
- 1 - The data read from QR code will be interpreted as hexadecimal value and then will be converted into decimal User ID

### SIGMA Lite / SIGMA Lite+ / SIGMA / SIGMA Extreme / VisionPass SP

Not applicable

Copyright © 2024, IDEMIA, All rights reserved. Reproduction in whole or in part in any form or medium without the express written permission of IDEMIA is prohibited.

# Access and Time Biometric Terminals Parameters Guide

[Main Page](#)

[Modules](#)

[Classes](#)

Defines

## Biometric Security Settings

---

## **Detailed Description**

This section covers parameters for biometric security configuration and threshold for matching.

---

## Define Documentation

### `bio_security_settings.matching_threshold`

Parameter to set the threshold for identification operations.

## Values

### SIGMA / SIGMA Lite / SIGMA Lite+ / SIGMA Extreme / MWC / MWSP

- 1 - 10 (**3** - Default)

### VisionPass / VisionPass SP

- 1,3,5,6,7,8,9 (**3** - Default)

Identification matching threshold values are detailed in the following table:

Parameter Value	Description
0	Lowest threshold value: the number of false rejects is very low, but the number of false acceptances is too high for a secure usage. It is strongly advised not to use this value, because the terminal becomes too tolerant.
1	FAR < 1 %
2	FAR < 0.5 %
3	FAR < 0.1% (Default value). Recommended value for physical

	access control applications using identification.
4	FAR < 0.05 %
5	FAR < 0.01 %
6	FAR < 0.001 %
7	FAR < 0.0001 %
8	FAR < 0.00001 %
9	FAR < 0.000001 %
10	Highest threshold value: the number of false acceptance is very low, but the number of false rejections is too high for the comfort of users. It is strongly advised not to use this value, because the terminal becomes too restrictive.

### **`bio_security_settings.authentication_matching_threshold`**

Parameter to set the threshold for authentication operations (biometric verification when user ID is provided separately).

## Values

**SIGMA / SIGMA Lite / SIGMA Lite+ / SIGMA Extreme / MWC / MWSP**

- 1 - 10 (**3 - Default**)



**Since:**

MorphoAccess® 4.6.0

MorphoWave® 1.5.0

**VisionPass / VisionPass SP**

- 1,3,5,6,7,8,9 (**3 - Default**)

Authentication matching threshold values are detailed in the following table:

<b>Parameter Value</b>	<b>Description</b>
1	FAR < 1 %
2	FAR < 0.5 %
3	FAR < 0.1% (Default value). Recommended value for physical access control applications using authentication.
4	FAR < 0.05 %

5	FAR < 0.01 %
6	FAR < 0.001 %
7	FAR < 0.0001 %
8	FAR < 0.00001 %
9	FAR < 0.000001 %
10	Highest threshold value: the number of false acceptance is very low, but the number of false rejections is too high for the comfort of users. It is strongly advised not to use this value, because the terminal becomes too restrictive.

### **bio\_security\_settingsffd\_security\_level**

Parameter to set Fake Finger Detection or Fake Face Detection threshold.

## Values

### SIGMA / SIGMA Lite / SIGMA Lite+ / MWC

- 0- disabled (**0 - Default**)
- 1- low
- 2- medium
- 3- high

#### Since:



MorphoAccess® 1.2.4 for MorphoAccess®  
SIGMA Lite+ and Lite terminals

### MWSP

- 0- disabled
- 1- low (**1 - Default**)
- 2- medium
- 3- high

### VisionPass / SIGMA Extreme

- 1- low (**1 - Default**)
- 2- medium
- 3- high

#### Note:



This key is only applicable for MorphoAccess® Extreme FFD terminals with integrated Fake Finger Detection (FFD) option. Should the upgraded MorphoAccess® EXTREME Terminal integrate Fake Finger Detection (FFD), this feature now requires a license MA\_FFD. Please contact your sales representative or IDEMIA support group.

## VisionPass SP

- 1- low (**1 - Default**)
- 2- medium
- 3- high
- 4- very high

### Note:



When the ffd security level is set to 4, biometric matching threshold is fixed to 9, by consequence the parameters **bio\_security\_settings.matching\_threshold** and **bio\_security\_settings.authentication\_matching\_threshold** have no effect.

## **bio\_security\_settings.intentional\_bio\_capture**

When enabled, the biometric data are captured only upon user's request, by pressing the dedicated key on the device screen.

## Values

### VisionPass / VisionPass SP

- 0- Biometric capture always enabled (**0 - Default**)
- 1- Biometric capture is enabled only on user's request.

### SIGMA / SIGMA Lite / SIGMA Lite+ / SIGMA Extreme / MWC / MWSP

Not applicable

Copyright © 2024, IDEMIA, All rights reserved. Reproduction in whole or in part in any form or medium without the express written permission of IDEMIA is prohibited.

# Access and Time Biometric Terminals Parameters Guide

[Main Page](#)

[Modules](#)

[Classes](#)

Defines

## Communication

---

## **Detailed Description**

Biometric terminals are able to communicate with distant systems such as controllers, videophone servers, etc. using various communication channels, viz. TCP (Ethernet/Wi-Fi™) and Serial Port. This section describes how to configure various communication channels.

---

## Define Documentation

### **comm\_channels\_state.disable\_IP**

This parameter allows to access the terminal over IPv4 protocol.

## Values

- 0 - IPv4 and IPv6 authorized (**0 - Default**)
- 1 - IPv4 disabled

## **comm\_channels\_state.TCP**

Starts/stops communication over TCP channel.

## **Values**

- 0 - Stops TCP communication channel
- 1 - Starts TCP communication channel

## On-Demand security mode

- 0 - Stops TCP communication channel
- 1 - Starts TCP communication channel (**1** - Default)

## Enforced Security

- 0 - Stops TCP communication channel (**0 - Default**)

### Note:



- In Enforced Security mode this key cannot be modified. Modification is only possible by switching to On-Demand security mode (using MorphoBioToolBox or by thrift command 'terminal\_set\_security\_state').
- When **comm\_channels\_state.TCP** and **in\_channel.SSL\_conn\_mode** are both enabled with the same port (**in\_channel.primary\_port** equals **in\_channel.secondary\_port**), then TLS channel is applied and clear TCP channel is stopped/closed.

### See also:

[\*\*in\\_channel.SSL\\_conn\\_mode\*\*](#), [\*\*in\\_channel.primary\\_port\*\*](#),  
[\*\*in\\_channel.secondary\\_port\*\*](#)

## comm\_channels\_state.web\_server

This parameter allows to access the terminal's webserver. The webserver is accessible from a standard web browser using the IP address of the terminal. Various parameters can be configured using Webserver interface.

## Values

- 0 - Terminal's webserver is disabled (*0 - Default*)
- 1 - Terminal's webserver is enabled

### Note:



In Enforced Security mode this key cannot be modified. Modification is only possible by switching to On-Demand security mode (using MorphoBioToolBox or by thrift command 'terminal\_set\_security\_state').

## comm\_channels\_state.USB\_script

This parameter allows to enable or disable the USB OTG port and USB script execution.

## Values

### SIGMA / SIGMA Lite / SIGMA Lite+ / SIGMA Extreme

- 0 - Disable USB (*0 - Default*)
- 1 - Enable Firmware upgrade via USB
- 2 - Enable configuration and Firmware upgrade via USB

### MWC / VisionPass / MWSP / VisionPass SP

- 0 - Disable USB OTG port and USB script execution (*0 - Default*)
- 1 - Enable USB OTG port and USB script execution

### SIGMA Lite / SIGMA Lite+



**Since:**  
MorphoAccess® 2.0

### SIGMA / SIGMA Extreme / MWC



**Since:**  
MorphoAccess® 3.0.0  
MorphoWave® 1.2.0



#### Note:

Please make sure to customize cypher key protecting USB script execution.

For MorphoWave® Compact, MorphoWave® SP, VisionPass and VisionPass SP this key is applicable only after reboot and, is only applicable in 'On demand security mode'.

For MorphoAccess® Sigma Lite, Sigma Lite+, SIGMA and Sigma Extreme terminals, value

2 is only applicable in 'On demand security mode'.

### **comm\_channels\_state.USB\_thrift**

This parameter allows to enable or disable the USB thrift execution.

## Values

### MWC / VisionPass

- 0 - Disable USB thrift execution (**0 - Default**)
- 1 - Enable USB thrift execution

### SIGMA / SIGMA Lite / SIGMA Lite+ / SIGMA Extreme / MWSP / VisionPass SP

Not applicable

#### Note:



USB channel for thrift is working only after terminal reboot. In Enforced Security mode this key can not be modified. Modification is only possible by switching to On-Demand security mode (using MorphoBioToolBox or by thrift command 'terminal\_set\_security\_state').

## comm\_channels\_state.serial

This parameter allows to start or stop the communication over Serial channel. Here, a remote host can connect to terminal using a RS422 or RS485 connection.

## Values

### SIGMA / SIGMA Extreme / MWC / VisionPass / MWSP / VisionPass SP

- 0 - Stops RS485/RS422 channel (**0 - Default**)
- 1 - Starts RS485/RS422 channel

### SIGMA Lite / SIGMA Lite+

- 0 - Stops RS485 channel (**0 - Default**)
- 1 - Starts RS485 channel

#### Note:



This parameter can be enabled, only if [`remote\_msg\_conf.send\_serial\_state`](#) is disable.

## [`comm\_channels\_state.upgrade\_firmware`](#)

This parameter allows to start or stop the Retrofit/Firmware upgrade port on the terminal.

## Values

**SIGMA Lite / SIGMA Lite+ / SIGMA / SIGMA Extreme / MWC / VisionPass**

- 0 - Retrofit port is closed (**0 - Default**)
- 1 - Retrofit port is open



**Since:**

MorphoAccess® 4.6.0

**MWSP / VisionPass SP**

Not applicable

## **comm\_channels\_state.cr\_file\_commit\_or\_cancel\_timeout**

When loading a certificate for TLS communication, a commit Thrift command, “file\_commit”, is required for the certificate to become valid. Otherwise, at the end of this configurable timeout, the certificate is revoked and previous certificate is reused.

## Values

- 30 - 300 (**60** - Default)



### Note:

Timeout in seconds

## comm\_channels\_state.legacy\_certificate

Parameter to manage the Openssl Legacy mode.

When this key is activated, Terminal accepts PKCS12 package encrypted with RC2 CBC 40.

## Values

### MWSP / VisionPass SP

- 0 - terminal doesn't authorise legacy certificate (**0 - Default**)
- 1 - terminal authorises legacy certificate

### SIGMA Lite / SIGMA Lite+ / SIGMA / SIGMA Extreme / MWC / VisionPass

Not applicable

#### Note:



This mode of encryption is deprecated, Idemia recommends to update your certificate to a state of art protection mode for your certificate.

The effect of this parameter change is applicable only after terminal reboot.

## in\_channel.SSL\_conn\_mode

Parameter to enable/disable SSL/TLS over TCP connections.

In case where **comm\_channels\_state.TCP** as well as **in\_channel.SSL\_conn\_mode** both are on, and also their ports (**in\_channel.primary\_port** and **in\_channel.secondary\_port** respectively) are equal, then SSL channel is applied and normal TCP channel is stopped/closed.

## Values

- 0 - SSL mode disabled
- 1 - SSL mode enabled (**1** - *Default*)

### Note:



In Enforced Security mode this key cannot be modified. Modification is only possible by switching to On-Demand security mode (using MorphoBioToolBox or by thrift command 'terminal\_set\_security\_state').

### See also:

[comm\\_channels\\_state.TCP](#), [in\\_channel.primary\\_port](#),  
[in\\_channel.secondary\\_port](#)

## in\_channel.profile\_id

Define SSL profile to be used for remote management.

## Values

- 0 - Use profile 0 (**0 - Default**)
- 1 - Use profile 1

### in\_channel.primary\_port

Define port number for remote management over TCP channel.

## Values

- 0 - 65535 (**11010** - Default)

### Note:



When `comm_channels_state.TCP` and `in_channel.SSL_conn_mode` are both enabled with the same port (`in_channel.primary_port` equals `in_channel.secondary_port`), then TLS channel is applied and clear TCP channel is stopped/closed.

### See also:

`comm_channels_state.TCP`,  
`in_channel.SSL_conn_mode`, `in_channel.secondary_port`

## in\_channel.secondary\_port

Define port number for remote management over SSL channel.

## Values

- 0 - 65535 (**11011** - Default)

### Note:



When `comm_channels_state.TCP` and `in_channel.SSL_conn_mode` are both enabled with the same port (`in_channel.primary_port` equals `in_channel.secondary_port`), then TLS channel is applied and clear TCP channel is stopped/closed.

The effect of this parameter change after a key reset is applicable only after terminal reboot.

### See also:

`comm_channels_state.TCP`,  
`in_channel.SSL_conn_mode`, `in_channel.primary_port`

## [misc.receive\\_state\\_machine\\_timeout](#)

Inter data timeout when receiving Thrift command. In case of timeout the connection is closed.

## Values

- 0 - 6000 (**3000** - Default) (A value of 0 indicates infinite timeout, i.e., the terminal waits indefinitely)



**Note:**

Timeout in milliseconds

## out\_channel.profile\_id

SSL profile to be used for remote message/ controller feedback over SSL channel.

## Values

- 0 - Use profile 0 (**0 - Default**)
- 1 - Use profile 1

### SSL\_profile\_0.name

Name for SSL profile 0.

## **Values**

- Any valid string (*for display purpose only*)

### **SSL\_profile\_0.protocol\_version**

Protocol version to be used for secure communication using profile 0.

## Values

### On-Demand security mode

**SIGMA Lite / SIGMA Lite+ / SIGMA / SIGMA Extreme / MWC / VisionPass**

- 0 - RFU
- 3 - sslv3 (SSLv3 is forced)
- 6 - tlsv1 (TLSv1 is forced)
- 9 - TLS version negotiation (TLSv1, TLSv1.1, TLSv1.2 are negotiated) (**9 - Default**)
- 12 - tlsv11 (TLSv1.1 is forced)
- 15 - tlsv12 (TLSv1.2 is forced)

### MWSP / VisionPass SP

- 0 - RFU
- 9 - TLS version negotiation (TLSv1.2, TLSv1.3 are negotiated) (**9 - Default**)
- 15 - tlsv12 (TLSv1.2 is forced)
- 18 - tlsv13 (TLSv1.3 is forced)

## Enforced Security

### SIGMA Lite / SIGMA Lite+ / SIGMA / SIGMA Extreme / MWC / VisionPass

- 0 - RFU
- 9 - TLS version negociation (TLSv1.2 only is negotiated) (**9 - Default**)
- 15 - tlsv12 (TLSv1.2 is forced)

### MWSP / VisionPass SP

- 0 - RFU
- 9 - TLS version negociation (TLSv1.2, TLSv1.3 are negotiated) (**9 - Default**)
- 15 - tlsv12 (TLSv1.2 is forced)
- 18 - tlsv13 (TLSv1.3 is forced)

#### Warning:

Since MorphoAccess® 1.2 firmware version



Due to SSLv3 "POODLE" flaw, SSLv3 is no more negotiated (i.e. when value is sslv23).

For compatibility purpose, SSLv3 could be used by setting parameter to sslv3 only. In this case, terminal accept only SSLv3, but is still vulnerable to "POODLE" flaw.

We strongly recommend upgrading to the last version of TLS.

### SSL\_profile\_0.cipher\_list

Bit field value containing list of supported cipher suites for SSL using profile 0.

## **Values**

**SIGMA / SIGMA Lite / SIGMA Lite+ / SIGMA Extreme / MWC / VisionPass**

## On-Demand security mode

- 0-14 bits of bitfield value allowed (**32767 - Default**)

## **Enforced Security**

- 11-14 bits of bitfield value allowed (**30720 - Default**)

## **MWSP / VisionPass SP**

## **Enforced Security/On-Demand Security mode**

- 11-15 bits of bitfield value allowed (**63488 - Default**)

### **Cipher suites list**

#### **VisionPass SP/ MWSP**

<b>Bit number</b>	<b>Cipher suite</b>	<b>tlsv1.2</b>	<b>tlsv1.3</b>
15	TLS-CHACHA20-POLY1305-SHA256	No	Yes
14	ECDHE-ECDSA-AES256-GCM-SHA384 TLS-AES-256-GCM-SHA384	Yes	Yes
13	ECDHE-RSA-AES256-GCM-SHA384 TLS-AES-256-GCM-SHA384	Yes	Yes

12	ECDHE- ECDSA- AES128-GCM- SHA256 TLS-AES-128- GCM-SHA256	Yes	Yes
11	ECDHE-RSA- AES128-GCM- SHA256 TLS-AES-128- GCM-SHA256	Yes	Yes

**SIGMA/ SIGMA Lite/ SIGMA Lite+/ SIGMA Extreme/ MWC/  
VisionPass**

Bit number	Cipher suite	sslv3	tlsv1	tlsv1.1	tlsv1.2
14	ECDHE- ECDSA- AES256- GCM- SHA384	No	No	No	Yes
13	ECDHE- RSA- AES256-	No	No	No	Yes

	GCM-SHA384				
12	ECDHE-ECDSA-AES128-GCM-SHA256	No	No	No	Yes
11	ECDHE-RSA-AES128-GCM-SHA256	No	No	No	Yes
10	ECDHE-RSA-AES256-SHA	Yes	Yes	Yes	Yes
9	ECDHE-RSA-AES128-SHA	Yes	Yes	Yes	Yes
8	ECDHE-ECDSA-AES128-SHA	Yes	Yes	Yes	Yes

	ECDH- ECDSA- AES128- SHA				
7	ECDHE- ECDSA- AES128- SHA256 ECDH- ECDSA- AES128- SHA256	No	No	No	Yes
6	ECDHE- ECDSA- AES128- GCM- SHA256 ECDH- ECDSA- AES128- GCM- SHA256	No	No	No	Yes
5	ECDHE- ECDSA- AES256- SHA ECDH-	Yes	Yes	Yes	Yes

	ECDSA-AES256-SHA				
4	AES128-GCM-SHA256	No	No	No	Yes
3	AES256-SHA256	No	No	No	Yes
2	AES128-SHA256	No	No	No	Yes
1	AES256-SHA	Yes	Yes	Yes	Yes
0	AES128-SHA	Yes	Yes	Yes	Yes

### SSL\_profile\_1.name

Name for SSL profile 1.

## **Values**

- Any valid string (*for display purpose only*)

### **SSL\_profile\_1.protocol\_version**

Protocol version to be used for secure communication using profile 1.

## Values

### On-Demand security mode

**SIGMA Lite / SIGMA Lite+ / SIGMA / SIGMA Extreme / MWC / VisionPass**

- 0 - RFU
- 3 - sslv3 (SSLv3 is forced)
- 6 - tlsv1 (TLSv1 is forced)
- 9 - TLS version negotiation (TLSv1, TLSv1.1, TLSv1.2 are negotiated) (**9 - Default**)
- 12 - tlsv11 (TLSv1.1 is forced)
- 15 - tlsv12 (TLSv1.2 is forced)

### MWSP / VisionPass SP

- 0 - RFU
- 9 - TLS version negotiation (TLSv1.2, TLSv1.3 are negotiated) (**9 - Default**)
- 15 - tlsv12 (TLSv1.2 is forced)
- 18 - tlsv13 (TLSv1.3 is forced)

## Enforced Security

### SIGMA Lite / SIGMA Lite+ / SIGMA / SIGMA Extreme / MWC / VisionPass

- 0 - RFU
- 9 - TLS version negociation (TLSv1.2 only is negotiated) (**9 - Default**)
- 15 - tlsv12 (TLSv1.2 is forced)

### MWSP / VisionPass SP

- 0 - RFU
- 9 - TLS version negociation (TLSv1.2, TLSv1.3 are negotiated) (**9 - Default**)
- 15 - tlsv12 (TLSv1.2 is forced)
- 18 - tlsv13 (TLSv1.3 is forced)

#### Warning:

Since MorphoAccess® 1.2 firmware version



Due to SSLv3 "POODLE" flaw, SSLv3 is no more negotiated (i.e. when value is sslv23).

For compatibility purpose, SSLv3 could be used by setting parameter to sslv3 only. In this case, terminal accept only SSLv3, but is still vulnerable to "POODLE" flaw.

We strongly recommend to upgrade to the last version of TLS.

### SSL\_profile\_1.cipher\_list

Bit field value containing list of supported cipher suites for SSL using profile 1.

## **Values**

**SIGMA / SIGMA Lite / SIGMA Lite+ / SIGMA Extreme / MWC / VisionPass**

## On-Demand security mode

- 0-14 bits of bitfield value allowed (**32767 - Default**)

## **Enforced Security**

- 11-14 bits of bitfield value allowed (**30720 - Default**)

## **MWSP / VisionPass SP**

## **Enforced Security/On-Demand Security mode**

- 11-15 bits of bitfield value allowed (**63488 - Default**)

### **Cipher suites list**

#### **VisionPass SP/ MWSP**

<b>Bit number</b>	<b>Cipher suite</b>	<b>tlsv1.2</b>	<b>tlsv1.3</b>
15	TLS-CHACHA20-POLY1305-SHA256	No	Yes
14	ECDHE-ECDSA-AES256-GCM-SHA384 TLS-AES-256-GCM-SHA384	Yes	Yes
13	ECDHE-RSA-AES256-GCM-SHA384 TLS-AES-256-GCM-SHA384	Yes	Yes

12	ECDHE- ECDSA- AES128-GCM- SHA256 TLS-AES-128- GCM-SHA256	Yes	Yes
11	ECDHE-RSA- AES128-GCM- SHA256 TLS-AES-128- GCM-SHA256	Yes	Yes

**SIGMA/ SIGMA Lite/ SIGMA Lite+/ SIGMA Extreme/ MWC/  
VisionPass**

Bit number	Cipher suite	sslv3	tlsv1	tlsv1.1	tlsv1.2
14	ECDHE- ECDSA- AES256- GCM- SHA384	No	No	No	Yes
13	ECDHE- RSA- AES256-	No	No	No	Yes

	GCM-SHA384				
12	ECDHE-ECDSA-AES128-GCM-SHA256	No	No	No	Yes
11	ECDHE-RSA-AES128-GCM-SHA256	No	No	No	Yes
10	ECDHE-RSA-AES256-SHA	Yes	Yes	Yes	Yes
9	ECDHE-RSA-AES128-SHA	Yes	Yes	Yes	Yes
8	ECDHE-ECDSA-AES128-SHA	Yes	Yes	Yes	Yes

	ECDH- ECDSA- AES128- SHA				
7	ECDHE- ECDSA- AES128- SHA256 ECDH- ECDSA- AES128- SHA256	No	No	No	Yes
6	ECDHE- ECDSA- AES128- GCM- SHA256 ECDH- ECDSA- AES128- GCM- SHA256	No	No	No	Yes
5	ECDHE- ECDSA- AES256- SHA ECDH-	Yes	Yes	Yes	Yes

	ECDSA-AES256-SHA				
4	AES128-GCM-SHA256	No	No	No	Yes
3	AES256-SHA256	No	No	No	Yes
2	AES128-SHA256	No	No	No	Yes
1	AES256-SHA	Yes	Yes	Yes	Yes
0	AES128-SHA	Yes	Yes	Yes	Yes

## ip\_restraining.mode

Parameter to enable or disable IP restrictions. If this parameter is enabled, then terminal authorizes only restricted number of IP addresses for distant command input connections. The authorized IP addresses can be set using authorized\_IP\_add or authorized\_IP\_add\_range Thrift commands (or with MorphoBioToolBox).

## Values

- 0 - Disabled (*0 - Default*)
- 1 - Enabled

Copyright © 2024, IDEMIA, All rights reserved. Reproduction in whole or in part in any form or medium without the express written permission of IDEMIA is prohibited.

# Access and Time Biometric Terminals Parameters Guide

[Main Page](#)

[Modules](#)

[Classes](#)

Defines

## Contact Details

---

## **Detailed Description**

This section allows to configure the contact information of the company. This information is displayed on Contact Details page of Webserver.

---

## Define Documentation

### **contact\_info.web**

Parameter to configure website address of the company.

The website address configured in this parameter is automatically reflected in the webserver's 'Contact Us' page.

For example: <https://biometricdevices.idemia.com>

## Values

- Any valid string (*for display purpose only*)

### **contact\_info.hotline\_mail**

Parameter to configure hotline email address of the company.

The email address configured in this parameter is automatically reflected in the webserver's 'Contact Us' page.

For example: [hotline.biometrics@idemia.com](mailto:hotline.biometrics@idemia.com)

## Values

- Any valid string (*for display purpose only*)

### **contact\_info.hotline\_number**

Parameter to configure contact phone number of the company.

The contact number configured in this parameter is automatically reflected in the webserver's 'Contact Us' page.

## Values

- Any valid string (*for display purpose only*)

### **contact\_info.HO\_address**

Parameter to configure address of the company head office.

The address configured in this parameter is automatically reflected in the webserver's 'Contact Us' page.

For example: 2, Place Samuel de Champlain, 92400 Courbevoie,  
FRANCE

## Values

- Any valid string (*for display purpose only*)

Copyright © 2024, IDEMIA, All rights reserved. Reproduction in whole or in part in any form or medium without the express written permission of IDEMIA is prohibited.

---

Generated by doxygen 1.7.6.1.

# Access and Time Biometric Terminals Parameters Guide

[Main Page](#)

[Modules](#)

[Classes](#)

Defines

## Controller Feedback

---

## **Detailed Description**

This section contains parameter keys related to Controller Feedback.

---

## Define Documentation

### `controller_feedback.panel_mode`

Parameter to enable/disable "PIN requested" feedback.

## Values

### SIGMA / SIGMA Lite+ / SIGMA Extreme / MWC / VisionPass / VisionPass SP

- 1 - Used input pin can define "Access granted", "Access denied" feedback (**1 - Default**)
- 2 - Used input pin can define "Access granted", "Access denied", "PIN requested" feedback

### SIGMA Lite / MWSP

Not applicable

#### Note:

To use the panel mode 2:



- **remote\_msg\_conf.feedback\_interface** shall be set to **input pins feedback**
- **controller\_feedback.feedback\_lines** shall be set to **pulse mode feedback**

### **controller\_feedback.feedback\_lines**

Parameter to set the mode of feedback to be used for controller feedback.

## Values

### SIGMA Lite / SIGMA / SIGMA Lite+ / SIGMA Extreme / MWC / VisionPass

- 1 - pulse mode feedback (**1 - Default**)
- 2 - level mode feedback

### MWSP / VisionPass SP

- 1 - pulse mode feedback
- 2 - level mode feedback (**2 - Default**)

#### Note:

When **level mode feedback** is used,

- "PIN requested" feedback is not possible (setting **controller\_feedback.panel\_mode** to 2 does not affect the terminal behavior)
- Result for level mode feedback is defined as follows (also depends on **controller\_feedback.pre\_check\_panel\_state**)



LED2 state	LED1 state	Result
High	Low	Access Granted
Low	X (shall not be considered)	Access Denied
High	High	Access Denied or Timeout

### **controller\_feedback.panel\_timeout**

Parameter to set timeout for controller feedback.

The behavior of the terminal after timeout is defined by the parameter  
**controller\_feedback.timeout\_as\_reject**

## Values

- 1000 - 30000 (**3000** - Default)



**Note:**

Timeout in milliseconds.

## `controller_feedback.pre_check_panel_state`

Parameter to set precheck panel state schedule for controller feedback via input pins.(in case of level mode feedback only) If this parameter is enabled, the terminal check the state of LED1 and LED2 first, and wait for the trigger only if both states are high.

## Values

- 0 - 1 (**0** - Default)

<b>LED2 Initial state</b>	<b>LED2 New state</b>	<b>LED1 Initial state</b>	<b>LED1 New state</b>	<b>Result <code>pre_check_panel_state</code> = 0</b>	<b>Result <code>pre_check_panel_state</code> = 1</b>
High	High	Low	Low	Access Denied or Timeout	Access Granted
High	High	Low	High	Access Denied or Timeout	Access Granted
High	High	High	Low	Access Granted	Access Granted
High	High	High	High	Timeout	Timeout
Low	Low	Low	Low	Access Denied	Access Denied
Low	Low	Low	High	Access Denied	Access Denied
Low	Low	High	Low	Access Denied	Access Denied
Low	Low	High	High	Access Denied	Access Denied
Low	High	Low	Low	Access Granted	Access Denied
Low	High	Low	High	Access Denied or Timeout	Access Denied
Low	High	High	Low	Access Granted	Access Denied
Low	High	High	High	Access Denied or Timeout	Access Denied

High	Low	Low	Low	Access Denied	Access Granted
High	Low	Low	High	Access Denied	Access Granted
High	Low	High	Low	Access Denied	Access Denied
High	Low	High	High	Access Denied	Access Denied



**Since:**  
MorphoAccess® 1.2.4

#### [controller\\_feedback.granted\\_pulse\\_width](#)

Pulse width to detect "Access granted" input pin feedback (used only in case of pulse mode feedback)

## Values

### SIGMA Lite / SIGMA / SIGMA Lite+ / SIGMA Extreme / MWC / VisionPass

- Custom pulse 50 - 1000 (**100** - Default)
- High pulse 0 (and `controller_feedback.granted_pulse_interval` shall be set to 1)
- Low pulse 1 (and `controller_feedback.granted_pulse_interval` shall be set to 0)

### MWSP / VisionPass SP

Not applicable



#### Note:

Width in milliseconds

### `controller_feedback.granted_pulse_interval`

Pulse interval to detect "Access granted" input pin feedback (used only in case of pulse mode feedback)

## Values

### SIGMA Lite / SIGMA / SIGMA Lite+ / SIGMA Extreme / MWC / VisionPass

- Custom pulse 50 - 1000 (**100** - Default)
- High pulse 1 (and `controller_feedback.granted_pulse_width` shall be set to 0)
- Low pulse 0 (and `controller_feedback.granted_pulse_width` shall be set to 1)

### MWSP / VisionPass SP

Not applicable



**Note:**

Interval in milliseconds

### `controller_feedback.denied_pulse_width`

Pulse width to detect "Access denied" input pin feedback (used only in case of pulse mode feedback)

## Values

SIGMA Lite / SIGMA / SIGMA Lite+ / SIGMA Extreme / MWC / VisionPass

- Custom pulse 50 - 1000 (**200** - Default)
- High pulse 0 (and **controller\_feedback.denied\_pulse\_interval** shall be set to 1)
- Low pulse 1 (and **controller\_feedback.denied\_pulse\_interval** shall be set to 0)
- None(timeout) -1 (and **controller\_feedback.denied\_pulse\_interval** shall be set to -1)

MWSP / VisionPass SP

Not applicable



**Note:**

Pulse in milliseconds

### **controller\_feedback.denied\_pulse\_interval**

Pulse interval to detect "Access denied" input pin feedback (used only in case of pulse mode feedback)

## Values

SIGMA Lite / SIGMA / SIGMA Lite+ / SIGMA Extreme / MWC / VisionPass

- Custom pulse 50 - 1000 (**200** - Default)
- High pulse 1 (and **controller\_feedback.denied\_pulse\_width** shall be set to 0)
- Low pulse 0 (and **controller\_feedback.denied\_pulse\_width** shall be set to 1)
- None(timeout) -1 (and **controller\_feedback.denied\_pulse\_width** shall be set to -1)

MWSP / VisionPass SP

Not applicable



**Note:**

Interval in milliseconds

### **controller\_feedback.PIN\_pulse\_width**

Pulse width to detect "PIN requested" input pin feedback (used only in case of pulse mode feedback)

## Values

### SIGMA / SIGMA Lite+ / SIGMA Extreme / MWC / VisionPass

- Custom pulse 50 - 1000 (**300** - Default)
- High pulse 0 (and **controller\_feedback.PIN\_pulse\_interval** shall be set to 1)
- Low pulse 1 (and **controller\_feedback.PIN\_pulse\_interval** shall be set to 0)

### SIGMA Lite / MWSP / VisionPass SP

Not applicable



**Note:**

Pulse in milliseconds

### **controller\_feedback.PIN\_pulse\_interval**

Pulse interval to detect "PIN requested" input pin feedback (used only in case of pulse mode feedback)

## Values

### SIGMA / SIGMA Lite+ / SIGMA Extreme / MWC / VisionPass

- Custom pulse 50 - 1000 (**300** - Default)
- High pulse 1 (and **controller\_feedback.PIN\_pulse\_width** shall be set to 0)
- Low pulse 0 (and **controller\_feedback.PIN\_pulse\_width** shall be set to 1)

### SIGMA Lite / MWSP / VisionPass SP

Not applicable



**Note:**

Interval in milliseconds

### **controller\_feedback.timeout\_as\_reject**

Parameter to set terminal's policy in case of timeout on feedback.

## Values

- 0 - Terminal denies the access, controller feedback attempt is logged with timeout error in transaction log
- 1 - Terminal denies the access, controller feedback attempt is logged with reject error in transaction log (**1 - Default**)

## controller\_feedback.keypad\_passthru\_timeout

Keypad passthrough timeout is used:

- as timeout to enter PIN for input pin controller feedback operation

## Values

**SIGMA / SIGMA Lite+ / SIGMA Extreme / MWC / VisionPass / VisionPass SP**

- 5 - 16 (**10** - Default)

**SIGMA Lite / MWSP**

Not applicable



**Note:**

Timeout in seconds

Copyright © 2024, IDEMIA, All rights reserved. Reproduction in whole or in part in any form or medium without the express written permission of IDEMIA is prohibited.

# Access and Time Biometric Terminals Parameters Guide

[Main Page](#)

[Modules](#)

[Classes](#)

Defines

## Dynamic Message and Font

## **Detailed Description**

Dynamic message is a feature by which customized texts/ images can be displayed to a particular user upon successful authentication/ identification. The dynamic message mode and its timeout can be configured.

---

## Define Documentation

### dynamic\_message.mode

Parameter to configure dynamic message mode.

Each bit of the following 0-11 bitfield represents Dynamic message mode for associated user control result. To Enable (1) / Disable (0) the Dynamic message for the user control result, the respective bit value must be set.

## Values

bitfield value, allowed range 0 - 65535 (**0** - Default)

### SIGMA / SIGMA Extreme / MWC / VisionPass / VisionPass SP

- bit 0: user control successful
- bit 1: biometric mismatch
- bit 2: pin mismatch
- bit 3: control timed out
- bit 4: rejected by schedule
- bit 5: temp validity expired
- bit 6: user not in white list
- bit 7: banned card listed
- bit 8: face not detected (Applicable to MASigma and Extreme only)
- bit 9: controller feedback action
- bit 10: job code check failure
- bit 11: user rule check failure
- bit 12: user timed anti passback
- bit 13: Reserved, should be set to 0
- bit 14: Reserved, should be set to 0
- bit 15: Reserved, should be set to 0

### SIGMA Lite / SIGMA Lite+ / MWSP

Not applicable

## dynamic\_message.timeout

Parameter to set duration for dynamic message display.

## Values

**SIGMA / SIGMA Extreme / MWC / VisionPass / VisionPass SP**

- 0 - 20 (**3 - Default**)

**SIGMA Lite / SIGMA Lite+ / MWSP**

Not applicable



**Note:**

Timeout in seconds

## font.size

Parameter to set the font size for access granted/access denied/dynamic messages.

## Values

### SIGMA

- 10 - 40 (**27** - Default)

### SIGMA Extreme

- 10 - 32 (**17** - Default)

### SIGMA Lite+

- 10 - 42 (**16** - Default)

### SIGMA / SIGMA Lite+ / SIGMA Extreme



Since:

MorphoAccess® 4.6.0

### MWC / VisionPass

- 10 - 32 (**25** - Default)



Since:

MorphoWave® Version 1.5.0

### VisionPass SP

- 10 - 32 (**30** - Default)

### SIGMA Lite / MWSP

Not applicable

## Display\_text.color

Parameter to set text color for the user control text, dynamic message text and OSDP text.

The value is an RGB color code.

## Values

### VisionPass SP

- 000000 - FFFFFF(430099 - *Default*)

**SIGMA / SIGMA Lite / SIGMA Lite+ / SIGMA Extreme / MWC / VisionPass / MWSP**

Not applicable

Copyright © 2024, IDEMIA, All rights reserved. Reproduction in whole or in part in any form or medium without the express written permission of IDEMIA is prohibited.

# Access and Time Biometric Terminals Parameters Guide

[Main Page](#)

[Modules](#)

[Classes](#)

Defines

## Error Log

---

## **Detailed Description**

This section covers parameters concerning logging of errors that occurred in terminal.

---

## Define Documentation

### **error\_log.enabled**

Parameter to enable/disable the error logging.

## Values

- 0 - Disabled (*0 - Default*)
- 1 - Enabled

## `error_log.osdp_debug_level`

Parameter to set OSDP error logging level.

## Values

- 0 - Fatal
- 1 - Alert
- 2 - Critical
- 3 - Error
- 4 - Warning
- 5 - Notice
- 6 - Info
- 7 - Debug (**7 - Default**)
- 8 - Trace

**Note:**



The effect of this parameter change is applicable only after terminal reboot.

### **error\_log.debug\_level**

Parameter to set error logging level.

## Values

- 0 - Fatal
- 1 - Alert
- 2 - Critical
- 3 - Error
- 4 - Warning
- 5 - Notice
- 6 - Info
- 7 - Debug (**7 - Default**)
- 8 - Trace

**Note:**



The effect of this parameter change is applicable only after terminal reboot.

### **error\_log.system\_file\_size**

Parameter to enable system logs and set the size of log file.

## Values

- 0 - 1024 (*0 - Default*)

## SIGMA Lite / SIGMA Lite+ / SIGMA / SIGMA Extreme

Not applicable

## `error_log.core_app_file_size`

Parameter to configure core app file size.

## Values

**MWC / VisionPass / MWSP / VisionPass SP**

- 5 - 100 (**5 - Default**)

**SIGMA Lite / SIGMA Lite+ / SIGMA / SIGMA Extreme**

Not applicable

## **error\_log\_sensor.enabled**

Parameter to enable/disable the sensor error logging.

## Values

- 0 - Disabled (**0 - Default**)
- 1 - Enabled

## SIGMA / SIGMA Extreme



**Since:**

MorphoAccess® 1.5.0

## SIGMA Lite / SIGMA Lite+



**Since:**

MorphoAccess® 3.0.0



**Note:**

Sensor errors will be logged if  
**error\_log\_sensor.enabled = 1** and  
**error\_log.enabled = 1**.

## error\_log\_sensor.modules

To be set only on hotline request.

## Values

**SIGMA Lite / SIGMA Lite+ / SIGMA / SIGMA Extreme / MWC / MWSP**

- 0 - 65535 (**1 - Default**)

**SIGMA / SIGMA Extreme**



**Since:**

MorphoAccess® 1.5.0

**SIGMA Lite / SIGMA Lite+**



**Since:**

MorphoAccess® 3.0.0

**VisionPass / VisionPass SP**

Not applicable



**Note:**

The effect of this parameter change is applicable only after terminal reboot.

# Access and Time Biometric Terminals Parameters Guide

[Main Page](#)

[Modules](#)

[Classes](#)

Defines

## **GPIO (General Purpose Input Output)**

## Detailed Description

Terminal's GPIO can be used for several purposes:

- Output pins can be used to send events to an external controller
- Input pins can be used to receive actions from external controller, to monitor a door or to receive threat level update from external controller.

General Purpose Input Output (GPIO) general mode is used to send events or receive actions from external device. By default, this mode is enabled.

GPIO pins consist below:

- GPO (General Purpose Output) have 3 output pins available, i.e. Pin 0, 1 and 2. Biometric terminals can send signals simultaneously through multiple configured GPO pins.
- GPI (General Purpose Input) have 3 input pins available, i.e. Pin 0, 1 and 2. The GPI pins can be configured to trigger an action on the Biometric terminal from distant system, when set as active (low and/or high).

Only one of either SDAC mode, GPIO mode, or Threat Level mode can be activated at a single point of time.

**Note:**



GPIO and WIEGAND values are modified during boot sequence. However, they are restored to their original values upon bootup completion.

## Define Documentation

### gpio.func\_mode

Configure for GPIO functional mode.

## Values

- 0 - GPIO general mode (*0 - Default*)
- 1 - Threat Level mode
- 2 - SDAC mode (Door monitoring)

### Note:



To set `gpio.func_mode` to 1 (Threat Level mode), `gpio.threat_level_mode` should be set to 0 (Threat Level is based on the GPI input pins status). Else value is rejected.

## `gpio.gpo0_default_state`

Configure state of GPO 0 in idle state.

## Values

- 0 - Low state (**0** - Default)
- 1 - High state

### gpio.gpo1\_default\_state

Configure state of GPO 1 in idle state.

## Values

- 0 - Low state (**0** - Default)
- 1 - High state

### gpio.gpo2\_default\_state

Configure state of GPO 2 in idle state.

## Values

### SIGMA / SIGMA Extreme / MWC / VisionPass / MWSP / VisionPass SP

- 0 - Low state (**0** - Default)
- 1 - High state

### SIGMA Lite / SIGMA Lite+

Not applicable

## gpio.gpi\_table\_gpi\_0

Parameter to set an action to be performed when GPI pin 0 is triggered.

**gpio.func\_mode** shall be configured to GPIO general mode

## Values

- 0 - No action (*0 - Default*)
- 4 - Delete Users database
- 5 - Reboot terminal
- 6 - Play Alarm MMI

See also:

[gpio.func\\_mode](#)

## [gpio.gpi\\_table\\_gpi\\_1](#)

Parameter to set an action to be performed when GPI pin 1 is triggered.

[gpio.func\\_mode](#) shall be configured to GPIO general mode

## Values

- 0 - No action (*0 - Default*)
- 4 - Delete Users database
- 5 - Reboot terminal
- 6 - Play Alarm

See also:

[gpio.func\\_mode](#)

## [gpio.gpi\\_table\\_gpi\\_2](#)

Parameter to set an action to be performed when GPI pin 2 is triggered.

[gpio.func\\_mode](#) shall be configured to GPIO general mode

## Values

### SIGMA / SIGMA Extreme / MWC / VisionPass / MWSP / VisionPass SP

- 0 - No action (*0 - Default*)
- 4 - Delete Users database
- 5 - Reboot terminal
- 6 - Play Alarm

### SIGMA Lite / SIGMA Lite+

Not applicable

#### See also:

[gpio.func\\_mode](#)

## gpio.gpo\_0\_duration

Duration for which GPO 0 is toggled on event(s).

## Values

- 0 - 16383 (**600** - Default)



### Note:

Duration in milliseconds

## gpio.gpo\_1\_duration

Duration for which GPO 1 is toggled on event(s).

## Values

- 0 - 16383 (**600** - Default)



### Note:

Duration in milliseconds

## gpio.gpo\_2\_duration

Duration for which GPO 2 is toggled on event(s).

## Values

**SIGMA / SIGMA Extreme / MWC / VisionPass / MWSP / VisionPass SP**

- 0 - 16383 (**600** - Default)

**SIGMA Lite / SIGMA Lite+**

Not applicable



**Note:**

Duration in milliseconds

## **gpio.gpi\_duration**

Minimum duration for which GPI should be triggered to consider it as a valid external event.

**gpio.func\_mode** shall be configured to GPIO general mode.

## Values

- 0 - 16383 (**200** - Default)



**Note:**

Duration in milliseconds

### See also:

[\*\*gpio.func\\_mode\*\*](#)

## [\*\*gpio.gpi\\_active\\_level\*\*](#)

Configure state of GPI in idle state.

**gpio.func\_mode** shall be configured to GPIO general mode.

## Values

- 0 - Low state
- 1 - High state (**1** - *Default*)

See also:

[gpio.func\\_mode](#)

Copyright © 2024, IDEMIA, All rights reserved. Reproduction in whole or in part in any form or medium without the express written permission of IDEMIA is prohibited.

# Access and Time Biometric Terminals Parameters Guide

[Main Page](#)

[Modules](#)

[Classes](#)

Defines

## Job Code

---

## **Detailed Description**

Job code verification is meant for keeping track of a user's job. If a user is authenticated / identified, then terminal prompts user to enter job code. Access is granted only on successful job code verification.

The Terminal can hold up to 128 job code lists.

Total 512 job codes per list are allowed.

A job code should be between 0 to 4294967295 [i.e.  $((2^{32})-1)$ ].

---

## Define Documentation

### jobcode.activate

Parameter to enable/disable jobcode check.

## Values

### SIGMA / SIGMA Extreme / MWC / VisionPass / VisionPass SP

- 0 - Job code check disabled (**0** - Default)
- 1 - Job code check enabled

### SIGMA Lite / SIGMA Lite+ / MWSP

Not applicable

## jobcode.timeout

Parameter to set duration within which the user has to input jobcode.

If user fails to enter jobcode and time exceeds, then access is denied.

## Values

### SIGMA / SIGMA Extreme / MWC / VisionPass / VisionPass SP

- 0 - 15 (**10** - Default)

### SIGMA Lite / SIGMA Lite+ / MWSP

Not applicable



#### Note:

Timeout in seconds

Copyright © 2024, IDEMIA, All rights reserved. Reproduction in whole or in part in any form or medium without the express written permission of IDEMIA is prohibited.

# Access and Time Biometric Terminals Parameters Guide

[Main Page](#)

[Modules](#)

[Classes](#)

Defines

## LCD Configuration

---

## **Detailed Description**

This section covers LCD related parameters like brightness, idle screen, display clock type, screen idle mode, video play etc.

---

## Define Documentation

### **LCD\_configuration.idle\_screen\_status**

Parameter to enable or disable LCD Idle screen mode.

## Values

**SIGMA / SIGMA Lite+ / SIGMA Extreme / MWC / VisionPass / VisionPass SP**

- 0 - Idle screen mode disabled
- 1 - Idle screen mode enabled. (**1 - Default**)

**SIGMA Lite / MWSP**

Not applicable

**Note:**



For MorphoWave® Compact products, this parameter deactivates the biometric sensor lightning 30s after starting of lightning.

For other applicable products, this parameter activates the playing of a video after [\*\*LCD\\_configuration.idle\\_screen\\_timeout\*\*](#).

**See also:**

[\*\*LCD\\_configuration.idle\\_video\\_timeout\*\*](#)

[\*\*LCD\\_configuration.idle\\_screen\\_timeout\*\*](#)

## [\*\*LCD\\_configuration.touch\\_sound\*\*](#)

Parameter to enable/disable touch sounds.

## Values

### SIGMA / SIGMA Lite+ / SIGMA Extreme

- 0 - Disable Touch Sounds (**0** - Default)
- 1 - Enable Touch Sounds



**Since:**

MorphoAccess® 4.6.0

### SIGMA Lite / MWC / VisionPass / MWSP / VisionPass SP

Not applicable

#### Note:



The buzzer sound associated to the touch screen will not be played or will be immediately stopped when another buzzer sound is requested (tamper buzzer, OSDP buzzer, ..)..

## LCD\_configuration.enable\_azerty\_kbd

Parameter to set the keyboard type.

## Values

### SIGMA

- 0 - QWERTY keyboard (**0 - Default**)
- 1 - AZERTY keyboard
- 2 - CYRILLIC keyboard



**Since:**

MorphoAccess® 4.3.0

### SIGMA Extreme / MWC / VisionPass / VisionPass SP

- 0/1 - ALPHABETIC keyboard (**0 - Default**)
- 2 - CYRILLIC keyboard



**Since:**

MorphoAccess® 4.3.1

### SIGMA Lite / SIGMA Lite+ / MWSP

Not applicable

## LCD\_configuration.low\_power\_disable\_sensor

Parameter to enable or disable biometric sensor when the terminal is in low consumption mode.

When sensor is disabled, biometric identification cannot be performed.

## Values

### SIGMA / SIGMA Lite+ / SIGMA Extreme

- 0 - Enable sensor in low consumption mode
- 1 - Disable sensor in low consumption mode (**1 - Default**)

### SIGMA Lite / MWC / VisionPass / MWSP / VisionPass SP

Not applicable

## LCD\_configuration.idle\_screen\_timeout

Parameter to set the idle duration. If no action is performed during this duration then screen will play a video.

For MorphoWave® Compact products, this parameter sets the duration to wait before entering standby mode.

## Values

### SIGMA / SIGMA Lite+ / SIGMA Extreme

- 1 - 3600 (**60** - Default)

### MWC / VisionPass / VisionPass SP

- 30 - 3600 (**60** - Default)

### SIGMA Lite / MWSP

Not applicable



#### Note:

Timeout in seconds

#### See also:

[LCD\\_configuration.standby\\_mode](#)  
[LCD\\_configuration.idle\\_screen\\_status](#)

## LCD\_configuration.idle\_video\_timeout

Parameter to set the duration for which video is played.

## Values

### SIGMA / SIGMA Extreme

- 0 - 600 (**60** - Default)

### MWC / VisionPass

- -1 - Do not play video
- 0 - 600 (**60** - Default) play duration

### SIGMA Lite / SIGMA Lite+ / MWSP / VisionPass SP

Not applicable

#### Note:



Timeout in seconds. 0 for infinite duration  
For MorphoWave® Compact products, video  
is played when  
**LCD\_configuration.standby\_mode** is  
enabled.

For other applicable products, video is played  
when  
**LCD\_configuration.idle\_screen\_status** is  
enabled.

#### See also:

[\*\*LCD\\_configuration.standby\\_mode\*\*](#)  
[\*\*LCD\\_configuration.idle\\_screen\\_status\*\*](#)

## **LCD\_configuration.brightness\_high**

Parameter to set highest value for auto adaptive LCD brightness.

## Values

### SIGMA Extreme

- 5 - 100 (**100** - Default)



**Since:**

MorphoAccess® 4.0.0

**SIGMA / SIGMA Lite / SIGMA Lite+ / MWC / VisionPass / MWSP / VisionPass SP**

Not applicable

### See also:

[\*\*LCD\\_configuration.brightness\\_autoadaptive\*\*](#)

## [\*\*LCD\\_configuration.brightness\\_low\*\*](#)

Parameter to set lowest value for auto adaptive LCD brightness.

## Values

### SIGMA Extreme

- 5 - 100 (**50** - Default)



**Since:**

MorphoAccess® 4.0.0

**SIGMA / SIGMA Lite / SIGMA Lite+ / MWC / VisionPass / MWSP / VisionPass SP**

Not applicable

### See also:

[\*\*LCD\\_configuration.brightness\\_autoadaptive\*\*](#)

## [\*\*LCD\\_configuration.brightness\*\*](#)

Parameter to set the general brightness of LCD.

A different brightness value can be applied to the video played in idle mode.

A high value could reduce the life period of the LCD backlight.

## Values

### SIGMA / SIGMA Lite+ / SIGMA Extreme

- 5 - 100 (**70** - Default)

### MWC / VisionPass / VisionPass SP

- 10 - 100 (**100** - Default)

### SIGMA Lite / MWSP

Not applicable

#### Note:



For MorphoAccess® Sigma Extreme series product, this parameter will not be applicable when parameter #LCD\_configuration.brightness\_autoadaptive is enable.

#### See also:

[LCD\\_configuration.video\\_play\\_brightness](#)  
[LCD\\_configuration.brightness\\_autoadaptive](#)  
[LCD\\_configuration.brightness\\_high](#)  
[LCD\\_configuration.brightness\\_low](#)

## LCD\_configuration.PIN\_keypad\_type

Parameter to display numeric or alphanumeric keypad to enter User PIN.

## Values

### SIGMA / SIGMA Extreme / MWC / VisionPass / VisionPass SP

- 0 - Alphanumeric keypad
- 1 - Numeric keypad (**1** - Default)



**Since:**

MorphoAccess® 1.4.0

### SIGMA Lite+

- 1 - Numeric keypad (**1** - Default)



**Since:**

MorphoAccess® 3.0.0

### SIGMA Lite / MWSP

Not applicable

## LCD\_configuration.brightness\_autoadaptive

Parameter to enable/disable auto adaptiveness of LCD brightness.

If light sensor value > Light\_Sensor.Threshold + Light\_Sensor.Hysteresis, LCD Brightness will be set to LCD\_configuration.Brightness\_High after a time of Light\_sensor.adaptation\_time. If during this time light sensor value never reached the condition: light sensor value < Light\_Sensor.Threshold - Light\_Sensor.Hysteresis

If light sensor value < Light\_Sensor.Threshold - Light\_Sensor.Hysteresis, LCD Brightness will be set to LCD\_configuration.Brightness\_Low after a time of Light\_sensor.adaptation\_time. If during this time light sensor value never reached the condition: light sensor value > Light\_Sensor.Threshold + Light\_Sensor.Hysteresis

## Values

### SIGMA Extreme

- 0 - Disable auto adaptiveness LCD brightness
- 1 - Enable auto adaptiveness LCD brightness (**1 - Default**)



**Since:**

MorphoAccess® 4.0.0

### SIGMA Lite / SIGMA Lite+ / SIGMA / MWC / VisionPass / MWSP / VisionPass SP

Not applicable

#### Note:



- Auto adaptiveness of the LCD backlight doesn't apply for the video.
- For MorphoAccess® Sigma Extreme series product, if this parameter is enable then parameter `#LCD_configuration.brightness` will not be applicable.

#### See also:

[\*\*LCD\\_configuration.brightness\*\*](#)

### [\*\*LCD\\_configuration.video\\_play\\_brightness\*\*](#)

Parameter to set the brightness of LCD in idle mode.

A high value could reduce the life period of the backlight LED.

## Values

### SIGMA / SIGMA Extreme

- 5 - 70 (**35** - Default)

### MWC

- 10 - 100 (**70** - Default)

### SIGMA Lite / SIGMA Lite+ / VisionPass / MWSP / VisionPass SP

Not applicable

## LCD\_configuration.icon\_set

Parameter to set icon selection to display during user control operation result message.

## Values

### SIGMA / SIGMA Extreme

- 1 - Access Granted and Access Denied message Selection 1  
*(1 - Default)*
- 2 - Access Granted and Access Denied message Selection 2



**Since:**

MorphoAccess® 3.2.0

### SIGMA Lite+

- 1 - Access Granted, Access Denied and Time & Attendance message Selection 1 *(1 - Default)*
- 2 - Access Granted, Access Denied and Time & Attendance message Selection 2



**Since:**

MorphoAccess® 3.2.0

### MWC

- 1 - Access Granted and Access Denied message Selection 1
- 2 - Access Granted and Access Denied message Selection 2  
*(2 - Default)*

### VisionPass / VisionPass SP

- 2 - Access Granted and Access Denied message Selection 2  
*(2 - Default)*

### SIGMA Lite / MWSP

Not applicable

## **LCD\_configuration.standby\_mode**

Parameter to enable or disable sensor standby mode.

In standby mode, video is played, sensor lightning is deactivated. Depending on **LCD\_configuration.idle\_screen\_status**, the terminal could be awaken by hand wave or not.

## Values

### MWC

- 0 - sensor standby mode disabled (**0** - Default)
- 1 - sensor standby mode enabled.

### SIGMA / SIGMA Lite / SIGMA Lite+ / SIGMA Extreme / VisionPass / MWSP / VisionPass SP

Not applicable

## LCD\_configuration.ID\_keypad\_type

Parameter to select normal or mask type of keypad ID.

## Values

**SIGMA / SIGMA Lite+ / SIGMA Extreme / MWC / VisionPass / VisionPass SP**

- 0 - normal ID keypad type (**0 - Default**)
- 1 - masked ID keypad type
- 2 - reserved



**Since:**

MorphoAccess® 3.5.0

**SIGMA Lite / MWSP**

Not applicable

## LCD\_configuration.play\_video\_during\_active\_mode

Parameter to set video play during active mode.

## Values

### VisionPass

- 0 - Switch to wallpaper display when user is detected (**0 - Default**)
- 1 - Continue to play idle video when user is detected

### SIGMA / SIGMA Lite / SIGMA Lite+ / SIGMA Extreme / MWC / MWSP / VisionPass SP

Not applicable

#### Note:

When video is played, icons are not displayed, the user should touch the screen to make them appear.

The icons are only displayed over the wallpaper or the default Background (never over the video)

The

`LCD_configuration.play_video_during_active_mode` value = '1' is applicable

\* When the OSDP feature is disable (`OSDP.channel` = 0)

\* When the Approach User Interface is disable (`MMI_state.user_guidance` = 0)

\* When the Privacy mode is disable (`bio_security_settings.intentional_bio_capture` = 0)

\* When the identification trigger is ON (all `ucc.trigger_events` with biometric input)

### `LCD_configuration.lighting_level`

Parameter to set lighting level used for identification in low lighting conditions.

## Values

### VisionPass SP

- 0 - Standard Lighting (**0** - Default)
- 1 - Full Lighting

### SIGMA / SIGMA Lite / SIGMA Lite+ / SIGMA Extreme / MWC / MWSP / VisionPass

Not applicable

#### Note:



Lighting level will not be considered if **bio\_security\_settings.ffd\_security\_level** is set to 0 or 1.

## misc.LCD\_administration

Parameter to enable/disable LCD administration menu.

## Values

**SIGMA / SIGMA Lite+ / SIGMA Extreme / MWC / VisionPass / VisionPass SP**

- 0 - Disabled
- 1 - Enabled (**1 - Default**)

**SIGMA Lite / MWSP**

Not applicable

## **misc.LCD\_login\_option**

Parameter to set the login policy for LCD administration menu.

## Values

SIGMA / SIGMA Extreme / MWC / VisionPass / VisionPass SP

- 0 : (Default)
  - ***On-Demand security mode***  
All management menu will be available and accessible
  - ***Enforced Security mode***  
Only information and communication menu will be available
- 1 : ID + Password
  - ***On-Demand security mode***
    - For users without administration rights : Only information menu visible and accessible
    - For users with full administration rights : All the Management Menu shall be accessed
    - For users with database administration rights : Only Information and User Management menu shall be accessed
    - For users with limited database administration rights : Only Information and User Management menu(not Edit and Delete User menu) shall be accessed
  - ***Enforced Security mode***
    - For users without administration rights : Only information menu shall be accessible
    - For users with full administration rights : Only information menu and Communication menu shall be accessible
    - For users with database administration rights : Only information menu shall be accessible

- For users with limited database administration rights : Only information menu shall be accessible

- **2 : ID + Password + BIO**

- For users without administration rights : Only information menu visible and accessible
- For users with full administration rights : All the Management Menu shall be accessed
- For users with database administration rights : Only Information and User Management menu shall be accessed
- For users with limited database administration rights : Only Information and User Management menu(not Edit and Delete User menu) shall be accessed

- **3 : ID + BIO**

- For users without administration rights : Only information menu visible
- For users with full administration rights : All the Management Menu shall be accessed
- For users with database administration rights : Only Information and User Management menu shall be accessed
- For users with limited database administration rights : Only Information and User Management menu(not Edit and Delete User menu) shall be accessed

## SIGMA Lite / SIGMA Lite+ / MWSP

Not applicable

**Note:**



When value is not 0, displayed information depends on user rights (i.e. standard, administrators).

**Warning:**

It is strongly advised to have at least one full administrator in the terminal before changing this parameter.

**See also:**

[misc.LCD\\_administration](#)

### **misc.language\_file\_name**

Parameter to set current display language.

To set the language, set filename from available language file list from terminal.

## Values

### SIGMA / SIGMA Extreme / MWC / VisionPass / VisionPass SP

- Any valid language file name string (*Empty for English - Default*)

### SIGMA Lite / SIGMA Lite+ / MWSP

Not applicable

## misc.language\_config\_display

Parameter to enable/disable display of the language selection menu on main screen.

## Values

### SIGMA / SIGMA Extreme / MWC / VisionPass / VisionPass SP

- 0 - Hide language selection menu
- 1 - Show language selection menu (**1 - Default**)



**Since:**

MorphoAccess® 1.2.4

### SIGMA Lite / SIGMA Lite+ / MWSP

Not applicable

## **misc.user\_id\_edit**

Parameter to allow modification of User ID after User ID is read from a contactless card during a user enrolment.

## Values

**SIGMA / SIGMA Extreme / MWC / VisionPass / VisionPass SP**

- 0 - Disabled
- 1 - Enabled (**1 - Default**)



**Since:**

MorphoAccess® 1.2.4

**SIGMA Lite / SIGMA Lite+ / MWSP**

Not applicable

## misc.display\_clock\_type

Parameter to enable/disable display of date and time on main screen.

## Values

**SIGMA / SIGMA Lite+ / SIGMA Extreme / MWC / VisionPass / VisionPass SP**

- 0 - Do not display date & time
- 2 - Display date & time (**2 - Default**)

**SIGMA Lite / MWSP**

Not applicable

## [misc.distant\\_session\\_timeout](#)

Parameter for distant session timeout. if distant session is started through distant command it close after this timeout, except if retrieve logs or upload users operation is ongoing. These two operations interrupt and reset the distant session timeout.

## Values

- 0 - 3600 (**60** - Default)

### SIGMA / SIGMA Extreme



**Since:**  
MorphoAccess® 1.5.0

### SIGMA Lite / SIGMA Lite+



**Since:**  
MorphoAccess® 3.0.0



**Note:**  
Timeout in seconds.

### [misc.customized\\_workflow](#)

Parameter for customized enroll workflow. Terminal's LCD enrolment parameters can be set to predetermined values by configuring this parameter.

## Values

### SIGMA / SIGMA Extreme

- 0 - Normal enroll workflow (**0 - Default**)
- 1 - Enroll type = card only, card expiry date = infinite, skip user name



**Since:**

MorphoAccess® 4.3.0

### SIGMA Lite / SIGMA Lite+ / VisionPass / MWC / MWSP / VisionPass SP

Not applicable

## LCD\_configuration.keypad\_layout

Parameter to define the type of keypad to be used (default keypad or modified keypad).

## Values

### SIGMA Lite+

- 0 - Default keypad layout shall be visible (*Default*)
- 1 - Modified Keypad layout shall be visible

**MWC / VisionPass / SIGMA / SIGMA Lite / SIGMA Extreme /  
MWSP / VisionPass SP**

Not applicable

Copyright © 2024, IDEMIA, All rights reserved. Reproduction in whole or in part in any form or medium without the express written permission of IDEMIA is prohibited.

# Access and Time Biometric Terminals Parameters Guide

[Main Page](#)

[Modules](#)

[Classes](#)

Defines

## MMI Configuration

---

## Detailed Description

This section details out the MMI (Man-Machine Interface) configurations related to LEDs and/or buzzer as applicable.



**Since:**

MorphoAccess® 3.1.0

## Define Documentation

### MMI\_state.finger\_trigger\_activate

Parameter to configure MMI LED status when only finger trigger is activated.

## Values

### SIGMA Lite / MWSP

- 0 : MMI LED is OFF when trigger is only "finger" (*0 - Default*)
- 1 : MMI LED is ON (blue) when trigger is only "finger".

### SIGMA / SIGMA Lite+ / SIGMA Extreme / MWC / VisionPass / VisionPass SP

Not applicable

## MMI\_state.user\_guidance

Parameter to configure MMI for user guidance. This MMI helps the user to position himself correctly in front of the biometric terminal.

## Values

### VisionPass

- 0 : No MMI is displayed during biometric acquisition (**0 - Default**)
- 1 : User guidance using icons.
- 2 : User guidance using camera live feed.

### VisionPass SP

- 0 : No MMI is displayed during biometric acquisition
- 1 : User guidance using icons.
- 2 : User guidance using camera live feed. (**2 - Default**)

### SIGMA / SIGMA Lite+ / SIGMA Extreme / MWC / SIGMA Lite / MWSP

Not applicable

Copyright © 2024, IDEMIA, All rights reserved. Reproduction in whole or in part in any form or medium without the express written permission of IDEMIA is prohibited.

# Access and Time Biometric Terminals Parameters Guide

[Main Page](#)

[Modules](#)

[Classes](#)

Defines

## NTP Service

---

## Detailed Description

Biometric terminals can communicate with NTP server to synchronize date and time of terminal.

To communicate with NTP server, it is pre-requisite to configure its IP address in the terminal.

As soon as the NTP server IP address is valid, date and time of terminal is updated after few minutes.

**Note:**



Since MorphoAccess® 1.3.2 release, it is possible to stop NTP service by configuring primary and secondary server address as either empty or with spaces.

## Define Documentation

### NTP\_server.primary\_ip\_address

Parameter of primary NTP server.

This would be IP address of primary NTP server.

### NTP\_server.secondary\_ip\_address

Parameter of secondary NTP server.

This would be IP address of secondary NTP server.

In case, communication with primary server fails then terminal tries to communicate with secondary server for date and time synchronization.

Copyright © 2024, IDEMIA, All rights reserved. Reproduction in whole or in part in any form or medium without the express written permission of IDEMIA is prohibited.

# Access and Time Biometric Terminals Parameters Guide

[Main Page](#)

[Modules](#)

[Classes](#)

Defines

## OSDP Protocol

---

## Detailed Description

Terminal supports the OSDP protocol. The terminal works as a Physical Device(PD) and process the request from control panel(CP).



**Since:**

MorphoAccess® 3.4.0

---

## Define Documentation

### OSDP.channel

Parameter to enable/disable communication using OSDP protocol.

## Values

- 0 - Disable (**0** - Default)
- 1 - Enable

## [\*\*OSDP.pin\\_over\\_osdp\*\*](#)

Parameter to enable/disable pin over OSDP functionality. PIN will be transmitted to the controller through the OSDP\_KEYPPAD response in reply to the OSDP\_POLL command.

## Values

### MWC / VisionPass

- 0 - Disable (**0 - Default**)
- 1 - Enable

### SIGMA / SIGMA Lite / SIGMA Lite+ / SIGMA Extreme / MWSP / VisionPass SP

Not applicable

## OSDP.secure\_connection

Parameter to enable/disable securing for OSDP communication.

## Values

- 0 - Disable (**0** - Default)
- 1 - Enable



**Since:**

MorphoAccess® 4.5.0

## OSDP.device\_serial\_address

Parameter to define the OSDP device identifier (Physical Device Address).

## Values

- 0 - 127 (**127** - Default)

## OSDP.ignore\_MMI

Parameter to play terminal default MMI when executing the commands OSDP\_LED, OSDP\_BUZ & OSDP\_TEXT. As it is not completely compliant to the OSDP specification, this feature shall be reserved for specific use cases, please contact IDEMIA before enabling it.

## Values

### MWC / VisionPass / MWSP / VisionPass SP

- 0 - Execute normally the commands OSDP\_LED, OSDP\_BUZ & OSDP\_TEXT (**0 - Default**)
- 1 - Acknowledge the commands OSDP\_LED, OSDP\_BUZ & OSDP\_TEXT but play terminal default MMI ("access\_denied" or "access\_granted") when OSDP\_LED command contains color RED or GREEN. No MMI will be played for other colors.
- 2 - RFU
- 3 - Acknowledge the commands OSDP\_LED, OSDP\_BUZ & OSDP\_TEXT but play terminal default MMI ("access\_denied" or "access\_granted") on successful comparison OSDP.access\_granted or OSDP.access\_denied key with osdp command data.

### SIGMA / SIGMA Lite / SIGMA Lite+

Not applicable

#### Note:



When this parameter is activated, for the OSDP\_LED command terminal will play MMI ("access\_denied" or "access\_granted"), only if the command contains color RED or GREEN. No MMI will be played for other colors.

#### See also:

[OSDP.access\\_granted](#) and [OSDP.access\\_denied](#)

[OSDP.access\\_granted](#)

Parameter to display default access granted MMI on successful matching with starting of OSDP command data.

## Values

- 0-128(*Empty - Default*)



### Note:

Value is hexadecimal string.

## OSDP.access\_denied

Parameter to display default access denied MMI on successful matching with starting of OSDP command data.

## Values

- 0-128(*Empty - Default*)



### Note:

Value is hexadecimal string.

## Display\_text.horizontal\_start

Parameter to set Display text horizontal position.

## Values

### VisionPass SP

- 0-420 (**0 - Default**)

**SIGMA / SIGMA Lite / SIGMA Lite+ / SIGMA Extreme / MWC / VisionPass / MWSP**

Not applicable

## Display\_text.vertical\_start

Parameter to set Display text vertical position.

## Values

### VisionPass SP

- 419-627 (**461 - Default**)

**SIGMA / SIGMA Lite / SIGMA Lite+ / SIGMA Extreme / MWC / VisionPass / MWSP**

Not applicable

Copyright © 2024, IDEMIA, All rights reserved. Reproduction in whole or in part in any form or medium without the express written permission of IDEMIA is prohibited.

# Access and Time Biometric Terminals Parameters Guide

[Main Page](#)

[Modules](#)

[Classes](#)

Defines

## RTC Validation

---

## Detailed Description

When the terminal battery is discharged or not plugged, the date and time used by the terminal from its startup, is incorrect until it is synchronized. In such cases, the terminal can forbid user control triggers so that an inaccurate timing is not logged in.



**Since:**

MorphoAccess® 1.3.2

---

## Define Documentation

### rtc.triggers\_block\_state

Parameter to enable/disable trigger blocking regarding RTC datetime.

If enabled, the terminal checks date-time and refuses control triggers if date-time is not synchronized yet. Triggers are blocked until the date-time is updated by an external host (using distant commands) or by use of NTP server.

## Values

- 0 - Disable (**0 - Default**)
- 1 - Enable

Copyright © 2024, IDEMIA, All rights reserved. Reproduction in whole or in part in any form or medium without the express written permission of IDEMIA is prohibited.

---

Generated by doxygen 1.7.6.1.

# Access and Time Biometric Terminals Parameters Guide

[Main Page](#)

[Modules](#)

[Classes](#)

Defines

## Remote Message

---

## **Detailed Description**

Terminal can send status messages in real-time to a controller via IP or serial communication channel. This section describes parameters associated with remote message.

---

## Define Documentation

### `remote_msg_conf.send_ethernet_state`

Parameter to enable/disable remote message sending over IP channel.

## Values

- 0 - Disable (**0** - Default)
- 1 - Enable

### `remote_msg_conf.send_serial_state`

Parameter to enable/disable remote message sending over serial channel (RS485/RS422).

## Values

- 0 - Disable (**0 - Default**)
- 1 - Enable

**Note:**



This Parameter can be enabled, only if **comm\_channels\_state.serial** is disabled.

## remote\_msg\_conf.format

This parameter is used to select event format and management over IP.

## Values

- 0 - Standard : Events are sent to controller over IP with standard format (for MorphoAccess® firmware up to 4.3 and for MorphoWave® firmware up to 1.1.0) (**0 - Default**)
- 1 - Extended : Events are sent to controller over IP with extended format
- 2 - Real time : Events are sent to controller over IP with extended format and events not transmitted are buffered for future retry

**Since:**



MorphoAccess® 4.5.0  
MorphoWave® 1.1.0

### **remote\_msg\_ip\_conf.mode**

Allows to select the IP host to which remote messages are sent to.

Used only if **remote\_msg\_conf.send\_ethernet\_state** is enabled.

## Values

- 0 - Send remote message to host 1 (*0 - Default*)
- 1 - Send remote message to both hosts 1 and 2
- 2 - Send remote message to host 1, then host 2 if host 1 fails

### Note:



For `remote_msg_conf.feedback_interface` is set 1 (feedback over IP) and `remote_msg_ip_conf.mode` is set to 1 (both hosts), final response will be considered as per following conditions:

- 2nd host's feedback will be considered when both hosts provides feedback.
- 1st host's feedback will be considered when terminal is not able to connect to 2nd host.

## `remote_msg_ip_conf.host_1_ip`

Primary remote host/controller IP address.

## Values

- IP address of the primary remote host in string.

### remote\_msg\_ip\_conf.host\_1\_port

Primary remote host/controller port number.

## Values

- 1 - 65000 (**11020** - Default)

### remote\_msg\_ip\_conf.host\_1\_timeout

Primary remote host/controller timeout used for connection, read, write operations.

## Values

- 1 - 65000 (**2000** - Default)



### Note:

Timeout in multiples of 10 milliseconds.

## remote\_msg\_ip\_conf.host\_1\_protocol

Primary remote host/controller protocol used for communication.

## Values

- 0 - TCP protocol (**0** - Default)
- 1 - UDP protocol
- 2 - SSL over TCP

### remote\_msg\_ip\_conf.host\_2\_ip

Secondary remote host/controller IP address.

## Values

- IP address of the secondary remote host in string.

### `remote_msg_ip_conf.host_2_port`

Secondary remote host/controller port number.

## Values

- 1 - 65000 (**11021** - Default)

### remote\_msg\_ip\_conf.host\_2\_timeout

Secondary remote host/controller timeout used for connection, read, write operations.

## Values

- 1 - 65000 (**2000** - Default)



### Note:

Timeout in multiples of 10 milliseconds.

## [remote\\_msg\\_ip\\_conf.host\\_2\\_protocol](#)

Secondary remote host/controller protocol used for communication.

### See also:

[remote\\_msg\\_ip\\_conf.host\\_1\\_protocol](#)

## [remote\\_msg\\_ip\\_conf.host\\_on\\_no\\_response](#)

Parameter to set whether Biometric terminal should act as a controller, in case there is no feedback from remote TCP or serial host.

Used only if [remote\\_msg\\_conf.send\\_ethernet\\_state](#) or [remote\\_msg\\_conf.send\\_serial\\_state](#) is enabled.

## Values

- 0 - Do not act as controller (*0 - Default*)
- 1 - Act as controller

### **remote\_msg\_serial\_conf.format**

Parameter allows to select the remote message protocol on serial channel.

## Values

**SIGMA / SIGMA Extreme / MWC / VisionPass / MWSP / VisionPass SP**

- 485 - RS485 protocol (**485 - Default**)
- 422 - RS422 protocol

**SIGMA Lite / SIGMA Lite+**

- 485 - RS485 protocol (**485 - Default**)



**Since:**

MorphoAccess® 3.1.0

### **remote\_msg\_conf.serial\_reply\_timeout**

Parameter to set the timeout for which terminal should wait for controller feedback on serial channel.

## Values

**SIGMA / SIGMA Extreme / MWC / VisionPass / MWSP / VisionPass SP**

- 0 - 3600 (**5** - Default)

**SIGMA Lite / SIGMA Lite+**

Not applicable



**Note:**

Timeout is in seconds

## remote\_msg\_conf.feedback\_interface

Parameter to set whether terminal should wait for the feedback message from the controller (i.e. enable/disable feedback).

It also defines the channel interface on which feedback is awaited.

## Values

### SIGMA / SIGMA Extreme / MWC / VisionPass / MWSP / VisionPass SP

- 0 - Do not wait for controller feedback (*0 - Default*)
- 1 - Wait controller feedback over **IP channel**
- 2 - Wait controller feedback over **serial channel** (applicable for RS422 protocol format only, refer [remote\\_msg\\_serial\\_conf.format](#))
- 3 - Wait controller feedback over **input pins** (also refer [controller\\_feedback.panel\\_mode](#) and [controller\\_feedback.feedback\\_lines](#))

### SIGMA Lite / SIGMA Lite+

- 0 - Do not wait for controller feedback (*0 - Default*)
- 1 - Wait controller feedback over **IP channel**
- 3 - Wait controller feedback over **input pins** (also refer [controller\\_feedback.panel\\_mode](#) and [controller\\_feedback.feedback\\_lines](#))

### **remote\_msg\_conf.serial\_feedback\_msg\_display\_timeout**

Display duration for serial ILV feedback message.

## Values

### SIGMA / SIGMA Extreme

- 1 - 20 (**3** - Default)



**Since:**

MorphoAccess® 3.1.0

### SIGMA Lite / SIGMA Lite+ / VisionPass / MWC / MWSP / VisionPass SP

Not applicable

Copyright © 2024, IDEMIA, All rights reserved. Reproduction in whole or in part in any form or medium without the express written permission of IDEMIA is prohibited.

# Access and Time Biometric Terminals Parameters Guide

[Main Page](#)

[Modules](#)

[Classes](#)

Defines

**SDAC (Single Door  
Access Control)**

## Detailed Description

SDAC (Single Door Access Controller) is used to trigger an internal relay which is connected to an electro-magnet lock on the door for door Open/Close and for monitoring door status on the entrance. The SDAC mode can be activated by setting the `gpio.func_mode` to SDAC mode.

**Only one of either SDAC mode, GPIO general mode, or Threat Level mode can be activated at a time.**

---

## Define Documentation

### `gpio.sdac_relay_default_state`

Internal relay idle state ( during which normally door remain locked ).

**Can only be set when `gpio.func_mode` is SDAC mode.**

## Values

### SIGMA / SIGMA Extreme

- 0 - Low state (**0** - Default)
- 1 - High state

### SIGMA Lite / SIGMA Lite+ / MWC / VisionPass / MWSP / VisionPass SP

Not applicable

#### See also:

[gpio.func\\_mode](#)

## gpio.sdac\_door\_unlock\_dur

Duration during which relay is triggered after successful user control.

Can only be set when [gpio.func\\_mode](#) is SDAC mode.

## Values

- 1 - 60

**MWC / VisionPass / MWSP / VisionPass SP**

**(1 - Default)**

**SIGMA / SIGMA Lite / SIGMA Lite+ / SIGMA Extreme**

**(10 - Default)**

**See also:**

[gpio.func\\_mode](#)



**Note:**

Timeout in seconds

## [gpio.sdac\\_max\\_door\\_held\\_open\\_dur](#)

Duration for which terminal will wait for door closing after [gpio.sdac\\_door\\_unlock\\_dur](#).

After successful user control, relay is triggered. Terminal closes the relay after [gpio.sdac\\_door\\_unlock\\_dur](#) and waits for [gpio.sdac\\_max\\_door\\_held\\_open\\_dur](#) to get door closed before generating "door held open" alarm.

**Can only be set when [gpio.func\\_mode](#) is in SDAC mode.**

## Values

- 1 - 3600 (**25** - Default)

See also:

[gpio.func\\_mode](#)



**Note:**

Timeout in seconds

## [gpio.sdac\\_rte\\_mode](#)

Parameter to select the request to exit mode in SDAC.

When request to exit occurred, terminal allows the door to be opened and does not generate "forced door open" alarm.

**Can only be set when [gpio.func\\_mode](#) is SDAC mode.**

## Values

- 0 - None (*0 - Default*)
- 1 - Push Button (User presses push button to request exit)
- 2 - Reserved (Should not be used)

See also:

[gpio.func\\_mode](#)

## [gpio.sdac\\_rte\\_egress\\_timeout](#)

Parameter to define a request to exit egress timeout, duration for which terminal will not generate alarm if door is opened by use of push button manual or forced door open without performing any user control in the terminal.

[gpio.sdac\\_rte\\_mode](#) should be set to 1 or 2.

**Can only be set when [gpio.func\\_mode](#) is SDAC mode.**

## Values

- 1 - 300 (**25** - Default)

See also:

[gpio.func\\_mode](#)



**Note:**

Timeout in seconds

## [gpio.sdac\\_push\\_btn\\_mode](#)

Parameter to define if the terminal should trigger the relay on push button request.

During single terminal installation on door, A push button switch can be used on opposite (where terminal is installed ) side of door to allow door opening. This push button switch is connected to the request to exit GPI of the terminal.

[gpio.sdac\\_rte\\_mode](#) should be set to 1.

**Can only be set when [gpio.func\\_mode](#) is SDAC mode.**

## Values

- 0 - Manual (Internal relay not triggered by terminal) (**0 - Default**)
- 1 - Electric (Internal relay triggered by the terminal)

### See also:

[gpio.func\\_mode](#)

## gpio.tom\_mode

Parameter to enable/disable Time Override Mode (TOM).

Time Override Mode (TOM) allows an administrator to temporarily suspend the need for user control for a specific period of time.

Whenever TOM is enabled on terminal, the door gets unlocked and terminal does not lock door till TOM is ended.

**Can only be set when [gpio.func\\_mode](#) is SDAC mode.**

## Values

- 0 - Disable (**0 - Default**)
- 1 - Enable

See also:

[gpio.func\\_mode](#)

## gpio.tom\_duration

Parameter to define TOM duration.

Once this duration is finished, the door is locked automatically.

**Can only be set when [gpio.func\\_mode](#) is SDAC mode.**

## Values

- 1 - 1440 (**1** - Default)

See also:

[gpio.func\\_mode](#)



**Note:**

Duration in minutes.

## [gpio.door\\_open\\_schedule](#)

Parameter to enable/disable door open schedule.

The door open schedule, defined in terminal, is used to open door when this parameter is enabled.

**Can only be set when [gpio.func\\_mode](#) is SDAC mode.**

## Values

- 0 - Disable (**0 - Default**)
- 1 - Enable

See also:

[gpio.func\\_mode](#)

Copyright © 2024, IDEMIA, All rights reserved. Reproduction in whole or in part in any form or medium without the express written permission of IDEMIA is prohibited.

# Access and Time Biometric Terminals Parameters Guide

[Main Page](#)

[Modules](#)

[Classes](#)

Defines

## SSCP Protocol

---

## Detailed Description

If terminal supports the SSCP protocol: works as a Physical Device(PD) and process the request from control panel(CP). A dedicated license (BT\_SSCP) is required for the below configuration keys to be available.



**Since:**

MorphoWaveSP® 2.1.4

---

## Define Documentation

### **SSCP.channel**

Parameter to enable/disable communication using SSCP protocol.

## Values

### MWSP

- 0 - Disable (**0 - Default**)
- 1 - Enable

**SIGMA / SIGMA Lite / SIGMA Lite+ / SIGMA Extreme / MWC / VisionPass / VisionPass SP**

Not applicable

## **SSCP.device\_serial\_address**

Parameter to define the SSCP device identifier (Physical Device Address).

## Values

### MWSP

- 0 - 127 (**0** - Default)

**SIGMA / SIGMA Lite / SIGMA Lite+ / SIGMA Extreme / MWC / VisionPass / VisionPass SP**

Not applicable

### **SSCP.intercharacter\_timeout**

SSCP serial inter-character timeout (ms). Timeout to receive two consecutive bytes.

## Values

### MWSP

- 0 - 20 (**20** - Default)

**SIGMA / SIGMA Lite / SIGMA Lite+ / SIGMA Extreme / MWC / VisionPass / VisionPass SP**

Not applicable

### [SSCP.start\\_of\\_frame\\_timeout](#)

SSCP serial start-of-frame timeout (ms). Timeout to wait new start of command.

## Values

### MWSP

- 0 - 8000 (**8000** - Default)

**SIGMA / SIGMA Lite / SIGMA Lite+ / SIGMA Extreme / MWC / VisionPass / VisionPass SP**

Not applicable

### **tamper.action\_reset\_SSCP**

When tamper is triggered: action to reset SSCP Authentication key to default value.

## Values

### MWSP

- 0 - Disable (**0 - Default**)
- 1 - Reset SSCP key

**SIGMA / SIGMA Lite / SIGMA Lite+ / SIGMA Extreme / MWC / VisionPass / VisionPass SP**

Not applicable

Copyright © 2024, IDEMIA, All rights reserved. Reproduction in whole or in part in any form or medium without the express written permission of IDEMIA is prohibited.

# Access and Time Biometric Terminals Parameters Guide

[Main Page](#)

[Modules](#)

[Classes](#)

Defines

## Sensors

---

## Detailed Description

This section describes configuration parameters related to different sensors:

- MorphoAccess® Sigma Extreme series product supports ambient light sensor to control terminal LCD brightness automatically
  - VisionPass SP series product supports motion sensor to activate people detection
-

## Define Documentation

### **motion\_sensor.activation**

Parameter to activate or deactivate motion sensor.

## Values

### VisionPass SP

- 0 - Deactivate motion sensor
- 1 - Activate motion sensor (**1** - Default)

### SIGMA / SIGMA Extreme / SIGMA Lite / SIGMA Lite+ / MWC / VisionPass / MWSP

Not applicable



#### Note:

Change in the value of this key is only applied after reboot.

## Light\_sensor.threshold

Parameter to configure threshold level of light sensor.

## Values

### SIGMA Extreme

- 1 - 65535 (**500** - Default)



**Since:**

MorphoAccess® 4.0.0

### SIGMA / SIGMA Lite / SIGMA Lite+ / MWC / VisionPass / MWSP / VisionPass SP

Not applicable

## Light\_sensor.hysteresis

Parameter to configure hysteresis level of light sensor.

## Values

### SIGMA Extreme

- 1 - 65535 (**100** - Default)



**Since:**

MorphoAccess® 4.0.0

**SIGMA / SIGMA Lite / SIGMA Lite+ / MWC / VisionPass / MWSP / VisionPass SP**

Not applicable

### Light\_sensor.adaptation\_time

Parameter to configure adaptation time of light sensor.

## Values

### SIGMA Extreme

- 1 - 300 (**5** - Default)



**Since:**

MorphoAccess® 4.0.0

**SIGMA / SIGMA Lite / SIGMA Lite+ / MWC / VisionPass / MWSP / VisionPass SP**

Not applicable

Copyright © 2024, IDEMIA, All rights reserved. Reproduction in whole or in part in any form or medium without the express written permission of IDEMIA is prohibited.

# Access and Time Biometric Terminals Parameters Guide

[Main Page](#)

[Modules](#)

[Classes](#)

Defines

## Smart Card

---

## Detailed Description

Users can be authenticated using the data stored on a contactless card. Generally a contactless card can store User ID, PIN, BIOPIN and Biometric Data on the card. The **ucc.trigger\_event** parameter shall allow contactless cards to be read and assessed by the terminal.

Users can be authenticated using the data stored on a contactless card. For details please refer to the document "Contactless Cards Specification".

---

## Define Documentation

### **sc.encode\_profile**

Parameter to set types of cards to be supported for encoding operations.

Bit field value:

**Applicable to MorphoWave® Compact, MorphoWave® SP, VisionPass MDPI and VisionPass SP MDI products:**

bit 4 - HID iClass®

**Applicable to MASigma Multi Family, MorphoWave® Compact MD, MorphoWave® Compact MDPI, MorphoWave® SP MD, MorphoWave® SP MDPI, VisionPass MD, VisionPass MDPI, VisionPass SP MD, and VisionPass SP MDI products:**

bit 3 - DESFire® AES

bit 2 - MIFARE® Plus

bit 1 - MIFARE® Classic

bit 0 - DESFire® 3DES

## Values

### SIGMA / SIGMA Lite / SIGMA Lite+ / SIGMA Extreme

- 1,2,3,4,5,8,10,12 (**3 - Default**)

### MWC / VisionPass / MWSP

- 1,2,3,4,5,8,10,12,16,17,18,19,24,26 (**3 - Default**)

### VisionPass SP

- 1,2,4,8,16 (**1 - Default**)

#### Note:



- It is not possible to detect several types of DESFire®(3DES and AES) or MIFARE® (Classic) or HID cards at the same time during encoding operations.
- sc.encode\_profile key is not evaluated using a MorphoAccess® Sigma iClass terminal.

## sc.read\_profile

Parameter to set types of cards to be supported for reading operations.

Bit field value:

bit 15 - Reserved, should be set to 0

bit 14 - Reserved, should be set to 0

bit 13 - PIV/TWIC® (**Applicable to MorphoWave® Compact MD, MorphoWave® Compact MDPI, MorphoWave® SP MD, MorphoWave® SP MDPI, VisionPass MD, VisionPass MDPI, VisionPass SP MD and VisionPass SP MDI products**)

bit 12 - Reserved, should be set to 0

bit 11 - HID Mobile Credential (**Applicable to MorphoWave® Compact MDPI-M, MorphoWave® SP MDPI-M and VisionPass MDPI-M products**)

bit 10 - Reserved, should be set to 0

bit 9 - Reserved, should be set to 0

bit 8 - HID Prox® (**Applicable to MorphoWave® Compact MDPI, MorphoWave® SP MDPI and VisionPass MDPI products**)

bit 7 - HID Seos® (**Applicable to MASigma iClass Family, MorphoWave® Compact MDPI, MorphoWave® SP MDPI, VisionPass MDPI and VisionPass SP MDI products**)

bit 6 - HID iClass® (**activated by default**)

bit 5 - Reserved, should be set to 0

bit 4 - MIFARE® Plus SL3 (**Applicable to MASigma Multi Family, MorphoWave® Compact MD, MorphoWave® SP MD, VisionPass MD and VisionPass SP MD products**)

bit 3 - DESFire® AES (**Applicable to MASigma Multi Family, MorphoWave® Compact MD, MorphoWave® SP MD and VisionPass MD and VisionPass SP MD products**)

bit 2 - Reserved, should be set to 0

bit 1 - MIFARE® Classic

bit 0 - DESFire® 3DES

## Values

### SIGMA Lite / SIGMA Lite+ / SIGMA / SIGMA Extreme

- 0 - 255 (**1** - Default)

### MWC / VisionPass / MWSP

- 1,2,3,8,9,10,11,16,17,18,19,24,25,26,27,64,128,192,256,257,258,264,265,272,320,384,2048,2112,2176,2240,2304,2368,2432,8192 (**1** - Default)

### VisionPass SP

- 1,2,3,8,9,10,11,16,17,18,19,24,25,26,27,64,128,192,8192 (**1** - Default)

#### Note:



- Any card can be read at same time.
- The effect of this parameter change is applicable only after terminal reboot. To read PACS data from HID Seos®, HID MIFARE® SE and HID DESFire® SE, HID Seos® profile should be activated.



#### Since:

MorphoAccess® 1.3.3, bit 6 and 7 added.

#### Warning:

- For MorphoWave® Compact MDPI, MorphoWave® SP MDPI and VisionPass MDPI products, only following combinations are allowed  
PIV/TWIC®  
HID Prox®

HID iClass®  
HID Seos®  
MIFARE® Classic  
DESFire® 3DES  
DESFire® AES  
MIFARE® Classic + DESFire® 3DES  
MIFARE® Classic + DESFire® AES  
MIFARE® Classic + DESFire® 3DES +  
DESFire® AES  
HID Prox® + iClass®  
HID Prox® + HID Seos®  
HID Prox® + DESFire® 3DES  
HID Prox® + DESFire® AES  
HID Prox® + DESFire® 3DES +  
DESFire® AES  
HID Prox® + MIFARE® Classic  
HID iClass® + HID Seos®  
Mifare® Plus  
Mifare® Classic + Mifare® Plus  
Mifare® Plus + DESFire® 3DES  
Mifare® Plus + DESFire® AES  
Mifare® Plus + DESFire® 3DES +  
DESFire® AES  
Mifare® Classic + Mifare® Plus +  
DESFire® 3DES  
Mifare® Classic + Mifare® Plus +  
DESFire® AES  
Mifare® Classic + Mifare® Plus +  
DESFire® 3DES + DESFire® AES  
HID Prox® + Mifare® Plus  
HID Mobile Credential  
HID Seos® + HID Mobile Credential  
HID iClass® + HID Mobile Credential  
HID Seos® + HID iClass® + HID Mobile  
Credential  
HID Prox® + iClass® + HID Mobile  
Credential



HID Prox® + HID Seos® + HID Mobile Credential  
HID Prox® + HID Mobile Credential

- For VisionPass SP MDI, only following combinations are allowed

PIV/TWIC®  
HID iClass®  
HID Seos®  
MIFARE® Classic  
DESFire® 3DES  
DESFire® AES  
MIFARE® Classic + DESFire® 3DES  
MIFARE® Classic + DESFire® AES  
MIFARE® Classic + DESFire® 3DES +  
DESFire® AES  
HID iClass® + HID Seos®  
Mifare® Plus  
Mifare® Classic + Mifare® Plus  
Mifare® Plus + DESFire® 3DES  
Mifare® Plus + DESFire® AES  
Mifare® Plus + DESFire 3DES +  
DESFire® AES  
Mifare® Classic + Mifare® Plus +  
DESFire® 3DES  
Mifare® Classic + Mifare® Plus +  
DESFire® AES  
Mifare® Classic + Mifare® Plus +  
DESFire®® 3DES + DESFire® AES

#### **sc.no\_data**

Parameter to set the reading of card data. There is no impact of this key on thrift communication.

## Values

### MWC / VisionPass / MWSP / VisionPass SP

- 0 - Device reads complete card content. (**0** - Default)
- 1 - Device should not try to read card content - Only CSN or PACS are read.

### SIGMA Lite / SIGMA Lite+ / SIGMA / SIGMA Extreme

Not applicable

### sc.zero\_tag\_read

Parameter to authorize the zero padding between TLV. Idemia strongly recommends this parameter not to be enabled.

## Values

### SIGMA / SIGMA Extreme / SIGMA Lite / SIGMA Lite+

- 0 - Reading of tag zero is disabled(**0** - *Default*)
- 1 - Reading of tag zero is enabled

### MWC / VisionPass / MWSP / VisionPass SP

Not applicable

## sc.encode\_timeout

Parameter to set the timeout used for encoding card.

## Values

**SIGMA / SIGMA Extreme / MWC / VisionPass / MWSP / VisionPass SP**

- 3 - 15 (**3 - Default**)

**SIGMA Lite / SIGMA Lite+**

Not applicable



**Note:**

Timeout in seconds



**Since:**

MorphoAccess® 1.2.4

## sc.support\_l1\_cards

Enable/Disable L1 card (reading operation) support.

## Values

### SIGMA / SIGMA Lite / SIGMA Lite+ / SIGMA Extreme

- 0 - Disable L1 card reading (*Default*)
- 1 - Enable L1 card reading
- 2 - Enable L1 card reading with extended ID
- 3 - Enable L1 card reading and Use Wiegand String

### MWC / VisionPass / MWSP / VisionPass SP

Not applicable



#### Since:

MorphoAccess® 4.3.0, value 2 is available.  
MorphoAccess® 4.6.0, value 3 is available.



#### Note:

The effect of this parameter change is applicable only after terminal reboot.

To enable "L1 card reading with extended ID" (i.e. `sc.support_l1_cards = 2`) feature, `sc.verify_user_id` configuration must be set to value 0 (No CSN).

If "L1 card reading and Use Wiegand String" (i.e. `sc.support_l1_cards = 3`) feature is enabled, `sc.verify_user_id` configuration will not be applicable for Wiegand output.

### `sc_l1_desfire.aid`

Set DESFire® application ID to read in L1 cards.

## Values

### SIGMA / SIGMA Lite / SIGMA Lite+ / SIGMA Extreme

- 0 to 16777215 (0x000000 to 0xFFFFFFF) (**15656448 for 0xEEE600 - Default**)

### MWC / VisionPass / MWSP / VisionPass SP

Not applicable



**Note:**

Value is in decimal.

### sc\_l1\_desfire.fid

Set DESFire® file ID to read in L1 cards.

## Values

### SIGMA / SIGMA Lite / SIGMA Lite+ / SIGMA Extreme

- 0 to 31 (0x00 to 0x1F) (**0x00 - Default**)

### MWC / VisionPass / MWSP / VisionPass SP

Not applicable



#### Note:

Value is in decimal.

## [\*\*sc\\_tlv\\_desfire.aid\\_list\*\*](#)

Parameter to set DESFire® multiple application IDs to be read in Morpho cards.

Applicable to standard DESFire AES and DES read profiles.

The value shall be a string containing hexadecimal values separates by “;”.

If the value is a list of AIDs then the terminal will search in the card for the first AID in the list, then the second AID in the list, etc.

If the value is empty then the legacy [\*\*sc\\_tlv\\_desfire.aid\*\*](#) parameter will be used.

Limit of number of AID = 5

## Values

- Any five valid AIDs separated by semicolon (;) of range 0 to 16777215 (0x000000 to 0xFFFFFFF) for each aid

**SIGMA / SIGMA Lite / SIGMA Lite+ / SIGMA Extreme / MWC / VisionPass / VisionPass SP / MWSP**

*Default value: Empty*

**Note:**



Value is in decimal. If **sc\_tlv\_desfire.aid\_list** is empty or any invalid value, **sc\_tlv\_desfire.aid** will be used. In case reading of the first AID of the list fails, it will read next AID of the list.

This feature is activated when MA\_DESFIRE\_DYN\_APP license is present in Terminal.

**See also:**

[\*\*sc\\_tlv\\_desfire.aid\*\*](#)

### [\*\*sc\\_tlv\\_desfire.aid\*\*](#)

Parameter to set DESFire® application ID to read/write in Morpho cards.

## Values

- 0 to 16777215 (0x000000 to 0xFFFFFFF)

### SIGMA / SIGMA Lite / SIGMA Lite+ / SIGMA Extreme

*Default value: **4344143 for 0x42494F***

### MWC / MWSP

*Default value: **7815542 for 0x774176***

### VisionPass / VisionPass SP

*Default value: **4604227 for 0x464143***



#### Note:

Value is in decimal.

## sc\_tlv\_desfire.fid

Parameter to set DESFire® file ID to read/write in Morpho cards.

## Values

- 0 to 31 (0x00 to 0x1F) (**0x00** - Default)



### Note:

Value is in decimal.

## sc\_tlv\_iclass.page\_offset

Parameter to set start block for HID iCLASS® 2APP Morpho cards.

## Values

- 0 - 255 (**19** - *Default*)

## sc\_tlv\_iclass.num\_block

Parameter to set number of data blocks to read from iCLASS® Morpho cards.

## Values

- 0 - 255

**SIGMA / SIGMA Lite / SIGMA Lite+ / SIGMA Extreme / MWC / MWSP**

*Default value:* **128**

**VisionPass / VisionPass SP**

*Default value:* **152**

## sc\_tlv\_iclass.book\_number

Parameter to set iCLASS® card book number for 32K Morpho cards.

## Values

- 0 - 16777215 (**0** - Default)

## sc\_tlv\_iclass.page\_layout

Parameter to set start page for HID iCLASS® 16APP Morpho cards.

## Values

- 1 - 5 (**1** - Default)

## sc\_l1\_iclass.page\_offset

Set start block for HID iCLASS® 2APP L1 cards.

## Values

**SIGMA / SIGMA Lite / SIGMA Lite+ / SIGMA Extreme**

- 0 to 255 (**19 - Default**)

**MWC / VisionPass / MWSP / VisionPass SP**

Not applicable

## **sc\_l1\_iclass.book\_number**

Set HID iCLASS® card book number for 32K L1 cards.

## Values

### SIGMA / SIGMA Lite / SIGMA Lite+ / SIGMA Extreme

- 0 - 16777215 (**0** - Default)

### MWC / VisionPass / MWSP / VisionPass SP

Not applicable

## sc\_l1\_iclass.page\_layout

Set iCLASS® card page layout for 16APP L1 cards.

## Values

### SIGMA / SIGMA Lite / SIGMA Lite+ / SIGMA Extreme

- 0 - 16777215 (**8421418** - Default)

### MWC / VisionPass / MWSP / VisionPass SP

Not applicable

#### Note:



User must set page layout for iCLASS® card according to custom layout configuration in 4G terminal.

## sc\_tlv\_seos.adf\_oid

Set HID SEOS® application ID to read/write in Morpho cards.

## Values

- Default is "2A8570811E1000070000020000" for Biometric SEOS cards



**Note:**

Value is hexadecimal string.

### sc\_tlv\_seos.first\_do\_tag

Parameter to set start data object read SEOS; Morpho cards.

## Values

- 192 - 199 (**192** - Default)

### sc\_tlv\_mifare.start\_block

Parameter to set start block number to read/write MIFARE® Morpho cards.

## Values

- 1 - 215 (**4** - Default)

### `sc_tlv_mifare.num_block`

Parameter to set number of data blocks to read MIFARE® Morpho cards (sector trailers are skipped).

## Values

**SIGMA / SIGMA Lite / SIGMA Lite+ / SIGMA Extreme / MWC / MWSP**

- 0 - 216 (**31** - Default)

**VisionPass / VisionPass SP**

- 0 - 216 (**84** - Default)

## sc\_l1\_mifare.kb\_number

Set active kilobyte number to read in MIFARE® L1 cards.

## Values

**SIGMA / SIGMA Lite / SIGMA Lite+ / SIGMA Extreme**

- 1 - 4 (*4 - Default*)

**MWC / VisionPass / MWSP / VisionPass SP**

Not applicable

## sc\_l1\_mifare.key\_policy

Set key policy to read MIFARE® L1 cards.

## Values

### SIGMA / SIGMA Lite / SIGMA Lite+ / SIGMA Extreme

- 1 - Try to read card first with Key A then Key B (**1 - Default**)
- 2 - Try to read card with Key A
- 3 - Try to read card with Key B

### MWC / VisionPass / MWSP / VisionPass SP

Not applicable

## sc.hashing\_enable

Enable L1 card hashing options, which are:

## Values

### SIGMA Lite / SIGMA Lite+ / SIGMA / SIGMA Extreme

- 2368513 - For(byte 0 to 4) 0x01,0x24,0x24,0x00
- 2368514 - For(byte 0 to 4) 0x02,0x24,0x24,0x00 (**2368514 - Default**)
- 2105347 - For(byte 0 to 4) 0x03,0x20,0x20,0x00
- 2367492 - For(byte 0 to 4) 0x04,0x20,0x24,0x00

### MWC / VisionPass / MWSP / VisionPass SP

Not applicable

#### Note:



To enable the hashing change value to '2368513'. Other options disable Hashing for L1 legacy card. This parameter also contains card security parameter but it is not useful as of now.

## sc\_tlv\_mifare.key\_policy

Parameter to set key policy to read MIFARE® Morpho cards.

## Values

- 1 - Try to read card first with Key A then Key B (**1 - Default**)
- 2 - Try to read card with Key A
- 3 - Try to read card with Key B

### **sc.auto\_key\_update**

Parameter to set specific operations on keys and cards.

It is used to deal with DESFire multi-applications cards, and to enable/disable the automatic key rolling on the card, when detected card has old keys.

## Values

- 0,1,2,3,4,5,6,7,16,17,18,19,20,21,22,23,32,33,34,35,36,37,38,39,48,49,50,51,52,53,54,55 (**2 - Default**)

For example:

- Bit 0: For DESFire® cards, do not format card before encoding
- Bit 1: Disable keys rotation on the fly
- Bit 2: For DESFire® cards, do not format card during local erasing
- Bit 3: Reserved
- Bit 4: For DESFire® cards, disable Master PICC key derivation
- Bit 5: For DESFire® cards, disable Application keys derivation

## SIGMA / SIGMA Extreme



### Since:

MorphoAccess® 1.2.4, value 4 is available.  
MorphoAccess® 1.3.2, value 5 is available.

## SIGMA Lite / SIGMA Lite+



### Since:

MorphoAccess® 3.0.0

## sc.enroll\_user\_id

Parameter to specify the type of user ID used during enrolment.

## Values

- 0 - User ID is encoded as a tag in the card (**0 - Default**)
- 1 - Using Standard CSN
- 2 - Using Reverse CSN
- 4 - Using 4G CSN (As per generated in SecureAdmin)
- 5 - HID card number (Only applicable for iClass and MDPI products)

## SIGMA Lite / SIGMA Lite+ / SIGMA / SIGMA Extreme / MWC / VisionPass / MWSP / VisionPass SP



### Note:

- The effect of this parameter change is applicable only for terminal reboot

## MWC / VisionPass / MWSP / VisionPass SP



### Note:

- The value 4 is not applicable for MorphoWave® Compact, MorphoWave® SP, VisionPass, VisionPass SP products.
- The value 5 is applicable for MorphoWave® Compact MDPI, MorphoWave® SP MDPI, VisionPass MDPI, VisionPass SP MDI products using iClass, Mifare SE and Desfire SE cards.



### Since:

MorphoAccess® 1.2.4, value 4 is available.  
MorphoAccess® 1.3.2, value 5 is available.

## **sc.verify\_user\_id**

Parameter to specify the type of user ID used during control.

## Values

- 0 - User ID is encoded as a tag in the card (**0 - Default**)
- 1 - Using Standard CSN
- 2 - Using Reverse CSN
- 3 - Enable Binary ID
- 4 - Using 4G CSN (As per generated in SecureAdmin)
- 5 - HID card number (only applicable for iClass product)
- 6 - HID card number Reverse(only applicable for iClass & Prox products)
- 7 - PIV/TWIC 75 bit format
- 8 - PIV/TWIC 200 bit format
- 9 - H10314 bit format (only applicable for iClass product)

**SIGMA Lite / SIGMA Lite+ / SIGMA / SIGMA Extreme / MWC / VisionPass / MWSP / VisionPass SP**

**Note:**



Binary ID is not supported for iClass and SEOS cards. Enable/Disable of Binary ID is applicable only after terminal reboot, rest all are applicable without terminal reboot.

**MWC / VisionPass / MWSP / VisionPass SP**

**Note:**



- The value 4 is not applicable for MorphoWave® Compact, MorphoWave® SP, VisionPass and VisionPass SP products.
- The value 5 is applicable for MorphoWave® Compact MDPI, MorphoWave® SP MDPI, VisionPass MDPI and VisionPass SP MDI products

products using iClass, Mifare SE and Desfire SE cards.

**Since:**

MorphoAccess® 1.2.4, values 3 and 4 are available.



MorphoAccess® 1.3.2, values 5 is available.

MorphoAccess® 1.3.5, values 6 for iClass is available.

MorphoAccess® 4.5.0, values 6 for Prox is available.

MorphoWave® 1.2.1, values 6 for Prox is available.

### [sc.verify\\_csn\\_start](#)

Parameter to set start 'bit' position to read from CSN during control.

## Values

- 0 - 79 (*0 - Default*)



### Note:

Parameter is applicable to value 'Standard CSN' or 'Reverse CSN' of [sc.verify\\_user\\_id](#).



### Warning:

It is strongly recommended to use the proper value of start 'bit' position of CSN as per Smartcard is used (start 'bit' position must be less than total length of CSN).



### Since:

MorphoAccess® 1.2.4

## [sc.verify\\_csn\\_length](#)

Parameter to set the number of 'bits'(Length) to read from CSN during control.

## Values

- 0 - 80 (*0 - Default*)

### Note:



Parameter is applicable to value 'Standard CSN' or 'Reverse CSN' of **sc.verify\_user\_id**. Default value '0' indicates to read full CSN regardless of the **sc.verify\_csn\_start**.

### Warning:



Value of parameter must be set as per the setting of **sc.verify\_csn\_start** and Smartcard CSN (**sc.verify\_csn\_length = CSN\_length - sc.verify\_csn\_start**).



### Since:

MorphoAccess® 1.2.4

## sc.enroll\_csn\_start

Parameter to set start 'bit' position to read from CSN during enrollment.

## Values

- 0 - 79 (*0 - Default*)



### Note:

Parameter is applicable to value 'Standard CSN' or 'Reverse CSN' of **sc.enroll\_user\_id**.



### Warning:

It is strongly recommended to use the proper value of start 'bit' position of CSN as per Smartcard is used (start 'bit' position must be less than total length of CSN).



### Since:

MorphoAccess® 1.2.4

## sc.enroll\_csn\_length

Parameter to set the number of 'bits'(Length) to read from CSN during enrollment.

## Values

- 0 - 80 (*0 - Default*)

### Note:



Parameter is applicable to value 'Standard CSN' or 'Reverse CSN' of **sc.enroll\_user\_id**. Default value '0' indicates to read full CSN regardless of the **sc.enroll\_csn\_start**.

### Warning:



Value of parameter must be set as per the setting of **sc.enroll\_csn\_start** and Smartcard CSN (`sc.verify_csn_length = CSN_length - sc.enroll_csn_start`).



### Since:

MorphoAccess® 1.2.4

## sc\_binary\_read.data\_type\_format

Parameter to set data type format to read binary data.

## Values

- 0 - 0xFFFFFFFF (**0** - Default)



### Note:

Parameter is used to store the value of binary read data type format.

## sc\_binary\_read.data\_type\_direction

Parameter to set data type direction to read binary data.

## Values

- 0 - Binary identifier read in LSB
- 1 - Binary identifier read in MSB (**1 - Default**)

### Example for Binary User ID Authentication:

Suppose there are two users enrolled with below ID:

- User ID = 1 (in ASCII format user id = 31)
- User ID = 72057594037927936 (in ASCII format user id = 37 32 30 35 37 35 39 34 30 33 37 39 32 37 39 33 36)
- Encode a card with data in block 4 = 0000000000000001FFFFFFFFFFFF

When such card is read by Terminal:

Suppose Data type direction = MSB first

- It reads ID starting from first bit in block 4, 8 bytes length : 00 00 00 00 00 00 00 01
- ID is MSB first (configuration parameter) so in decimal, ID read is 1
- Converted in ASCII, it gives 0x31
- Terminal asks a biometric for User ID 0x31 = '1' for authentication

Suppose Data type direction = LSB first

- It reads ID starting from first bit in block 4, 8 bytes length : 00 00 00 00 00 00 00 01
- ID is LSB first so in decimal, ID read is 72057594037927936
- Converted in ASCII, it gives 37 32 30 35 37 35 39 34 30 33 37 39 32 37 39 33 36
- Terminal asks a biometric for User ID 32 30 35 37 35 39 34 30 33 37 39 32 37 39 33 36 = '72057594037927936' for authentication

## **sc\_binary\_read.data\_offset\_num\_bytes**

Parameter to set binary reading starting position in bytes from start block.

## Values

- 0 - 4294967295 (**0** - Default)

See also:

[sc.verify\\_user\\_id](#)

**Note:**



Offset is from start block  
([sc\\_tlv\\_mifare.start\\_block](#)).

## [sc\\_binary\\_read.data\\_offset\\_add\\_bits](#)

Parameter to set binary reading starting position in bits from bytes offset.

## Values

- 0 - 4294967295 (**0** - Default)

### See also:

[sc\\_binary\\_read.data\\_offset\\_num\\_bytes](#),  
[sc.verify\\_user\\_id](#)

#### Note:



Additional bits are counted after offset in bytes.

## sc\_binary\_read.data\_length\_num\_bytes

Parameter to set number of bytes of binary data to read.

## Values

- 0 - 4294967295 (**8** - Default)

See also:

[sc.verify\\_user\\_id](#)

## [sc\\_binary\\_read.data\\_length\\_add\\_bits](#)

Parameter to set additional bits of binary data to read.

## Values

- 0 - 4294967295 (**0** - Default)

### See also:

[sc\\_binary\\_read.data\\_length\\_num\\_bytes](#),  
[sc.verify\\_user\\_id](#)

#### Note:



Additional bits are counted after length in bytes.

## sc\_tlv\_mifare\_plus.start\_block

Set start block number to read/write MIFARE® Plus SL3 Morpho cards.

## Values

- 1 - 215 (**4** - Default)



**Since:**

MorphoWave® 1.1.0

## sc\_tlv\_mifare\_plus.num\_block

Set number of data blocks to read MIFARE® Plus SL3 Morpho cards (sector trailers are skipped).

## Values

- 0 - 216 (**84** - Default)



**Since:**

MorphoWave® 1.1.0

## `sc_tlv_mifare_plus.key_policy`

Set key policy to read MIFARE® Plus Morpho cards.

## Values

- 1 - Try to read card first with Key A then Key B (**1 - Default**)
- 2 - Try to read card with Key A
- 3 - Try to read card with Key B



**Since:**

MorphoWave® 1.1.0

## sc.HID\_card\_number\_format

Applicable only to terminals with HID capabilities.

Parameter to define Wiegand format of HID application for HID cards.

## Values

- [\*\*Wiegand\\_format\\_type::type\*\*](#)

Default value:

[\*\*Wiegand\\_format\\_type::wiegand\\_fmt\\_standard\\_26\*\*](#)

### Note:



- Custom format (i.e. [\*\*Wiegand\\_format\\_type::wiegand\\_fmt\\_custom\\_slot0\*\*](#) to [\*\*Wiegand\\_format\\_type::wiegand\\_fmt\\_custom\\_slot7\*\*](#)) can only be set if format is defined in corresponding slot
- For Prox product refer [\*\*wiegand.prox\\_port\\_input\\_format\*\*](#)



### Since:

MorphoAccess® 1.3.2

## sc.encrypted\_data

Parameter to enable encryption on Smartcard data.

## Values

- 0 - Disable data encryption on Smartcard. Smartcard encoding is always in plain(unencrypted) data. Smartcard reading supports plain(unencrypted) data and encrypted data.(0 - Default)
- 1 - Enable data encryption on Smartcard. Smartcard encoding is always in encrypted data. Smartcard reading supports only encrypted data.



**Since:**

MorphoAccess® 4.6.0

MorphoWave® 1.3.0

Copyright © 2024, IDEMIA, All rights reserved. Reproduction in whole or in part in any form or medium without the express written permission of IDEMIA is prohibited.

# Access and Time Biometric Terminals Parameters Guide

[Main Page](#)

[Modules](#)

[Classes](#)

Defines

## TCP client

---

## Detailed Description

Biometric terminals are capable of connecting to TCP server and wait for distant commands to be executed. This section describes parameters associated with TCP server configuration.

**Since:**



MorphoAccess® 1.6.0 SIGMA / SIGMA Extreme  
MorphoAccess® 3.0.0 SIGMA Lite / SIGMA Lite+

## Define Documentation

### **comm\_channels\_state.TCP\_client**

Parameter to enable/disable TCP client.

If enabled, the terminal tries to connect to PC(using **TCP\_client.host\_ip** and **TCP\_client.host\_port**).

## Values

- 0 - Disable (**0 - Default**)
- 1 - Enable

### TCP\_client.host\_ip

IP address of the machine where server is running.

### TCP\_client.host\_port

Mutually decided port number between server and client.

## Values

- 1 - 65535 (**11022** - Default)

## TCP\_client.connection\_period

Period before retrying a connection after previous one ends (failed or succeeded).

## Values

- 10 - 86400 (**60** - Default)



### Note:

Value of period is in seconds

## TCP\_client.connection\_timeout

Read/Write/Idle timeout after connection to the server is established.

## Values

- 10 - 600 (**10** - Default)



### Note:

Value of timeout is in seconds

## TCP\_client.connection\_retry

Number of retry attempt in case of connection to the server is not established.

## Values

- 0 - 10 (**0** - Default)

### TCP\_client.SSL\_conn\_state

Parameter to enable/disable SSL/TLS on TCP client channel. In case where comm\_channels\_state.TCP\_client as well as TCP\_client.SSL\_conn\_state both are on, then SSL/TLS is applied on TCP client channel and normal TCP client over TCP socket will be stopped/closed.

## Values

- 0 - Disable
- 1 - Enable (**1** - Default)

### Note:



In Enforced Security mode this key cannot be modified. Modification is only possible by switching to On-Demand security mode (using MorphoBioToolBox or by thrift command 'terminal\_set\_security\_state').



### Since:

MorphoAccess® 4.6.0  
MorphoWave® 1.2.0

## TCP\_client.profile\_id

Define SSL profile to be used for SSL/TLS on TCP client.

## Values

- 0 - Use profile 0 (*0 - Default*)
- 1 - Use profile 1



**Since:**

MorphoAccess® 4.6.0

MorphoWave® 1.2.0

Copyright © 2024, IDEMIA, All rights reserved. Reproduction in whole or in part in any form or medium without the express written permission of IDEMIA is prohibited.

# Access and Time Biometric Terminals Parameters Guide

[Main Page](#)

[Modules](#)

[Classes](#)

Defines

## TOR Mode

---

## Detailed Description

Terminal supports a Time override mode function to check if the door does not remain open for too long (time is configurable). A dedicated license (MA\_TOR) is required for the below configuration keys to be available.



**Since:**

MorphoAccess® 4.6.11

---

## Define Documentation

`time_override_mode.tor_mode`

Enable/Disable TOR Mode feature.

## Values

### SIGMA / SIGMA Lite / SIGMA Lite+ / SIGMA Extreme

- 0 - Disable (*Default*)
- 1 - Enable

### MWC / VisionPass / MWSP / VisionPass SP

Not applicable

## **time\_override\_mode.tor\_mode\_F1\_KEY**

Parameter to define the time override mode duration value, for the T&A key F1.

## Values

### SIGMA / SIGMA Lite / SIGMA Lite+ / SIGMA Extreme

- 1 - 43200 (**300** - Default)

### MWC / VisionPass / MWSP / VisionPass SP

Not applicable

## **time\_override\_mode.tor\_mode\_F2\_KEY**

Parameter to define the time override mode duration value, for the T&A key F2.

## Values

### SIGMA / SIGMA Lite / SIGMA Lite+ / SIGMA Extreme

- 1 - 43200 (**300** - Default)

### MWC / VisionPass / MWSP / VisionPass SP

Not applicable

## **time\_override\_mode.tor\_mode\_F3\_KEY**

Parameter to define the time override mode duration value, for the T&A key F3.

## Values

### SIGMA / SIGMA Lite / SIGMA Lite+ / SIGMA Extreme

- 1 - 43200 (**300** - Default)

### MWC / VisionPass / MWSP / VisionPass SP

Not applicable

## **time\_override\_mode.tor\_mode\_F4\_KEY**

Parameter to define the time override mode duration value, for the T&A key F4.

## Values

### SIGMA / SIGMA Lite / SIGMA Lite+ / SIGMA Extreme

- 1 - 43200 (**300** - Default)

### MWC / VisionPass / MWSP / VisionPass SP

Not applicable

### **time\_override\_mode.tor\_mode\_EXPIRATION\_TIME**

The terminal will display an alert message after **time\_override\_mode.tor\_mode\_EXPIRATION\_TIME** if the door is still opened to warn that the door will be closed shortly.

## Values

### SIGMA / SIGMA Lite / SIGMA Lite+ / SIGMA Extreme

- 1 - 43200 (**300** - Default)

### MWC / VisionPass / MWSP / VisionPass SP

Not applicable

Copyright © 2024, IDEMIA, All rights reserved. Reproduction in whole or in part in any form or medium without the express written permission of IDEMIA is prohibited.

# Access and Time Biometric Terminals Parameters Guide

[Main Page](#)

[Modules](#)

[Classes](#)

Defines

## Tamper

---

## **Detailed Description**

Biometric terminals can detect two intrusion attempt types:

- Someone tries to steal the complete terminal,
- Someone tries to open the terminal

On such intrusions, tamper switch is triggered on the terminal. It can sound off the alarm and transmit an alarm alert to a remote host using an output channel. Contact connections are provided on I/O board for the same (open circuit equals detection).

---

## Define Documentation

### tamper.state

Parameter to enable/disable tamper detection.

## Values

- 0 - Disable (**0 - Default**)
- 1 - Enable
- 2 - Clear and re-enable tamper

## MWC / VisionPass / MWSP / VisionPass SP

- 3 - Enable and temporary suspend tamper detection. Refer to [\*\*tamper.suspension\\_duration\*\*](#).

### Note:



- After clearing tamper (value 2), this parameter is set to value 1 by the terminal.
- Tamper suspension is disabled once tamper switch is back to normal for defined time or automatically after suspension duration time.

## [\*\*tamper.action\\_auth\\_iden\*\*](#)

Parameter to disable user control on tamper detection.

## Values

- 0 - User control not interrupted (**0** - *Default*)
- 1 - User control disabled

### tamper.action\_play\_mmi

Parameter to enable/disable MMI playing on tamper detection.

## Values

- 0 - No MMI
- 1 - Play MMI (sound and message) (**1** - *Default*)

## tamper.action\_erase\_biometrics

Parameter to enable/disable erasing user database on tamper detection.

## Values

- 0 - Biometrics database not deleted (**0** - Default)
- 1 - Biometrics database deleted

## tamper.action\_erase\_security\_data

Parameter to enable/disable erasing security data on tamper detection.

## Values

- 0 - Security data not deleted (**0** - Default)
- 1 - Security data deleted

## tamper.alarm\_interval

Parameter to set time interval for sending alarm to a remote server on tamper.

## Values

- 0 - 3000 (**1500** - Default)



### Note:

Interval in multiples of 10 milliseconds.

## tamper.photo\_taking

Parameter to enable/disable capture photo on tamper detection.

## Values

### SIGMA Extreme

- 0 - Disable photo capture on tamper detection(**0 - Default**)
- 1 - Enable photo capture on tamper detection



**Since:**

MorphoAccess® 4.0.0

### SIGMA / SIGMA Lite / SIGMA Lite+ / MWC / VisionPass / MWSP / VisionPass SP

Not applicable

## tamper.suspension\_duration

Parameter to set duration of tamper suspension.

After expiration of this duration, or 30s after closing the tamper, suspension is automatically disabled and terminal starts monitoring tamper switch.

## Values

### MWC / VisionPass / MWSP / VisionPass SP

- 60 - 600 (**60** - Default)

### SIGMA / SIGMA Lite / SIGMA Lite+ / SIGMA Extreme

Not applicable



#### Note:

Duration in seconds.

Copyright © 2024, IDEMIA, All rights reserved. Reproduction in whole or in part in any form or medium without the express written permission of IDEMIA is prohibited.

# Access and Time Biometric Terminals Parameters Guide

[Main Page](#)

[Modules](#)

[Classes](#)

Defines

## Terminal Information

---

## **Detailed Description**

Using parameters in this section, some terminal information can be customized to be displayed to users.

---

## Define Documentation

### **terminal\_information.desc\_name**

Parameter to set a descriptive name of the terminal.

The terminal name is used in USB export features and in videophone.

## **Values**

Any string containing characters from 0 to 9, A to Z, a to z.  
Allowed name size is max. 192 bytes.

## **MWC**

Default value: "MORPHOWAVE COMPACT"

## **SIGMA / SIGMA Lite / SIGMA Lite+ / SIGMA Extreme**

Default value: "MORPHOACCESS"

## **VisionPass**

Default value: "VisionPass"

## **MWSP**

Default value: "MorphoWaveSP"

## **VisionPass SP**

Default value: "VisionPassSP"

Copyright © 2024, IDEMIA, All rights reserved. Reproduction in whole or in part in any form or medium without the express written permission of IDEMIA is prohibited.

# Access and Time Biometric Terminals Parameters Guide

[Main Page](#)

[Modules](#)

[Classes](#)

Defines

## Threat Level

---

## **Detailed Description**

This feature allows users to set Threat Level (the level of global security) of terminal for user control as per configuration. Current threat level can be changed using 2 GPIO or command as per selected mode.

---

## Define Documentation

### `gpio.threat_level_mode`

Terminal threat level mode.

Input pins based, command based or disabled.

Only useful when `gpio.func_mode` is configured to **Threat Level mode**

## Values

- 0 - Threat Level is based on the GPI input pins status
- 1 - Threat Level is defined by the **gpio.cmd\_based\_active\_threat\_level** parameter
- 2 - Threat Level is disabled (**2 - Default**)

### gpio.cmd\_based\_active\_threat\_level

Parameter to set the current threat level.

Applicable only when **gpio.threat\_level\_mode** is set to 1.

## Values

- 0 to 3 - Threat level (**1** - Default)

See also:

[gpio.threat\\_level\\_mode](#)

## [gpio.threat\\_level\\_gpi\\_0](#)

Threat level value for GPIO=LOW and GPI1=LOW.

Applicable only when [gpio.threat\\_level\\_mode](#) is set to 0.

## Values

- 0 - 3 (*0 - Default*) 0 for Threat level 0 up to 3 for Threat level 3

See also:

[gpio.threat\\_level\\_mode](#)

## [gpio.threat\\_level\\_gpi\\_1](#)

Threat level value for GPIO0=HIGH and GPIO1=LOW.

Applicable only when [gpio.threat\\_level\\_mode](#) is set to 0.

## Values

- 0 - 3 (**1** - *Default*) 0 for Threat level 0 up to 3 for Threat level 3

### See also:

[gpio.threat\\_level\\_mode](#)

## gpio.threat\_level\_gpi\_2

Threat level value for GPIO=LOW and GPI1=HIGH.

Applicable only when [gpio.threat\\_level\\_mode](#) is set to 0.

## Values

- 0 - 3 (**2** - *Default*) 0 for Threat level 0 up to 3 for Threat level 3

### See also:

[gpio.threat\\_level\\_mode](#)

## gpio.threat\_level\_gpi\_3

Threat level value for GPIO0=HIGH and GPIO1=HIGH.

Applicable only when [gpio.threat\\_level\\_mode](#) is set to 0.

## Values

- 0 - 3 (**3** - *Default*) 0 for Threat level 0 up to 3 for Threat level 3

See also:

[gpio.threat\\_level\\_mode](#)

Copyright © 2024, IDEMIA, All rights reserved. Reproduction in whole or in part in any form or medium without the express written permission of IDEMIA is prohibited.

# Access and Time Biometric Terminals Parameters Guide

[Main Page](#)

[Modules](#)

[Classes](#)

Defines

## Time and Attendance

---

## **Detailed Description**

This section contains parameters related to Time and Attendance.

When Time & Attendance mode is enabled, the terminal logs capture details such as entry time, lunch in/out, exit on user control.

---

## Define Documentation

### `time_and_attendance.tna_mode`

Parameter to enable or disable the Time and Attendance mode (T&A).

## Values

**SIGMA / SIGMA Lite+ / SIGMA Extreme / MWC / VisionPass / VisionPass SP**

- 0 - T&A is disabled (**0 - Default**)
- 1 - T&A mode is enabled

**SIGMA Lite / MWSP**

Not applicable

## time\_and\_attendance.tna\_mandatory\_mode

Parameter to set T&A as mandatory or optional.

If it is set as mandatory, it is compulsory for the user to enter T&A input.

## Values

### SIGMA / SIGMA Lite+ / SIGMA Extreme / MWC

- 0 - T&A action selection is not mandatory (*0 - Default*)
- 1 - T&A action selection is mandatory

### SIGMA Lite / VisionPass / MWSP / VisionPass SP

Not applicable

## time\_and\_attendance.tna\_user\_control

Parameter to set the T&A action order.

This parameter indicates if T&A action should be selected after or before user control.

## Values

### SIGMA / SIGMA Lite+ / SIGMA Extreme / MWC

- 0 - T&A action is requested before or after user control (**0 - Default**)
- 1 - T&A action is requested after user control

### SIGMA Lite / VisionPass / MWSP / VisionPass SP

Not applicable

## time\_and\_attendance.tna\_extended\_mode

Parameter to select 4 or 16 actions mode of T&A.

When extended Time & Attendance is enabled, there are 16 actions are enabled indicating 16 function keys that are configurable and displayed to the user for T&A function selection.

## Values

### SIGMA / SIGMA Extreme / MWC / VisionPass / VisionPass SP

- 0 - Normal 4 actions mode T&A (**0 - Default**)
- 1 - Extended 16 actions mode T&A
- 2 - Extended 16 actions mode T&A with 2x8 screen

### SIGMA Lite / SIGMA Lite+ / MWSP

Not applicable



**Since:**

MorphoAccess® 1.3.5, Option 2 is available

### time\_and\_attendance.tna\_message\_timeout

Parameter to set the duration of an Access control result message and a T&A message displayed on terminal LCD.

## Values

### SIGMA / SIGMA Lite+ / SIGMA Extreme

- 0 - no access control result message and T&A message shall be displayed
- 100 - 20000 (**3000 - Default**)



#### Note:

Timeout in milliseconds

### MWC / VisionPass / VisionPass SP

- 1 - 60 (**3 - Default**)



#### Note:

Timeout in seconds

### SIGMA Lite / MWSP

Not applicable

## time\_and\_attendance.message\_text\_mode

Parameter to choose whether 4 actions mode uses texts or icons.

In text mode, text displayed on LCD can be customized. In icon mode, the pre-set icons/images are displayed for function keys.

## Values

### SIGMA / SIGMA Extreme / MWC / VisionPass / VisionPass SP

- 0 - 4 actions in texts (*0 - Default*)
- 1 - 4 actions in icons

### SIGMA Lite / SIGMA Lite+ / MWSP

Not applicable

### **time\_and\_attendance.f1\_key\_message\_text**

Parameter to define T&A F1 key message text (normal mode).

## **Values**

**SIGMA / SIGMA Lite+ / SIGMA Extreme / MWC / VisionPass / VisionPass SP**

Any UTF8-string containing max. 40 bytes.

Default value: "IN"

**SIGMA Lite / MWSP**

Not applicable

## **time\_and\_attendance.f2\_key\_message\_text**

Parameter to define T&A F2 key message text (normal mode).

## **Values**

**SIGMA / SIGMA Lite+ / SIGMA Extreme / MWC / VisionPass / VisionPass SP**

Any UTF8-string containing max. 40 bytes.

Default value: "OUT"

**SIGMA Lite / MWSP**

Not applicable

## **time\_and\_attendance.f3\_key\_message\_text**

Parameter to define T&A F3 key message text (normal mode).

## Values

### **SIGMA / SIGMA Extreme / MWC / VisionPass / VisionPass SP**

Any UTF8-string containing max. 40 bytes.

Default value: "IN DUTY"

### **SIGMA Lite / SIGMA Lite+ / MWSP**

Not applicable

## **time\_and\_attendance.f4\_key\_message\_text**

Parameter to define T&A F4 key message text (normal mode).

## **Values**

### **SIGMA / SIGMA Extreme / MWC / VisionPass / VisionPass SP**

Any UTF8-string containing max. 40 bytes.

Default value: "OUT DUTY"

### **SIGMA Lite / SIGMA Lite+ / MWSP**

Not applicable

## **time\_and\_attendance.ext\_f1\_key\_message\_text**

Parameter to define T&A F1 key message text (extended mode).

## **Values**

### **SIGMA / SIGMA Extreme / MWC / VisionPass / VisionPass SP**

Any UTF8-string containing max. 40 bytes.

Default value: "IN1"

### **SIGMA Lite / SIGMA Lite+ / MWSP**

Not applicable

## **time\_and\_attendance.ext\_f2\_key\_message\_text**

Parameter to define T&A F2 key message text (extended mode).

## Values

### **SIGMA / SIGMA Extreme / MWC / VisionPass / VisionPass SP**

Any UTF8-string containing max. 40 bytes.

Default value: "IN2"

### **SIGMA Lite / SIGMA Lite+ / MWSP**

Not applicable

## time\_and\_attendance.ext\_f3\_key\_message\_text

Parameter to define T&A F3 key message text (extended mode).

## **Values**

### **SIGMA / SIGMA Extreme / MWC / VisionPass / VisionPass SP**

Any UTF8-string containing max. 40 bytes.

Default value: "IN3"

### **SIGMA Lite / SIGMA Lite+ / MWSP**

Not applicable

## **time\_and\_attendance.ext\_f4\_key\_message\_text**

Parameter to define T&A F4 key message text (extended mode).

## **Values**

### **SIGMA / SIGMA Extreme / MWC / VisionPass / VisionPass SP**

Any UTF8-string containing max. 40 bytes.

Default value: "IN4"

### **SIGMA Lite / SIGMA Lite+ / MWSP**

Not applicable

## **time\_and\_attendance.ext\_f5\_key\_message\_text**

Parameter to define T&A F5 key message text (extended mode).

## **Values**

### **SIGMA / SIGMA Extreme / MWC / VisionPass / VisionPass SP**

Any UTF8-string containing max. 40 bytes.

Default value: "OUT1"

### **SIGMA Lite / SIGMA Lite+ / MWSP**

Not applicable

## **time\_and\_attendance.ext\_f6\_key\_message\_text**

Parameter to define T&A F6 key message text (extended mode).

## **Values**

### **SIGMA / SIGMA Extreme / MWC / VisionPass / VisionPass SP**

Any UTF8-string containing max. 40 bytes.

Default value: "OUT2"

### **SIGMA Lite / SIGMA Lite+ / MWSP**

Not applicable

## **time\_and\_attendance.ext\_f7\_key\_message\_text**

Parameter to define T&A F7 key message text (extended mode).

## **Values**

### **SIGMA / SIGMA Extreme / MWC / VisionPass / VisionPass SP**

Any UTF8-string containing max. 40 bytes.

Default value: "OUT3"

### **SIGMA Lite / SIGMA Lite+ / MWSP**

Not applicable

## **time\_and\_attendance.ext\_f8\_key\_message\_text**

Parameter to define T&A F8 key message text (extended mode).

## **Values**

### **SIGMA / SIGMA Extreme / MWC / VisionPass / VisionPass SP**

Any UTF8-string containing max. 40 bytes.

Default value: "OUT4"

### **SIGMA Lite / SIGMA Lite+ / MWSP**

Not applicable

## **time\_and\_attendance.ext\_f9\_key\_message\_text**

Parameter to define T&A F9 key message text (extended mode).

## **Values**

### **SIGMA / SIGMA Extreme / MWC / VisionPass / VisionPass SP**

Any UTF8-string containing max. 40 bytes.

Default value: "IN DUTY1"

### **SIGMA Lite / SIGMA Lite+ / MWSP**

Not applicable

## **time\_and\_attendance.ext\_f10\_key\_message\_text**

Parameter to define T&A F10 key message text (extended mode).

## **Values**

### **SIGMA / SIGMA Extreme / MWC / VisionPass / VisionPass SP**

Any UTF8-string containing max. 40 bytes.

Default value: "IN DUTY2"

### **SIGMA Lite / SIGMA Lite+ / MWSP**

Not applicable

## **time\_and\_attendance.ext\_f11\_key\_message\_text**

Parameter to define T&A F11 key message text (extended mode).

## Values

### **SIGMA / SIGMA Extreme / MWC / VisionPass / VisionPass SP**

Any UTF8-string containing max. 40 bytes.

Default value: "IN DUTY3"

### **SIGMA Lite / SIGMA Lite+ / MWSP**

Not applicable

## time\_and\_attendance.ext\_f12\_key\_message\_text

Parameter to define T&A F12 key message text (extended mode).

## Values

### **SIGMA / SIGMA Extreme / MWC / VisionPass / VisionPass SP**

Any UTF8-string containing max. 40 bytes.

Default value: "IN DUTY4"

### **SIGMA Lite / SIGMA Lite+ / MWSP**

Not applicable

## time\_and\_attendance.ext\_f13\_key\_message\_text

Parameter to define T&A F13 key message text (extended mode).

## **Values**

### **SIGMA / SIGMA Extreme / MWC / VisionPass / VisionPass SP**

Any UTF8-string containing max. 40 bytes.

Default value: "OUT DUTY1"

### **SIGMA Lite / SIGMA Lite+ / MWSP**

Not applicable

## **time\_and\_attendance.ext\_f14\_key\_message\_text**

Parameter to define T&A F14 key message text (extended mode).

## **Values**

### **SIGMA / SIGMA Extreme / MWC / VisionPass / VisionPass SP**

Any UTF8-string containing max. 40 bytes.

Default value: "OUT DUTY2"

### **SIGMA Lite / SIGMA Lite+ / MWSP**

Not applicable

## **time\_and\_attendance.ext\_f15\_key\_message\_text**

Parameter to define T&A F15 key message text (extended mode).

## Values

### **SIGMA / SIGMA Extreme / MWC / VisionPass / VisionPass SP**

Any UTF8-string containing max. 40 bytes.

Default value: "OUT DUTY3"

### **SIGMA Lite / SIGMA Lite+ / MWSP**

Not applicable

## time\_and\_attendance.ext\_f16\_key\_message\_text

Parameter to define T&A F16 key message text (extended mode).

## **Values**

### **SIGMA / SIGMA Extreme / MWC / VisionPass / VisionPass SP**

Any UTF8-string containing max. 40 bytes.

Default value: "OUT DUTY4"

### **SIGMA Lite / SIGMA Lite+ / MWSP**

Not applicable

## **time\_and\_attendance.key\_select\_timeout**

Parameter to set the duration within which user action selection is prompted for T&A.

## Values

**SIGMA / SIGMA Lite+ / SIGMA Extreme / MWC / VisionPass / VisionPass SP**

- 3 - 60 (**10** - Default)

**SIGMA Lite / MWSP**

Not applicable



**Note:**

Timeout in seconds

### **time\_and\_attendance.active\_key\_timeout**

Parameter to set the duration within which user action is prompted for T&A.

After timeout, the active key is reset.

## Values

### SIGMA / SIGMA Lite+ / SIGMA Extreme / MWC

- 3 - 60 (**10** - Default)

### SIGMA Lite / VisionPass / MWSP / VisionPass SP

Not applicable



#### Note:

Timeout in seconds

## time\_and\_attendance.jobcode\_by\_key

Parameter to map Enable/Disable Jobcode by f\_key.

For example, if 1st bit is set to 0, then terminal do not ask for job code for F\_KEY\_1 in identification and authentication.

## Values

### SIGMA / SIGMA Extreme / MWC / VisionPass / VisionPass SP

- 0 - 65535 (**65535** - *Default*)



**Since:**  
MorphoAccess® 1.5.0

### SIGMA Lite / SIGMA Lite+ / MWSP

Not applicable

Copyright © 2024, IDEMIA, All rights reserved. Reproduction in whole or in part in any form or medium without the express written permission of IDEMIA is prohibited.

# Access and Time Biometric Terminals Parameters Guide

[Main Page](#)

[Modules](#)

[Classes](#)

Defines

## Transaction Log

## Detailed Description

Biometric terminals can record each event occurred at a terminal. Such logs which contain both triggered actions and terminal results, are called transaction logs. Transaction logs are stored in a rolling file.

The events that can be logged are:

- Successful User identification
- Failure of User identification
- Time and Attendance actions
- Error occurrences
- Image capture and storage with Face detection
- ...



**Note:**

Events that are cancelled by user are not logged.

All events are recorded in a local file. The logs contains varied information, such as User ID, Name of User, Role of User, Time of action triggered, Biometric Matching Score, ...

---

## Define Documentation

### `transaction_log.logging`

Parameter to enable/disable transactions logging.

## Values

- 0 - No Log
- 1 - Access Control Logs. Only user control results along with timings and profile details are logged.
- 2 - Full Logs. All actions performed on terminal are logged. (2 - *Default*)

### Note:



For MorphoAccess® Extreme only, photo resolution in transaction logs will be 640x480 instead of 320x240 if value for this key is set to (2 - Full Logs).

## transaction\_log.action\_erase\_log

Parameter to set erase policy when log file is full.

The number of logs which can be stored depends on available licenses in terminal.

## Values

- 0 - Erase specific number of logs (**0** - Default)
- 1 - Erase all logs

See also:

[transaction\\_log.action\\_num\\_erase\\_log](#)

## [transaction\\_log.action\\_num\\_erase\\_log](#)

Parameter to set the number of logs to be erased when log file is full.

This parameter is used only if 'transaction\_log.action\_erase\_log' is set to 0.

## Values

- 0 - 100000 (**1** - *Default*)

See also:

[transaction\\_log.action\\_erase\\_log](#)

## [transaction\\_log.format](#)

Parameter to select the type of logs. When identified logs is selected, each log contains a timestamp and a unique identifier.

## Values

- 0 - Standard logs (**0 - Default**)
- 1 - Identified logs

### Note:



All previous logs will be lost as an effect of parameter change. The transaction log mode will be applicable only after terminal reboot.



### Since:

MorphoAccess® 4.5.0  
MorphoWave® 1.1.0

Copyright © 2024, IDEMIA, All rights reserved. Reproduction in whole or in part in any form or medium without the express written permission of IDEMIA is prohibited.

# Access and Time Biometric Terminals Parameters Guide

[Main Page](#)

[Modules](#)

[Classes](#)

Defines

## User Control Configuration

---

## **Detailed Description**

This section consists in user control(authentication and identification) related parameters.

---

## Define Documentation

### **ucc.trigger\_event**

Parameter to configure the specific triggered events, on which the terminal will initiate a user control workflow, at threat level 0: biometric input, contactless card, keypad, external port trigger or QR code.

Bit field value:

- bit 4 - QR code
- bit 3 - External port
- bit 2 - Keypad
- bit 1 - Contactless card
- bit 0 - Biometric input

## Values

### SIGMA Lite+ / SIGMA / SIGMA Extreme

- 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15 (**3 - Default**)

### SIGMA Lite

- 0, 1, 2, 3, 8, 9, 10, 11 (**3 - Default**)

### MWC

- 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31 (**3 - Default**)

### VisionPass

- 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31 (**1 - Default**)

### MWSP

- 0, 1, 2, 3, 8, 9, 10, 11, 16, 17, 18, 19, 24, 25, 26, 27 (**3 - Default**)

### VisionPass SP

- 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15 (**1 - Default**)

#### Warning:



For MORPHOWAVE SP products, User additional controls are not applicable to QR code credentials. Terminal reads a User ID from a QR code and sends it to the controller. This may be leveraged by an attacker to bypass other controls of the terminal (biometric control for instance). If you enable the QR code feature, please evaluate the possible security vulnerabilities on the overall system

## ucc.trigger\_event\_TL1

Parameter to configure on which triggered events, terminal should start user control workflow, at threat level 1.

## Values

### SIGMA Lite

Default value: 11

### SIGMA Lite+ / SIGMA / SIGMA Extreme / VisionPass SP

Default value: 15

### MWC / VisionPass

Default value: 31

### MWSP

Default value: 27

#### See also:

[ucc.trigger\\_event](#)

## [ucc.trigger\\_event\\_TL2](#)

Parameter to configure the triggered events, on which the terminal should initiate user control workflow, at threat level 2.

## Values

### SIGMA Lite

Default value: 11

### SIGMA Lite+ / SIGMA / SIGMA Extreme / VisionPass SP

Default value: 15

### MWC / VisionPass

Default value: 31

### MWSP

Default value: 27

#### See also:

[ucc.trigger\\_event](#)

## [ucc.trigger\\_event\\_TL3](#)

Parameter to configure the triggered events, on which the terminal should initiate user control workflow, at threat level 3.

## Values

### SIGMA Lite

Default value: 11

### SIGMA Lite+ / SIGMA / SIGMA Extreme / VisionPass SP

Default value: 15

### MWC / VisionPass

Default value: 31

### MWSP

Default value: 27

#### See also:

[ucc.trigger\\_event](#)

## [ucc.user\\_record\\_reference](#)

Parameter to configure user record reference source to be used during user control operation, at threat level 0.

## Values

- If "0", then reference source is based on trigger event (**0 - Default**)

i.e. reference is smartcard for smartcard trigger source, QR code for QR code trigger source and terminal for other trigger source.

- If "1", reference is terminal for all trigger sources.

### [ucc.user\\_record\\_reference\\_TL1](#)

Same as [ucc.user\\_record\\_reference](#) but for threat level 1.

**See also:**

[ucc.user\\_record\\_reference](#)

### [ucc.user\\_record\\_reference\\_TL2](#)

Same as [ucc.user\\_record\\_reference](#) but for threat level 2.

**See also:**

[ucc.user\\_record\\_reference](#)

### [ucc.user\\_record\\_reference\\_TL3](#)

Same as [ucc.user\\_record\\_reference](#) but for threat level 3.

**See also:**

[ucc.user\\_record\\_reference](#)

### [ucc.per\\_user\\_rules](#)

Biometric terminal allows to configure rules for specific users.

One can set user-based rules at the time of enrolment or set them in the user template. A user rule could contain the allowed trigger source, record reference source, the additional controls to be performed, and BIO substitution policy.

This parameter configures the terminal to use user-based rules at threat level 0.

## Values

- If "0", it means per user rule check is disabled. (**0 - Default**)
- If "1", it means per user rule check is enabled and user rule reference is trigger\_event.

i.e. user rules are retrieved from smartcard or QR Code if trigger source is smartcard or QR code respectively else user rules are from terminal's database.

- If "2", it means per user rule check is enabled and user rule reference is terminal for all trigger sources.

### Note:



- If no user rules are specified for a given user because the field is missing on the card or in the terminal database, the user will be rejected.
- When using QR codes: the user rule is always ID only if "per user rule" check is enabled and user rule reference is trigger\_event.

### [ucc.per\\_user\\_rules\\_TL1](#)

Same as [ucc.per\\_user\\_rules](#) but for threat level 1.

#### See also:

[ucc.per\\_user\\_rules](#)

### [ucc.per\\_user\\_rules\\_TL2](#)

Same as [ucc.per\\_user\\_rules](#) but for threat level 2.

#### See also:

[ucc.per\\_user\\_rules](#)

### [ucc.per\\_user\\_rules\\_TL3](#)

Same as [ucc.per\\_user\\_rules](#) but for threat level 3.

#### See also:

[ucc.per\\_user\\_rules](#)

### [ucc.check\\_additional\\_users](#)

Parameter to enable/disable multi-user controls to grant the access.

When this feature is enabled, the terminal perform verification of two users and grant access if both authenticated successfully.

## Values

SIGMA / SIGMA Lite / SIGMA Lite+ / SIGMA Extreme / MWC / MWSP

- 0 - 1 (**0 - Default**)

VisionPass / VisionPass SP

Not applicable

### [ucc.check\\_additional\\_users\\_TL1](#)

Same as [ucc.check\\_additional\\_users](#) but for threat level 1.

**See also:**

[ucc.check\\_additional\\_users](#)

### [ucc.check\\_additional\\_users\\_TL2](#)

Same as [ucc.check\\_additional\\_users](#) but for threat level 2.

**See also:**

[ucc.check\\_additional\\_users](#)

### [ucc.check\\_additional\\_users\\_TL3](#)

Same as [ucc.check\\_additional\\_users](#) but for threat level 3.

**See also:**

[ucc.check\\_additional\\_users](#)

### [misc.multifinger\\_timeout](#)

Related to additional users check, parameter to set a duration within which another user have to provide his credentials for controls.

## Values

SIGMA / SIGMA Lite / SIGMA Lite+ / SIGMA Extreme

- 1 - 30 (**20** - Default)



**Note:**

Timeout is in seconds.

VisionPass / MWSP / VisionPass SP

Not applicable

MWC

Deprecated since Version 2.4.0, Please refer alternative parameter **misc.multiuser\_timeout**

### **misc.multiuser\_timeout**

Related to additional users check, parameter to set a duration within which another user have to provide his credentials for controls.

## Values

### MWC / MWSP

- 1 - 30 (**20** - Default)



**Note:**

Timeout is in seconds.

### SIGMA / SIGMA Lite / SIGMA Lite+ / SIGMA Extreme / VisionPass SP / VisionPass

Not applicable

## ucc.allow\_record\_fallback

Parameter to allow terminal to look for backup data in terminal database.

When user\_record\_reference that is supposed to be in the smartcard has some data missing, required for allowing control, this parameter makes the terminal looking for the missing data in the user database.

## Values

- 0 - Fallback not allowed (**0 - Default**)
- 1 - Fallback allowed

### [ucc.allow\\_record\\_fallback\\_TL1](#)

Same as [ucc.allow\\_record\\_fallback](#) but for threat level 1.

**See also:**

[ucc.allow\\_record\\_fallback](#)

### [ucc.allow\\_record\\_fallback\\_TL2](#)

Same as [ucc.allow\\_record\\_fallback](#) but for threat level 2.

**See also:**

[ucc.allow\\_record\\_fallback](#)

### [ucc.allow\\_record\\_fallback\\_TL3](#)

Same as [ucc.allow\\_record\\_fallback](#) but for threat level 3.

**See also:**

[ucc.allow\\_record\\_fallback](#)

### [ucc.allow\\_biopin\\_user\\_rule](#)

Biopin Check feature allows replacing biometric check, by a numeric code (BIOPIN or PIN) check.

## Values

### SIGMA / SIGMA Lite+ / SIGMA Extreme / MWC

- 0 - BIO substitution not allowed for all the users. (**0 - Default**)
- 1 - BIO substitution and BIO check is substituted by BIOPIN check. BIOPIN data is only stored on smartcard.
- 2 - BIO substitution and BIO check is substituted by PIN check.

### VisionPass / VisionPass SP

- 0 - BIO substitution not allowed for all the users. (**0 - Default**)
- 2 - BIO substitution and BIO check is substituted by PIN check.

### SIGMA Lite / MWSP

Not applicable



#### Note:

If substitution by PIN is allowed and PIN control is also enabled, then only one PIN check is performed

### [ucc.allow\\_biopin\\_user\\_rule\\_TL1](#)

Same as [ucc.allow\\_biopin\\_user\\_rule](#) but for threat level 1.

#### See also:

[ucc.allow\\_biopin\\_user\\_rule](#)

### [ucc.allow\\_biopin\\_user\\_rule\\_TL2](#)

Same as [ucc.allow\\_biopin\\_user\\_rule](#) but for threat level 2.

#### See also:

[ucc.allow\\_biopin\\_user\\_rule](#)

### [ucc.allow\\_biopin\\_user\\_rule\\_TL3](#)

Same as [ucc.allow\\_biopin\\_user\\_rule](#) but for threat level 3.

#### See also:

[ucc.allow\\_biopin\\_user\\_rule](#)

### [ucc.allow\\_duress\\_finger](#)

User who has registered duress finger can generate duress alarm.

Duress alarm is only generated if biometric check is successful.

## Values

### SIGMA / SIGMA Lite / SIGMA Lite+ / SIGMA Extreme

- 0 - Duress finger check is disabled. (**0 - Default**)
- 1 - Duress finger check is enabled and set to 'Alarm only'. The standard workflow applies, but an additional "duress alarm" event is raised before the eventual user acceptance or rejection.

### MWC / VisionPass / MWSP / VisionPass SP

Not applicable

#### [ucc.allow\\_duress\\_finger\\_TL1](#)

Same as [ucc.allow\\_duress\\_finger](#) but for threat level 1.

**See also:**

[ucc.allow\\_duress\\_finger](#)

#### [ucc.allow\\_duress\\_finger\\_TL2](#)

Same as [ucc.allow\\_duress\\_finger](#) but for threat level 2.

**See also:**

[ucc.allow\\_duress\\_finger](#)

#### [ucc.allow\\_duress\\_finger\\_TL3](#)

Same as [ucc.allow\\_duress\\_finger](#) but for threat level 3.

**See also:**

[ucc.allow\\_duress\\_finger](#)

#### [ucc.allow\\_vip\\_auth\\_bypass](#)

Parameter to enable/disable VIP bypass.

At the time of enrollment, user can be marked as VIP User.

This parameter enable access to users without identity checks (without finger bio, pin, face detection check) during user control operation.

Trusted source of VIP user trigger is the contactless card and the user finger (Keyboard and External trigger source excluded).

Face capture is still performed if configured.

Other checks such as schedule access, holiday schedule, stolen card reporting, whitelist addition, expiry date are still performed normally.

## Values

- 0 - VIP authentication bypass not allowed (**0 - Default**)
- 1 - VIP authentication bypass allowed

### [ucc.allow\\_vip\\_auth\\_bypass\\_TL1](#)

Same as [ucc.allow\\_vip\\_auth\\_bypass](#) but for threat level 1.

**See also:**

[ucc.allow\\_vip\\_auth\\_bypass](#)

### [ucc.allow\\_vip\\_auth\\_bypass\\_TL2](#)

Same as [ucc.allow\\_vip\\_auth\\_bypass](#) but for threat level 2.

**See also:**

[ucc.allow\\_vip\\_auth\\_bypass](#)

### [ucc.allow\\_vip\\_auth\\_bypass\\_TL3](#)

Same as [ucc.allow\\_vip\\_auth\\_bypass](#) but for threat level 3.

**See also:**

[ucc.allow\\_vip\\_auth\\_bypass](#)

### [ucc.finger\\_bio\\_auth\\_rule](#)

Parameter to enable/disable biometric authentication (1vs1).

## Values

### SIGMA / SIGMA Lite / SIGMA Lite+ / SIGMA Extreme

- 0 - Biometric authentication rule disabled
- 1 - Biometric authentication rule enabled (**1 - Default**)

### VisionPass / MWSP / VisionPass SP

Not applicable

### MWC

Deprecated since Version 2.4.0, Please refer alternative parameter [ucc.biometric\\_auth\\_rule](#)

#### [ucc.finger\\_bio\\_auth\\_rule\\_TL1](#)

Same as [ucc.finger\\_bio\\_auth\\_rule](#) but for threat level 1.

**See also:**

[ucc.finger\\_bio\\_auth\\_rule](#)

#### [ucc.finger\\_bio\\_auth\\_rule\\_TL2](#)

Same as [ucc.finger\\_bio\\_auth\\_rule](#) but for threat level 2.

**See also:**

[ucc.finger\\_bio\\_auth\\_rule](#)

#### [ucc.finger\\_bio\\_auth\\_rule\\_TL3](#)

Same as [ucc.finger\\_bio\\_auth\\_rule](#) but for threat level 3.

**See also:**

[ucc.finger\\_bio\\_auth\\_rule](#)

#### [ucc.biometric\\_auth\\_rule](#)

Parameter to enable/disable biometric authentication (1vs1).

## Values

### VisionPass / MWC / MWSP / VisionPass SP

- 0 - Biometric authentication rule disabled
- 1 - Biometric authentication rule enabled (**1 - Default**)

### SIGMA / SIGMA Lite / SIGMA Lite+ / SIGMA Extreme

Not applicable

#### [ucc.biometric\\_auth\\_rule\\_TL1](#)

Same as [ucc.biometric\\_auth\\_rule](#) but for threat level 1.

**See also:**

[ucc.biometric\\_auth\\_rule](#)

#### [ucc.biometric\\_auth\\_rule\\_TL2](#)

Same as [ucc.biometric\\_auth\\_rule](#) but for threat level 2.

**See also:**

[ucc.biometric\\_auth\\_rule](#)

#### [ucc.biometric\\_auth\\_rule\\_TL3](#)

Same as [ucc.biometric\\_auth\\_rule](#) but for threat level 3.

**See also:**

[ucc.biometric\\_auth\\_rule](#)

#### [ucc.mask\\_auth\\_rule](#)

Parameter to enable the mask control. When activated, a user without a mask will be rejected.

## Values

### VisionPass

- 0 - Mask is mandatory
- 1 - Mask is not requested (**1** - Default)

SIGMA / SIGMA Lite / SIGMA Lite+ / SIGMA Extreme / MWC / MWSP / VisionPass SP

Not applicable



Since:

VisionPass 2.5.0

## ucc.pin\_auth\_rule

Parameter to enable/disable user PIN code check.

## Values

**SIGMA / SIGMA Lite+ / SIGMA Extreme / MWC / VisionPass / VisionPass SP**

- 0 - PIN code check not performed (**0 - Default**)
- 1 - PIN code check performed

**SIGMA Lite / MWSP**

Not applicable

### [ucc.pin\\_auth\\_rule\\_TL1](#)

Same as [ucc.pin\\_auth\\_rule](#) but for threat level 1.

**See also:**

[ucc.pin\\_auth\\_rule](#)

### [ucc.pin\\_auth\\_rule\\_TL2](#)

Same as [ucc.pin\\_auth\\_rule](#) but for threat level 2.

**See also:**

[ucc.pin\\_auth\\_rule](#)

### [ucc.pin\\_auth\\_rule\\_TL3](#)

Same as [ucc.pin\\_auth\\_rule](#) but for threat level 3.

**See also:**

[ucc.pin\\_auth\\_rule](#)

### [ucc.face\\_auth\\_rule](#)

Parameter to configure face detection policy.

Face detection is performed in parallel to other user control operations.

## Values

### SIGMA / SIGMA Extreme

- 0 - Face detection is disabled (**0 - Default**)
- 1 - Photo Capture: One picture is captured and saved in transaction log.
- 2 - Optional face detection: Similar to photo capture functionality but multiple pictures are captured during face detection.  
If a face is detected in one or multiple photos, the pictures are saved.  
The face detection process ends when user control workflow gets completed.
- 3 - Mandatory face detection: if no face is detected, the user is rejected.  
Face detection is performed till timeout if no face is detected.

### VisionPass / VisionPass SP

- 0 - Disable : Pictures will not be stored in transaction log for the users. (**0 - Default**)
- 1 - Photo Capture: Pictures will be stored in transaction log for the users.



**Since:**

MorphoAccess® 2.5.1

#### Note:

- In case of VIP/VisionPass SP user, face detection mandatory workflow becomes face detection optional. Other face detection workflows remain same.
- Since MorphoAccess® 1.3.2, if per user rule (see [ucc.per\\_user\\_rules](#)) is enabled, face rule will be applied as following:

User Rule	Terminal configuration (ucc.face_auth_rule)	Face rule to follow (Sigma/Sigma Extreme)	Face rule to follow (VisionPass/(VisionPass SP))
X (shall not be considered)	Mandatory face detection	Mandatory face detection	NA
Disable	Optional face detection	Optional face detection	NA
Photo taking	Optional face detection	Optional face detection	NA
Optional face	Optional face detection	Optional face detection	NA



detection			
Mandatory face detection	Optional face detection	Mandatory face detection	NA
Disable	Photo taking	Photo taking	Photo taking
Photo taking	Photo taking	Photo taking	Photo taking
Optional face detection	Photo taking	Optional face detection	NA
Mandatory face detection	Photo taking	Mandatory face detection	NA
Disable	Disable	Disable	Disable
Photo taking	Disable	Photo taking	Photo taking
Optional face detection	Disable	Optional face detection	NA
Mandatory face detection	Disable	Mandatory face detection	NA

In case of a VIP/VisionPass SP user, mandatory workflow attribute of face detection is changed to an optional attribute of face detection. Other face detection workflow remain the same.

#### SIGMA Lite / SIGMA Lite+ / MWC / MWSP

Not applicable

#### **ucc.users\_photo\_policy**

Parameter to configure user photo capture policy. [photo taking / face detection is performed based on value of [ucc.face\\_auth\\_rule](#)].

Photo capture is performed in parallel to other user control operations.

## Values

### SIGMA / SIGMA Extreme / VisionPass / VisionPass SP

- 1 - Photo capture is performed for accepted users only (**1 - Default**)
- 2 - Photo capture is performed for rejected users only
- 3 - Photo capture is performed for all users whether accepted or rejected

ucc.face_auth_rule	ucc.users_photo_policy	Behavior of terminal
0	X (shall not be considered)	Disable
1 or 2 or 3	1	Photo taking / face detection will be performed on the basis of "ucc.face_auth_rule" for accepted users only
1 or 2 or 3	2	Photo taking / face detection will be performed on the basis of "ucc.face_auth_rule" for rejected users only
1 or 2 or 3	3	Photo taking / face detection will be performed on the basis of "ucc.face_auth_rule" for all users whether accepted or rejected



Since:

MorphoAccess® 1.2.4

### SIGMA Lite / SIGMA Lite+ / MWC / MWSP

Not applicable

#### ucc.face\_auth\_rule\_TL1

Same as **ucc.face\_auth\_rule** but for Threat Level 1.

## Values

- See also:  
[ucc.face\\_auth\\_rule](#)

### VisionPass / VisionPass SP

Not applicable

### [ucc.face\\_auth\\_rule\\_TL2](#)

Same as [ucc.face\\_auth\\_rule](#) but for Threat Level 2.

## Values

- See also:  
[ucc.face\\_auth\\_rule](#)

### VisionPass / VisionPass SP

Not applicable

### [ucc.face\\_auth\\_rule\\_TL3](#)

Same as [ucc.face\\_auth\\_rule](#) but for Threat Level 3.

## Values

- See also:  
[ucc.face\\_auth\\_rule](#)

### VisionPass / VisionPass SP

Not applicable

## ucc.check\_user\_id\_whitelist

Parameter to enable/disable whitelist check.

Access is denied if user is not in terminal's whitelist.

Users can be whitelisted during enrolment or user modification.

## Values

- 0 - User ID White list check not performed (**0 - Default**)
- 1 - User ID White list check performed

### [ucc.check\\_user\\_id\\_whitelist\\_TL1](#)

Same as [ucc.check\\_user\\_id\\_whitelist](#) but for threat level 1.

**See also:**

[ucc.check\\_user\\_id\\_whitelist](#)

### [ucc.check\\_user\\_id\\_whitelist\\_TL2](#)

Same as [ucc.check\\_user\\_id\\_whitelist](#) but for threat level 2.

**See also:**

[ucc.check\\_user\\_id\\_whitelist](#)

### [ucc.check\\_user\\_id\\_whitelist\\_TL3](#)

Same as [ucc.check\\_user\\_id\\_whitelist](#) but for threat level 3.

**See also:**

[ucc.check\\_user\\_id\\_whitelist](#)

### [ucc.enable\\_external\\_database](#)

Parameter to enable/disable polling mode.

In the polling mode, user authentication is initiated on the terminal, wherein the User ID is polled out to the external controller. The corresponding template (if it exists) is sent by the external controller to the terminal for authentication.

Terminal does not use its local database for template verification.

## Values

- 0 - Polling mode disabled (**0** - Default)
- 1 - Polling mode enabled

## ucc.check\_access\_schedule

Parameter to enable/disable access schedule check.

The access schedule feature allows to set the duration within which a user is allowed to be controlled. Apart from the defined schedule time, the terminal does not grant access to the users, even if authenticated successfully.

## Values

- 0 - Access schedule check disabled (**0 - Default**)
- 1 - Access schedule check enabled

### **ucc.check\_holiday\_schedule**

Parameter to enable/disable holiday schedule check.

Holiday schedule feature allows to schedule for the days on which a user is not allowed to access.

Holidays can be defined for an entire year. The terminal does not grant access to the users on an holiday, even if the users are authenticated successfully.

## Values

- 0 - Holiday schedule check disabled (**0** - Default)
- 1 - Holiday schedule check enabled

### **ucc.check\_stolen\_card\_list**

Parameter to enable/disable stolen card list check.

In order to prevent unauthorized access with stolen card enable this check.

## Values

- 0 - Stolen card list check disabled (**0** - Default)
- 1 - Stolen card list check enabled

### ucc.check\_expiry\_date

Parameter to enable/disable expiry date check.

During user enrolment, expiry date of a user can be set. After the user record is expired, the user will not be allowed to access.

## Values

- 0 - Expiry date check disabled (**0** - Default)
- 1 - Expiry date check enabled

## face\_detection.timeout

Parameter to set duration for face detection.

If terminal does not detect face during user control within this duration, then access is denied.

## Values

### SIGMA / SIGMA Extreme

- 3 - 10 (**3** - Default)

### SIGMA Lite / SIGMA Lite+ / MWC / VisionPass / MWSP / VisionPass SP

Not applicable



**Note:**

Timeout in seconds

## **success\_message.display\_information**

Parameter allows to select the content of the message displayed on a successful user authentication:  
User ID, name, or timestamp.

## Values

SIGMA / SIGMA Lite+ / SIGMA Extreme / MWC / VisionPass / VisionPass SP

Parameter Value	Success Message
0 ( <b>Default Value</b> )	User Information will not be displayed
1	Only user ID to be displayed
2	Only user name to be displayed
3	User ID and user name are displayed
4	Only timestamp is displayed
5	User ID and timestamp are displayed
6	User name and timestamp are displayed
7	User ID, user Name and timestamp are displayed

SIGMA Lite / MWSP

Not applicable

## reject\_message.display\_reason

Parameter to display the reason of failure during control.

For security purposes, the display of the reason for failure is not recommended.

## Values

### SIGMA / SIGMA Extreme / MWC / VisionPass / VisionPass SP

- 0 - Do not display reason of rejection (**0 - Default**)
- 1 - Display reason of rejection

### SIGMA Lite / SIGMA Lite+ / MWSP

Not applicable

### **ucc.enable\_timed\_anti\_passback**

Parameter to enable/disable the timed anti-passback feature When this feature is activated, after being identified, same user will be systematically rejected during time define by the key **auth\_param.timed\_anti\_passback\_same\_user\_timeout**.

## Values

- 0 - Disabled (**0 - Default**)
- 1 - Enabled

### SIGMA Lite / SIGMA Lite+



**Since:**

MorphoAccess® 2.0

### SIGMA / SIGMA Extreme



**Since:**

MorphoAccess® 3.0.0

### See also:

[auth\\_param.timed\\_anti\\_passback\\_same\\_user\\_timeout](#)

# Access and Time Biometric Terminals Parameters Guide

[Main Page](#)

[Modules](#)

[Classes](#)

Defines

**Wiegand/Clock and  
data**

## Detailed Description

Biometric terminals support interaction with remote hosts over wiegand/clock&data pins. There is specific format associated with each event, that is understood by both terminal and remote host.

For this feature, the parameters under this section control the wiegand or clock and data strings sent and received.

Input wiegand format and output wiegand format for various events can also be configured using parameters under this section.

**Note:**



GPIO and WIEGAND values are modified during boot sequence. However, they are restored to their original values upon bootup completion.

When OSDP protocol is activated, output wiegand format is also used to define content of the OSDP\_RAW answer.

## Define Documentation

### wiegand.external\_port\_output\_status

Parameter to enable/disable wiegand output functionality.

## Values

- **Wiegand\_output\_status::type**

Default value: **Wiegand\_output\_status::never\_send**

## wiegand.external\_port\_input\_format

Parameter to define external port wiegand input format.

## Values

- `Wiegand_format_type::type`

Default value:

`Wiegand_format_type::wiegand_fmt_standard_26`

### Note:



Custom format (i.e. `Wiegand_format_type::wiegand_fmt_cust` to `Wiegand_format_type::wiegand_fmt_cust` `om_slot7`) can only be set if format is defined in corresponding slot

## wiegand.prox\_port\_input\_format

Parameter to define wiegand format for Prox cards.

Useful only on Prox capable terminals.

## Values

- [\*\*Wiegand\\_format\\_type::type\*\*](#)

Default value:

[\*\*Wiegand\\_format\\_type::wiegand\\_fmt\\_standard\\_26\*\*](#)

## VisionPass SP

Not applicable

### Note:



- Custom format (i.e. [\*\*Wiegand\\_format\\_type::wiegand\\_fmt\\_custom\\_slot0\*\*](#) to [\*\*Wiegand\\_format\\_type::wiegand\\_fmt\\_custom\\_slot7\*\*](#)) can only be set if format is defined in corresponding slot
- For iClass product refer [\*\*sc.HID\\_card\\_number\\_format\*\*](#)

## wiegand.custom\_format\_slot0

Slot 0 for storing custom wiegand format.

## Values

- Refer document "MorphoAccess Sigma - Wiegand AN.docx" for binary format (**empty [no format]** - Default)

### Note:



To clear wiegand format from slot set empty data. If format is in use it can not be cleared(either in input or in output events).

## wiegand.custom\_format\_slot1

Slot 1 for storing custom wiegand format.

## Values

- Refer document "MorphoAccess Sigma - Wiegand AN.docx" for binary format (**empty [no format]** - Default)

### Note:



To clear wiegand format from slot set empty data. If format is in use it can not be cleared(either in input or in output events).

## wiegand.custom\_format\_slot2

Slot 2 for storing custom wiegand format.

## Values

- Refer document "MorphoAccess Sigma - Wiegand AN.docx" for binary format (**empty [no format]** - Default)

### Note:



To clear wiegand format from slot set empty data. If format is in use it can not be cleared(either in input or in output events).

## wiegand.custom\_format\_slot3

Slot 3 for storing custom wiegand format.

## Values

- Refer document "MorphoAccess Sigma - Wiegand AN.docx" for binary format (**empty [no format]** - Default)

### Note:



To clear wiegand format from slot set empty data. If format is in use it can not be cleared(either in input or in output events).

## wiegand.custom\_format\_slot4

Slot 4 for storing custom wiegand format.

## Values

- Refer document "MorphoAccess Sigma - Wiegand AN.docx" for binary format (**empty [no format]** - Default)

### Note:



To clear wiegand format from slot set empty data. If format is in use it can not be cleared(either in input or in output events).

## wiegand.custom\_format\_slot5

Slot 5 for storing custom wiegand format.

## Values

- Refer document "MorphoAccess Sigma - Wiegand AN.docx" for binary format (**empty [no format]** - Default)

### Note:



To clear wiegand format from slot set empty data. If format is in use it can not be cleared(either in input or in output events).

## wiegand.custom\_format\_slot6

Slot 6 for storing custom wiegand format.

## Values

- Refer document "MorphoAccess Sigma - Wiegand AN.docx" for binary format (**empty [no format]** - Default)

### Note:



To clear wiegand format from slot set empty data. If format is in use it can not be cleared(either in input or in output events).

## wiegand.custom\_format\_slot7

Slot 7 for storing custom wiegand format.

## Values

- Refer document "MorphoAccess Sigma - Wiegand AN.docx" for binary format (**empty [no format]** - Default)

### Note:



To clear wiegand format from slot set empty data. If format is in use it can not be cleared(either in input or in output events).

## wiegand.pulse\_width

Pulse width of wiegand output pulses.

## Values

- 20 - 100 (**60** - Default)



### Note:

Timeout in microseconds

## wiegand.pulse\_interval

Pulse interval of wiegand output pulses.

## Values

- 200 - 20000 (**2000** - Default)



**Note:**

Timeout in microseconds

## wiegand.event\_duress\_finger

Parameter to define wiegand format used in duress event.

## Values

**SIGMA Lite / SIGMA Lite+ / SIGMA / SIGMA Extreme**

- [Wiegand\\_duress\\_event\\_format\\_type::type](#)

Default value:

[Wiegand\\_duress\\_event\\_format\\_type::duress\\_wiegand\\_fmt\\_none](#)

**MWC / VisionPass / MWSP / VisionPass SP**

Not applicable

**Note:**



Custom format (i.e. [Wiegand\\_duress\\_event\\_format\\_type::wieg\\_and\\_fmt\\_custom\\_slot0](#) to [Wiegand\\_duress\\_event\\_format\\_type::wieg\\_and\\_fmt\\_custom\\_slot7](#)) can only be set if format is defined in corresponding slot.

### wiegand.event\_tamper

Parameter to define wiegand format used in tamper event.

## Values

- [\*\*Wiegand\\_tamper\\_event\\_format\\_type::type\*\*](#)

Default value:

[\*\*Wiegand\\_tamper\\_event\\_format\\_type::wiegand\\_fmt\\_130\\_bit\\_serial\\_number\*\*](#)

**Note:**



Custom format (i.e. [\*\*Wiegand\\_tamper\\_event\\_format\\_type::wiegand\\_fmt\\_custom\\_slot0\*\*](#) to [\*\*Wiegand\\_tamper\\_event\\_format\\_type::wiegand\\_fmt\\_custom\\_slot7\*\*](#)) can only be set if format is defined in corresponding slot.

## wiegand.event\_verify\_fail

Parameter to define wiegand format used in authentication failure event.

## Values

- `Wiegand_event_format_type::type`

Default value: `Wiegand_event_format_type::wiegand_fmt_no`  
i.e. not send any wiegand on failure

## wiegand.event\_verify\_pass

Parameter to define wiegand format used in authentication success event.

## Values

- **Wiegand\_event\_format\_type::type**

Default value: **Wiegand\_event\_format\_type::wiegand\_fmt\_no**  
i.e. use format defined by `wiegand.external_port_input_format`

### Note:



Custom format (i.e. **Wiegand\_event\_format\_type::wiegand\_fmt\_custom\_slot0** to **Wiegand\_event\_format\_type::wiegand\_fmt\_custom\_slot7**) can only be set if format is defined in corresponding slot.

## wiegand.event\_identify\_fail

Parameter to define wiegand format used in identification failure event.

## Values

- **Wiegand\_event\_format\_type::type**

Default value: **Wiegand\_event\_format\_type::wiegand\_fmt\_no**  
i.e. not send any wiegand on failure

### Note:



Custom format (i.e. **Wiegand\_event\_format\_type::wiegand\_fmt\_custom\_slot0** to **Wiegand\_event\_format\_type::wiegand\_fmt\_custom\_slot7**) can only be set if format is defined in corresponding slot.

## wiegand.event\_identify\_pass

Parameter to define wiegand format used in identification success event.

## Values

- **Wiegand\_event\_format\_type::type**

Default value: **Wiegand\_event\_format\_type::wiegand\_fmt\_no**  
i.e. use format defined by `wiegand.external_port_input_format`

### Note:



Custom format (i.e. **Wiegand\_event\_format\_type::wiegand\_fmt\_custom\_slot0** to **Wiegand\_event\_format\_type::wiegand\_fmt\_custom\_slot7**) can only be set if format is defined in corresponding slot.

## wiegand.site\_code\_checking

Parameter to enable/disable site code checking of incoming Wiegand string (from contactless card, like PACS data, or input port).

When activated, site code value is extracted from the input Wiegand frame and compared to the value defined in the Wiegand frame configuration. If values don't match, the user will be rejected.

## Values

- 0 - Disable site code check (**0** - Default)
- 1 - Enable site code check

### wiegand.external\_port\_input\_type

Parameter to set external input port type.

## Values

- 0 - External input port is wiegand (**0 - Default**)
- 1 - External input port is clock and data

### wiegand.external\_port\_output\_type

Parameter to set external output port type.

## Values

- 0 - External output port is wiegand (**0 - Default**)
- 1 - External output port is clock and data

### wiegand\_protocol.output\_byte\_order

Set parameter to send wiegand output either standard(no reverse) or reverse.

## Values

- 0 - Standard(No Reverse Wiegand Output) (**0 - Default**)
- 1 - Reverse Wiegand Output



**Since:**

MorphoAccess® 1.3.5

## `clock_and_data_protocol.input_data_line_level`

Parameter to set external port input data pin level.

When "wiegand.external\_port\_input\_type" is  
External\_port\_type::clock\_and\_data

## Values

- 0 - Non inverted (**0 - Default**)
- 1 - Level inverted

### **clock\_and\_data\_protocol.input\_clock\_line\_level**

Parameter to set external port input clock pin level.

When "wiegand.external\_port\_input\_type" is  
External\_port\_type::clock\_and\_data

## Values

- 0 - Non inverted (**0 - Default**)
- 1 - Level inverted

### **clock\_and\_data\_protocol.output\_data\_line\_level**

Parameter to set external port output data pin level.

When "wiegand.external\_port\_input\_type" is  
External\_port\_type::clock\_and\_data

## Values

- 0 - Non inverted (**0 - Default**)
- 1 - Level inverted

### **clock\_and\_data\_protocol.output\_clock\_line\_level**

Parameter to set external port output clock pin level.

When "wiegand.external\_port\_input\_type" is  
External\_port\_type::clock\_and\_data

## Values

- 0 - Non inverted (**0 - Default**)
- 1 - Level inverted

### wiegand.site\_code\_propagation

Parameter to enable/disable site code propagation.

When activated, allows to copy site code of incoming Wiegand string (from contactless card, like PACS data, or input port) to output Wiegand frame.

## Values

- 0 - disable (**0 - Default**)
- 1 - enable



**Since:**

MorphoAccess® 3.1.0

## wiegand.input\_bits\_detection\_timeout

Parameter to set bits detection timeout for wiegand input.

## Values

- 50 - 1000 (**50** - Default)

**Note:**

Timeout in milliseconds

**Since:**

MorphoAccess® 3.1.0

## wiegand.pin\_burst\_mode

Parameter to define if PIN is verified internally to the device or sent in burst mode.

## Values

### SIGMA Lite+

- 0 - PIN is verified internally to the device (*Default*)
- 1 - PIN is sent in 8 bit burst format with an additional pound (#) symbol

**MWC / VisionPass / SIGMA / SIGMA Lite / SIGMA Extreme / MWSP / VisionPass SP**

Not applicable

Copyright © 2024, IDEMIA, All rights reserved. Reproduction in whole or in part in any form or medium without the express written permission of IDEMIA is prohibited.

# Access and Time Biometric Terminals Parameters Guide

Main Page	Modules	Classes
Class List	Class Members	

# Class List

Here are the classes, structs, unions and interfaces with brief descriptions:

<a href="#"><b>Wiegand_duress_event_format_type</b></a>	Wiegand format types for duress event
<a href="#"><b>Wiegand_event_format_type</b></a>	Wiegand format types for events
<a href="#"><b>Wiegand_format_type</b></a>	Wiegand format types
<a href="#"><b>Wiegand_output_status</b></a>	Enable/Disable wiegand event sending
<a href="#"><b>Wiegand_tamper_event_format_type</b></a>	Wiegand format types for tamper event

Copyright © 2024, IDEMIA, All rights reserved. Reproduction in whole or in part in any form or medium without the express written permission of IDEMIA is prohibited.

# Access and Time Biometric Terminals Parameters Guide

Main Page

Modules

Classes

Class List

Class Members

Public Types

## **Wiegand\_duress\_event\_format\_type Struct Reference**

Wiegand format types for duress event. [More...](#)

[List of all members.](#)

### Public Types

```
enum type {
    duress_wiegand_fmt_none = 0,
    duress_reverse_wiegand_fmt = 1,
    wiegand_fmt_custom_slot0 = 10,
    wiegand_fmt_custom_slot1 = 11,
    wiegand_fmt_custom_slot2 = 12,
    wiegand_fmt_custom_slot3 = 13,
    wiegand_fmt_custom_slot4 = 14,
    wiegand_fmt_custom_slot5 = 15,
    wiegand_fmt_custom_slot6 = 16,
    wiegand_fmt_custom_slot7 = 17
}
```

Enumeration for different wiegand format. [More...](#)

## **Detailed Description**

Wiegand format types for duress event.

---

## Member Enumeration Documentation

### enum type

Enumeration for different wiegand format.

#### Enumerator:

*duress\_wiegand\_fmt\_none*

None format.

*duress\_reverse\_wiegand\_fmt*

Generate reverse wiegand string for duress  
(verify/identify pass event  
wiegand string is reversed)

*wiegand\_fmt\_custom\_slot0*

Custom wiegand format slot 0, this value can only be set if format exists in custom wiegand slot.

*wiegand\_fmt\_custom\_slot1*

Custom wiegand format slot 1, this value can only be set if format exists in custom wiegand slot.

*wiegand\_fmt\_custom\_slot2*

Custom wiegand format slot 2, this value can only be set if format exists in custom wiegand slot.

*wiegand\_fmt\_custom\_slot3*

Custom wiegand format slot

3, this value can only be set if format exists in custom wiegand slot.

*wiegand\_fmt\_custom\_slot4*

Custom wiegand format slot 4, this value can only be set if format exists in custom wiegand slot.

*wiegand\_fmt\_custom\_slot5*

Custom wiegand format slot 5, this value can only be set if format exists in custom wiegand slot.

*wiegand\_fmt\_custom\_slot6*

Custom wiegand format slot 6, this value can only be set if format exists in custom wiegand slot.

*wiegand\_fmt\_custom\_slot7*

Custom wiegand format slot 7, this value can only be set if format exists in custom wiegand slot.

# Access and Time Biometric Terminals Parameters Guide

[Main Page](#)

[Modules](#)

[Classes](#)

[Class List](#)

[Class Members](#)

[Public Types](#)

## **Wiegand\_event\_form at\_type Struct Reference**

Wiegand format types for events. [More...](#)

[List of all members.](#)

### Public Types

```
enum type {
    wiegand_fmt_no = -1,
    wiegand_fmt_standard_26 = 0,
    wiegand_fmt_apollo_44 = 1,
    wiegand_fmt_northern_34 = 2,
    wiegand_fmt_northern_34_np = 3,
    wiegand_fmt_ademco_34 = 4,
    wiegand_fmt_hid_corporate_1000 = 5,
    wiegand_fmt_hid_37 = 6,
    wiegand_fmt_TWIC_75 = 7,
    wiegand_fmt_TWIC_200 = 8,
    wiegand_fmt_custom_slot0 = 10,
    wiegand_fmt_custom_slot1 = 11,
    wiegand_fmt_custom_slot2 = 12,
    wiegand_fmt_custom_slot3 = 13,
    wiegand_fmt_custom_slot4 = 14,
    wiegand_fmt_custom_slot5 = 15,
    wiegand_fmt_custom_slot6 = 16,
```

```
wiegand_fmt_custom_slot7 = 17,  
wiegand_fmt_last_fmt_input = 18  
}
```

Enumeration for different wiegand format. [More...](#)

---

## **Detailed Description**

Wiegand format types for events.

---

## Member Enumeration Documentation

### enum type

Enumeration for different wiegand format.

#### Enumerator:

*wiegand\_fmt\_no*

None format.

*wiegand\_fmt\_standard\_26*

standard 26 bit format

*wiegand\_fmt\_apollo\_44*

Apollo 44 bit format.

*wiegand\_fmt\_northern\_34*

Northen 34 bit format.

*wiegand\_fmt\_northern\_34\_np*

Northen 34 bit format (no parity)

*wiegand\_fmt\_ademco\_34*

Ademco 34 bit format.

*wiegand\_fmt\_hid\_corporate\_1000*

HID corporate 1000 format.

*wiegand\_fmt\_hid\_37*

HID 37 bit format.

*wiegand\_fmt\_TWIC\_75*

PIV/TWIC format 75 bits.

<i>wiegand_fmt_TWIC_200</i>	PIV/TWIC format FASC-N 200 bits.
<i>wiegand_fmt_custom_slot0</i>	Custom wiegand format slot 0, this value can only be set if format exists in custom wiegand slot.
<i>wiegand_fmt_custom_slot1</i>	Custom wiegand format slot 1, this value can only be set if format exists in custom wiegand slot.
<i>wiegand_fmt_custom_slot2</i>	Custom wiegand format slot 2, this value can only be set if format exists in custom wiegand slot.
<i>wiegand_fmt_custom_slot3</i>	Custom wiegand format slot 3, this value can only be set if format exists in custom wiegand slot.
<i>wiegand_fmt_custom_slot4</i>	Custom wiegand format slot 4, this value can only be set if format exists in custom wiegand slot.
<i>wiegand_fmt_custom_slot5</i>	Custom wiegand format slot 5, this value can only be set if format exists in custom wiegand slot.

*wiegand\_fmt\_custom\_slot6*

Custom wiegand format slot 6, this value can only be set if format exists in custom wiegand slot.

*wiegand\_fmt\_custom\_slot7*

Custom wiegand format slot 7, this value can only be set if format exists in custom wiegand slot.

*wiegand\_fmt\_last\_fmt\_input*

apply last input wiegand frame format to output. If no wiegand input has been processed, apply custom slot0

Copyright © 2024, IDEMIA, All rights reserved. Reproduction in whole or in part in any form or medium without the express written permission of IDEMIA is prohibited.

# Access and Time Biometric Terminals Parameters Guide

Main Page	Modules	Classes
Class List	Class Members	Public Types
		<b>Wiegand_format_type Struct Reference</b>

Wiegand format types. [More...](#)

[List of all members.](#)

## Public Types

```
enum type {
    wiegand_fmt_standard_26 = 0,
    wiegand_fmt_apollo_44 = 1,
    wiegand_fmt_northern_34 = 2,
    wiegand_fmt_northern_34_np = 3,
    wiegand_fmt_ademco_34 = 4,
    wiegand_fmt_hid_corporate_1000 = 5,
    wiegand_fmt_hid_37 = 6,
    wiegand_fmt_TWIC_75 = 7,
    wiegand_fmt_TWIC_200 = 8,
    wiegand_fmt_custom_slot0 = 10,
    wiegand_fmt_custom_slot1 = 11,
    wiegand_fmt_custom_slot2 = 12,
    wiegand_fmt_custom_slot3 = 13,
    wiegand_fmt_custom_slot4 = 14,
    wiegand_fmt_custom_slot5 = 15,
    wiegand_fmt_custom_slot6 = 16,
    wiegand_fmt_custom_slot7 = 17,
```

```
wiegand_fmt_autodetect = 18
```

```
}
```

Enumeration for different wiegand formats. More...

---

## **Detailed Description**

Wiegand format types.

---

## Member Enumeration Documentation

### enum type

Enumeration for different wiegand formats.

#### Enumerator:

<i>wiegand_fmt_standard_26</i>	standard 26 bit format
<i>wiegand_fmt_apollo_44</i>	Apollo 44 bit format.
<i>wiegand_fmt_northern_34</i>	Northen 34 bit format.
<i>wiegand_fmt_northern_34_np</i>	Northen 34 bit format (no parity)
<i>wiegand_fmt_ademco_34</i>	Ademco 34 bit format.
<i>wiegand_fmt_hid_corporate_1000</i>	HID corporate 1000 format.
<i>wiegand_fmt_hid_37</i>	HID 37 bit format.
<i>wiegand_fmt_TWIC_75</i>	PIV/TWIC format 75 bits.
<i>wiegand_fmt_TWIC_200</i>	PIV/TWIC format FASC-N 200 bits.

*wiegand\_fmt\_custom\_slot0*

Custom wiegand format slot 0, this value can only be set if format exists in custom wiegand slot.

*wiegand\_fmt\_custom\_slot1*

Custom wiegand format slot 1, this value can only be set if format exists in custom wiegand slot.

*wiegand\_fmt\_custom\_slot2*

Custom wiegand format slot 2, this value can only be set if format exists in custom wiegand slot.

*wiegand\_fmt\_custom\_slot3*

Custom wiegand format slot 3, this value can only be set if format exists in custom wiegand slot.

*wiegand\_fmt\_custom\_slot4*

Custom wiegand format slot 4, this value can only be set if format exists in custom wiegand slot.

*wiegand\_fmt\_custom\_slot5*

Custom wiegand format slot 5, this value can only be set if format exists in custom wiegand slot.

*wiegand\_fmt\_custom\_slot6*

Custom wiegand format slot 6, this value can only be set if format exists in custom wiegand slot.

*wiegand\_fmt\_custom\_slot7*

Custom wiegand format slot 7, this value can only be set if format exists in custom wiegand slot.

*wiegand\_fmt\_autodetect*

Auto detect input format, this value tries to detect input wiegand frame format among format defined in custom slot 0 to 7 and applies it.

Copyright © 2024, IDEMIA, All rights reserved. Reproduction in whole or in part in any form or medium without the express written permission of IDEMIA is prohibited.

# Access and Time Biometric Terminals Parameters Guide

Main Page	Modules	Classes
Class List	Class Members	Public Types
<b>Wiegand_output_status Struct Reference</b>		

Enable/Disable wiegand event sending. [More...](#)

[List of all members.](#)

## Public Types

```
enum type {  
    never_send = 0,  
    always_send = 1,  
    selective_send = -1  
}
```

Wiegand output port status. [More...](#)

## **Detailed Description**

Enable/Disable wiegand event sending.

---

# Member Enumeration Documentation

## enum type

Wiegand output port status.

### Enumerator:

*never\_send*

External port sending is disabled.

*always\_send*

Terminal sends events on external port  
whatever the user control trigger source is.

*selective\_send*

Terminal sends events on external port only  
when verification initiated from wiegand  
source.

Copyright © 2024, IDEMIA, All rights reserved. Reproduction in whole or in part in  
any form or medium without the express written permission of IDEMIA is prohibited.

# Access and Time Biometric Terminals Parameters Guide

[Main Page](#)

[Modules](#)

[Classes](#)

[Class List](#)

[Class Members](#)

[Public Types](#)

## **Wiegand\_tamper\_ev ent\_format\_type Struct Reference**

Wiegand format types for tamper event. [More...](#)

[List of all members.](#)

### Public Types

```
enum type {
    tamper_wiegand_fmt_none = 0,
    wiegand_fmt_130_bit_serial_number = 1,
    wiegand_fmt_custom_slot0 = 10,
    wiegand_fmt_custom_slot1 = 11,
    wiegand_fmt_custom_slot2 = 12,
    wiegand_fmt_custom_slot3 = 13,
    wiegand_fmt_custom_slot4 = 14,
    wiegand_fmt_custom_slot5 = 15,
    wiegand_fmt_custom_slot6 = 16,
    wiegand_fmt_custom_slot7 = 17
}
```

Enumeration for different wiegand format. [More...](#)

## **Detailed Description**

Wiegand format types for tamper event.

---

## Member Enumeration Documentation

### enum type

Enumeration for different wiegand format.

#### Enumerator:

*tamper\_wiegand\_fmt\_none*

None format.

*wiegand\_fmt\_130\_bit\_serial\_number*

Generate 130 bit  
wiegand string  
containing 128 bit  
device serial number.

*wiegand\_fmt\_custom\_slot0*

Custom wiegand  
format slot 0, this  
value can only be set if  
format exists in custom  
wiegand slot.

*wiegand\_fmt\_custom\_slot1*

Custom wiegand  
format slot 1, this  
value can only be set if  
format exists in custom  
wiegand slot.

*wiegand\_fmt\_custom\_slot2*

Custom wiegand  
format slot 2, this  
value can only be set if  
format exists in custom  
wiegand slot.

*wiegand\_fmt\_custom\_slot3*

Custom wiegand format slot 3, this value can only be set if format exists in custom wiegand slot.

*wiegand\_fmt\_custom\_slot4*

Custom wiegand format slot 4, this value can only be set if format exists in custom wiegand slot.

*wiegand\_fmt\_custom\_slot5*

Custom wiegand format slot 5, this value can only be set if format exists in custom wiegand slot.

*wiegand\_fmt\_custom\_slot6*

Custom wiegand format slot 6, this value can only be set if format exists in custom wiegand slot.

*wiegand\_fmt\_custom\_slot7*

Custom wiegand format slot 7, this value can only be set if format exists in custom wiegand slot.

**Copyright © 2024, IDEMIA, All rights reserved. Reproduction in whole or in part in any form or medium without the express written permission of IDEMIA is prohibited.**

---

Generated by doxygen 1.7.6.1.

# Access and Time Biometric Terminals Parameters Guide

[Main Page](#)

[Modules](#)

[Classes](#)

[Class List](#)

[Class Members](#)

## Class Index

**W**

[Wiegand\\_event\\_format\\_type](#)

[Wiegand\\_output\\_status](#)

**W**

[Wiegand\\_format\\_type](#)

[Wiegand\\_tamper\\_event\\_form](#)

[Wiegand\\_duress\\_event\\_format\\_type](#)

**W**

Copyright © 2024, IDEMIA, All rights reserved. Reproduction in whole or in part in any form or medium without the express written permission of IDEMIA is prohibited.

Generated by doxygen 1.7.6.1.

# Access and Time Biometric Terminals Parameters Guide

---

Main Page	Modules	Classes			
Class List	Class Members				
All	Enumerations	Enumerator			
a	d	n	s	t	w

Here is a list of all documented class members with links to the class documentation for each member:

- a -

- always\_send  
: [Wiegand\\_output\\_status](#)

- d -

- duress\_reverse\_wiegand\_fmt
  - : **Wiegand\_duress\_event\_format\_type**
- duress\_wiegand\_fmt\_none
  - : **Wiegand\_duress\_event\_format\_type**

- n -

- never\_send
  - : **Wiegand\_output\_status**

- s -

- selective\_send
  - : **Wiegand\_output\_status**

- t -

- tamper\_wiegand\_fmt\_none
  - : **Wiegand\_tamper\_event\_format\_type**
- type
  - : **Wiegand\_output\_status** ,  
**Wiegand\_tamper\_event\_format\_type** ,  
**Wiegand\_duress\_event\_format\_type** ,  
**Wiegand\_event\_format\_type** , **Wiegand\_format\_type**

- w -

- wiegand\_fmt\_130\_bit\_serial\_number
  - : **Wiegand\_tamper\_event\_format\_type**
- wiegand\_fmt\_ademco\_34
  - : **Wiegand\_format\_type** , **Wiegand\_event\_format\_type**
- wiegand\_fmt\_apollo\_44
  - : **Wiegand\_format\_type** , **Wiegand\_event\_format\_type**
- wiegand\_fmt\_autodetect
  - : **Wiegand\_format\_type**
- wiegand\_fmt\_custom\_slot0
  - : **Wiegand\_event\_format\_type** ,  
**Wiegand\_duress\_event\_format\_type** ,  
**Wiegand\_tamper\_event\_format\_type** ,  
**Wiegand\_format\_type**
- wiegand\_fmt\_custom\_slot1
  - : **Wiegand\_format\_type** , **Wiegand\_event\_format\_type** ,  
**Wiegand\_duress\_event\_format\_type** ,  
**Wiegand\_tamper\_event\_format\_type**
- wiegand\_fmt\_custom\_slot2
  - : **Wiegand\_event\_format\_type** ,  
**Wiegand\_duress\_event\_format\_type** ,  
**Wiegand\_tamper\_event\_format\_type** ,  
**Wiegand\_format\_type**

- `wiegand_fmt_custom_slot3`  
: `Wiegand_format_type` , `Wiegand_event_format_type` ,  
`Wiegand_duress_event_format_type` ,  
`Wiegand_tamper_event_format_type`
- `wiegand_fmt_custom_slot4`  
: `Wiegand_format_type` , `Wiegand_event_format_type` ,  
`Wiegand_duress_event_format_type` ,  
`Wiegand_tamper_event_format_type`
- `wiegand_fmt_custom_slot5`  
: `Wiegand_format_type` , `Wiegand_event_format_type` ,  
`Wiegand_duress_event_format_type` ,  
`Wiegand_tamper_event_format_type`
- `wiegand_fmt_custom_slot6`  
: `Wiegand_event_format_type` ,  
`Wiegand_duress_event_format_type` ,  
`Wiegand_tamper_event_format_type` ,  
`Wiegand_format_type`
- `wiegand_fmt_custom_slot7`  
: `Wiegand_event_format_type` ,  
`Wiegand_duress_event_format_type` ,  
`Wiegand_tamper_event_format_type` ,  
`Wiegand_format_type`
- `wiegand_fmt_hid_37`  
: `Wiegand_format_type` , `Wiegand_event_format_type`
- `wiegand_fmt_hid_corporate_1000`  
: `Wiegand_event_format_type` , `Wiegand_format_type`

- wiegand\_fmt\_last\_fmt\_input
  - : **Wiegand\_event\_format\_type**
- wiegand\_fmt\_no
  - : **Wiegand\_event\_format\_type**
- wiegand\_fmt\_northern\_34
  - : **Wiegand\_format\_type** , **Wiegand\_event\_format\_type**
- wiegand\_fmt\_northern\_34\_np
  - : **Wiegand\_event\_format\_type** , **Wiegand\_format\_type**
- wiegand\_fmt\_standard\_26
  - : **Wiegand\_event\_format\_type** , **Wiegand\_format\_type**
- wiegand\_fmt\_TWIC\_200
  - : **Wiegand\_format\_type** , **Wiegand\_event\_format\_type**
- wiegand\_fmt\_TWIC\_75
  - : **Wiegand\_format\_type** , **Wiegand\_event\_format\_type**

Copyright © 2024, IDEMIA, All rights reserved. Reproduction in whole or in part in any form or medium without the express written permission of IDEMIA is prohibited.

# Access and Time Biometric Terminals Parameters Guide

Main Page	Modules	Classes
Class List	Class Members	
All	Enumerations	Enumerator

- type : [Wiegand\\_format\\_type](#) , [Wiegand\\_output\\_status](#) , [Wiegand\\_tamper\\_event\\_format\\_type](#) , [Wiegand\\_duress\\_event\\_format\\_type](#) , [Wiegand\\_event\\_format\\_type](#)

Copyright © 2024, IDEMIA, All rights reserved. Reproduction in whole or in part in any form or medium without the express written permission of IDEMIA is prohibited.

# Access and Time Biometric Terminals Parameters Guide

---

Main Page	Modules	Classes			
Class List	Class Members				
All	Enumerations	Enumerator			
a	d	n	s	t	w

- a -

- always\_send  
[: Wiegand\\_output\\_status](#)

- d -

- duress\_reverse\_wiegand\_fmt  
[: Wiegand\\_duress\\_event\\_format\\_type](#)
- duress\_wiegand\_fmt\_none

: **Wiegand\_duress\_event\_format\_type**

- n -

- never\_send

: **Wiegand\_output\_status**

- s -

- selective\_send

: **Wiegand\_output\_status**

- t -

- tamper\_wiegand\_fmt\_none

: **Wiegand\_tamper\_event\_format\_type**

- w -

- wiegand\_fmt\_130\_bit\_serial\_number

: **Wiegand\_tamper\_event\_format\_type**

- wiegand\_fmt\_ademco\_34

: **Wiegand\_format\_type , Wiegand\_event\_format\_type**

- wiegand\_fmt\_apollo\_44

**: Wiegand\_format\_type , Wiegand\_event\_format\_type**

- **wiegand\_fmt\_autodetect**

**: Wiegand\_format\_type**

- **wiegand\_fmt\_custom\_slot0**

**: Wiegand\_event\_format\_type ,  
Wiegand\_duress\_event\_format\_type ,  
Wiegand\_tamper\_event\_format\_type ,  
Wiegand\_format\_type**

- **wiegand\_fmt\_custom\_slot1**

**: Wiegand\_format\_type , Wiegand\_event\_format\_type ,  
Wiegand\_duress\_event\_format\_type ,  
Wiegand\_tamper\_event\_format\_type**

- **wiegand\_fmt\_custom\_slot2**

**: Wiegand\_event\_format\_type ,  
Wiegand\_duress\_event\_format\_type ,  
Wiegand\_tamper\_event\_format\_type ,  
Wiegand\_format\_type**

- **wiegand\_fmt\_custom\_slot3**

**: Wiegand\_format\_type , Wiegand\_event\_format\_type ,  
Wiegand\_duress\_event\_format\_type ,  
Wiegand\_tamper\_event\_format\_type**

- **wiegand\_fmt\_custom\_slot4**

**: Wiegand\_format\_type , Wiegand\_event\_format\_type ,  
Wiegand\_duress\_event\_format\_type ,  
Wiegand\_tamper\_event\_format\_type**

- **wiegand\_fmt\_custom\_slot5**

- wiegand\_fmt\_custom\_slot6
  - : Wiegand\_format\_type , Wiegand\_event\_format\_type ,  
Wiegand\_duress\_event\_format\_type ,  
Wiegand\_tamper\_event\_format\_type
- wiegand\_fmt\_custom\_slot7
  - : Wiegand\_event\_format\_type ,  
Wiegand\_duress\_event\_format\_type ,  
Wiegand\_tamper\_event\_format\_type ,  
Wiegand\_format\_type
- wiegand\_fmt\_hid\_37
  - : Wiegand\_format\_type , Wiegand\_event\_format\_type
- wiegand\_fmt\_hid\_corporate\_1000
  - : Wiegand\_event\_format\_type , Wiegand\_format\_type
- wiegand\_fmt\_last\_fmt\_input
  - : Wiegand\_event\_format\_type
- wiegand\_fmt\_no
  - : Wiegand\_event\_format\_type
- wiegand\_fmt\_northern\_34
  - : Wiegand\_format\_type , Wiegand\_event\_format\_type
- wiegand\_fmt\_northern\_34\_np

**: Wiegand\_event\_format\_type , Wiegand\_format\_type**

- **wiegand\_fmt\_standard\_26**

**: Wiegand\_event\_format\_type , Wiegand\_format\_type**

- **wiegand\_fmt\_TWIC\_200**

**: Wiegand\_format\_type , Wiegand\_event\_format\_type**

- **wiegand\_fmt\_TWIC\_75**

**: Wiegand\_format\_type , Wiegand\_event\_format\_type**

Copyright © 2024, IDEMIA, All rights reserved. Reproduction in whole or in part in any form or medium without the express written permission of IDEMIA is prohibited.

# Access and Time Biometric Terminals Parameters Guide

Main Page	Modules	Classes
Class List	Class Members	

## Wiegand\_duress\_event\_format\_type Member List

This is the complete list of members for [Wiegand\\_duress\\_event\\_format\\_type](#), including all inherited members.

<a href="#">duress_reverse_wiegand_fmt</a> enum value	<a href="#">Wiegand_duress_event_format_type</a>
<a href="#">duress_wiegand_fmt_none</a> enum value	<a href="#">Wiegand_duress_event_format_type</a>
<a href="#">type</a> enum name	<a href="#">Wiegand_duress_event_format_type</a>
<a href="#">wiegand_fmt_custom_slot0</a> enum value	<a href="#">Wiegand_duress_event_format_type</a>
<a href="#">wiegand_fmt_custom_slot1</a> enum value	<a href="#">Wiegand_duress_event_format_type</a>
<a href="#">wiegand_fmt_custom_slot2</a> enum value	<a href="#">Wiegand_duress_event_format_type</a>
<a href="#">wiegand_fmt_custom_slot3</a> enum value	<a href="#">Wiegand_duress_event_format_type</a>
<a href="#">wiegand_fmt_custom_slot4</a> enum value	<a href="#">Wiegand_duress_event_format_type</a>
<a href="#">wiegand_fmt_custom_slot5</a> enum value	<a href="#">Wiegand_duress_event_format_type</a>
<a href="#">wiegand_fmt_custom_slot6</a> enum value	<a href="#">Wiegand_duress_event_format_type</a>
<a href="#">wiegand_fmt_custom_slot7</a> enum value	<a href="#">Wiegand_duress_event_format_type</a>

**Copyright © 2024, IDEMIA, All rights reserved. Reproduction in whole or in part in any form or medium without the express written permission of IDEMIA is prohibited.**

---

Generated by doxygen 1.7.6.1.

# Access and Time Biometric Terminals Parameters Guide

Main Page	Modules	Classes
Class List	Class Members	

## Wiegand\_event\_format\_type Member List

This is the complete list of members for [Wiegand\\_event\\_format\\_type](#), including all inherited members.

<code>type</code> enum name	<a href="#">Wiegand_event_format_type</a>
<code>wiegand_fmt_ademco_34</code> enum value	<a href="#">Wiegand_event_format_type</a>
<code>wiegand_fmt_apollo_44</code> enum value	<a href="#">Wiegand_event_format_type</a>
<code>wiegand_fmt_custom_slot0</code> enum value	<a href="#">Wiegand_event_format_type</a>
<code>wiegand_fmt_custom_slot1</code> enum value	<a href="#">Wiegand_event_format_type</a>
<code>wiegand_fmt_custom_slot2</code> enum value	<a href="#">Wiegand_event_format_type</a>
<code>wiegand_fmt_custom_slot3</code> enum value	<a href="#">Wiegand_event_format_type</a>
<code>wiegand_fmt_custom_slot4</code> enum value	<a href="#">Wiegand_event_format_type</a>
<code>wiegand_fmt_custom_slot5</code> enum value	<a href="#">Wiegand_event_format_type</a>
<code>wiegand_fmt_custom_slot6</code> enum value	<a href="#">Wiegand_event_format_type</a>
<code>wiegand_fmt_custom_slot7</code> enum value	<a href="#">Wiegand_event_format_type</a>
<code>wiegand_fmt_hid_37</code> enum value	<a href="#">Wiegand_event_format_type</a>

<code>wiegand_fmt_hid_corporate_1000</code> enum value	<code>Wiegand_event_format_type</code>
<code>wiegand_fmt_last_fmt_input</code> enum value	<code>Wiegand_event_format_type</code>
<code>wiegand_fmt_no</code> enum value	<code>Wiegand_event_format_type</code>
<code>wiegand_fmt_northern_34</code> enum value	<code>Wiegand_event_format_type</code>
<code>wiegand_fmt_northern_34_np</code> enum value	<code>Wiegand_event_format_type</code>
<code>wiegand_fmt_standard_26</code> enum value	<code>Wiegand_event_format_type</code>
<code>wiegand_fmt_TWIC_200</code> enum value	<code>Wiegand_event_format_type</code>
<code>wiegand_fmt_TWIC_75</code> enum value	<code>Wiegand_event_format_type</code>

Copyright © 2024, IDEMIA, All rights reserved. Reproduction in whole or in part in any form or medium without the express written permission of IDEMIA is prohibited.

# Access and Time Biometric Terminals Parameters Guide

Main Page	Modules	Classes
Class List	Class Members	

## Wiegand\_format\_type Member List

This is the complete list of members for [Wiegand\\_format\\_type](#), including all inherited members.

<a href="#">type enum name</a>	<a href="#">Wiegand_format_type</a>
<a href="#">wiegand_fmt_ademco_34 enum value</a>	<a href="#">Wiegand_format_type</a>
<a href="#">wiegand_fmt_apollo_44 enum value</a>	<a href="#">Wiegand_format_type</a>
<a href="#">wiegand_fmt_autodetect enum value</a>	<a href="#">Wiegand_format_type</a>
<a href="#">wiegand_fmt_custom_slot0 enum value</a>	<a href="#">Wiegand_format_type</a>
<a href="#">wiegand_fmt_custom_slot1 enum value</a>	<a href="#">Wiegand_format_type</a>
<a href="#">wiegand_fmt_custom_slot2 enum value</a>	<a href="#">Wiegand_format_type</a>
<a href="#">wiegand_fmt_custom_slot3 enum value</a>	<a href="#">Wiegand_format_type</a>
<a href="#">wiegand_fmt_custom_slot4 enum value</a>	<a href="#">Wiegand_format_type</a>
<a href="#">wiegand_fmt_custom_slot5 enum value</a>	<a href="#">Wiegand_format_type</a>
<a href="#">wiegand_fmt_custom_slot6 enum value</a>	<a href="#">Wiegand_format_type</a>
<a href="#">wiegand_fmt_custom_slot7 enum value</a>	<a href="#">Wiegand_format_type</a>
<a href="#">wiegand_fmt_hid_37 enum value</a>	<a href="#">Wiegand_format_type</a>
<a href="#">wiegand_fmt_hid_corporate_1000 enum value</a>	<a href="#">Wiegand_format_type</a>
<a href="#">wiegand_fmt_northern_34 enum value</a>	<a href="#">Wiegand_format_type</a>
<a href="#">wiegand_fmt_northern_34_np enum value</a>	<a href="#">Wiegand_format_type</a>
<a href="#">wiegand_fmt_standard_26 enum value</a>	<a href="#">Wiegand_format_type</a>
<a href="#">wiegand_fmt_TWIC_200 enum value</a>	<a href="#">Wiegand_format_type</a>
<a href="#">wiegand_fmt_TWIC_75 enum value</a>	<a href="#">Wiegand_format_type</a>

**Copyright © 2024, IDEMIA, All rights reserved. Reproduction in whole or in part in any form or medium without the express written permission of IDEMIA is prohibited.**

---

Generated by doxygen 1.7.6.1.

# Access and Time Biometric Terminals Parameters Guide

Main Page	Modules	Classes
Class List	Class Members	

## Wiegand\_output\_status Member List

This is the complete list of members for [Wiegand\\_output\\_status](#), including all inherited members.

<a href="#">always_send</a>	enum value	<a href="#">Wiegand_output_status</a>
<a href="#">never_send</a>	enum value	<a href="#">Wiegand_output_status</a>
<a href="#">selective_send</a>	enum value	<a href="#">Wiegand_output_status</a>
<a href="#">type</a>	enum name	<a href="#">Wiegand_output_status</a>

Copyright © 2024, IDEMIA, All rights reserved. Reproduction in whole or in part in any form or medium without the express written permission of IDEMIA is prohibited.

# Access and Time Biometric Terminals Parameters Guide

Main Page	Modules	Classes
Class List	Class Members	

## Wiegand\_tamper\_event\_format\_type Member List

This is the complete list of members for [Wiegand\\_tamper\\_event\\_format\\_type](#), including all inherited members.

tamper_wiegand_fmt_none enum value	<a href="#">Wiegand_tamper_event_format_type</a>
type enum name	<a href="#">Wiegand_tamper_event_format_type</a>
wiegand_fmt_130_bit_serial_number enum value	<a href="#">Wiegand_tamper_event_format_type</a>
wiegand_fmt_custom_slot0 enum value	<a href="#">Wiegand_tamper_event_format_type</a>
wiegand_fmt_custom_slot1 enum value	<a href="#">Wiegand_tamper_event_format_type</a>
wiegand_fmt_custom_slot2 enum value	<a href="#">Wiegand_tamper_event_format_type</a>
wiegand_fmt_custom_slot3 enum value	<a href="#">Wiegand_tamper_event_format_type</a>
wiegand_fmt_custom_slot4 enum value	<a href="#">Wiegand_tamper_event_format_type</a>
wiegand_fmt_custom_slot5 enum value	<a href="#">Wiegand_tamper_event_format_type</a>
wiegand_fmt_custom_slot6 enum value	<a href="#">Wiegand_tamper_event_format_type</a>
wiegand_fmt_custom_slot7 enum value	<a href="#">Wiegand_tamper_event_format_type</a>