



Community™ Release Notes

Community 2.0

Welcome

Community is a web-based access management software for our multihousing property employees to easily configure resident, vendor and staff access. Community empowers property managers to intuitively authenticate and manage authorization throughout the entire property providing security, convenience and operational efficiency.

Community offers web-based access from a desktop computer, laptop or mobile device while on the property's network. Property configuration and access management of residents, staff and vendors can be programmed remotely at any time 24/7.

What's New

Community 2.0 includes the following new features:

Community API

For complete information about the Community API, refer to *Community Client API Documentation* version 1.15.

- Up to 542 variable access points can now be encoded on Staff (variable access) and Vendor 4K keys. This functionality is also supported in the [Staff/Vendor Keys](#) module.



Locks may take up to six seconds to unlock depending on the number of access points the key gives access to and to which lock the key is presented.

- New/modified Community API support for:

- Returning list of configured encoders
- Returning the latest access point audit information for the specified access point
- Erasing a key
- Encoding Cancel keys for Resident, Staff (variable access) and Vendor key instances
- Reading and returning the Mifare key UID for Resident, Staff (variable access) and Vendor keys
- Returning the Mifare key UID for existing Resident, Staff (variable access) and Vendor keys

Online Communication

- The Gateway II API online integration interface is now fully supported for Community to perform all remote operations, monitor online events and status, and send related notifications.

RAC5 Elevator Profile

Community extends support for the RAC5 (Remote Access Controller) elevator profile. The RAC5 profile can be configured to control up to 64 distinct floors and supports the same online operations and events as the MFC elevator controller.

For online environments, go to [Device Management > Gateway Configuration](#) to configure the RAC5 elevator controller over USB.

The following RAC5-specific events are now included in the Access Point Audit Report and Monitoring (Online/Events) details:

- "Request To Exit Open"
- "Request To Exit Close" (Monitoring only)
- "Remote Unlock Open"
- "Remote Unlock Close"
- "Fire Alarm Activated"
- "Fire Alarm Deactivated"

Reports

The Access Point Audit Report now includes the following events:

- "Escape Return Start"
- "Escape Return End"
- "Deadbolt Deactivation"
- "Auto Unlatch Schedule Started" (previously "Auto Unlatch")
- "Auto Unlatch Schedule Ended" (previously "Auto Latch")



Supported lock types: MT4, Pixel, RCU4, RT+, Saffire LX, RAC5. Latest lock firmware required.

Corrected Issues

This section lists corrected issues. An internal reference number may follow the fix description.

System Settings

- Key Expiration. The default expiration for Block/Unblock/Resequence/Cancel keys no longer affects the expiration selected at key-making time. (29012)

Mobile Keys

- Upon modifying mobile key settings in *System Settings > Advanced*, staff/vendor-level access points are now flagged for reprogramming as expected. (27919)

Community API

- An intermittent API issue that prevented key encoding is resolved. (32476/SD-1065)
- An intermittent API issue that prevented staff/vendor mobile keys from being deleted is resolved. (33049/SD-1143)
- An intermittent API issue that prevented some resident keys with certain lease IDs to fail encoding is resolved. (33052/SD-1117)
- An intermittent API issue that prevented some resident mobile keys with multiple units to be issued is resolved. (33149/SD-1160)

Aurora

- Upon resynchronizing data between Aurora and Community, only Community credentials are deleted. All credentials added directly in Aurora persist. (33060)

Known Issues

This section lists known issues and provides detailed work-around instructions. An internal reference number may follow the issue description.

Community API

- To ensure proper behavior, upon requesting a resident key for an existing lease, all units already assigned to the lease must be passed in the request in addition to the new units. (33292)

System Settings

- Database Backup & Archiving. For online installs only. The MongoDB database is not part of the manual backup as done by clicking the [Back Up Database](#) button. (only backing up SQL DB). (32954)
 - 🔗 Make sure MongoDB backup is scheduled or is backed up manually outside of Community to an external location.

Device Management

- Upon deactivating the ZigBee antenna for a gateway, the antenna status is "pair off" when it should be "deactivated". (32624)

Role Management

- A custom role created with the [Staff/Vendor Keys](#) system right enabled and related key rights ONLY does not allow the operator assigned to this role to assign a key holder upon encoding staff keys. (32996)
 - 🔗 Enable the [Staff/Vendor Management](#) system right or default [Maintenance Supervisor](#) system rights to the custom role.

Reports

- Read Key operations for Block, Unblock, Cancel and Resequence keys are not correctly displayed in the [System Activity Report](#). (28315)
- The "Key Type" column in the [System Activity Report](#) is blank for transactions related to mobile keys. (30600)


Encoders

- Encoders communicating via TCP/IP takes up to one minute to appear as *online* after connected/reconnected. (32936)

Online Communication

- If an access point is paired to a GWY II device, RAC5 device or GWY II API-associated controller and needs to be reconfigured as a different access point (for example, unit 100 needs to be reprogrammed as room 200), the original pairing persists causing remote operations to fail. (32988)
 - 🔗 Unpair the access point, then pair the newly configured access point to the GWY II device, RAC5 device or GWY II API-associated controller.

Monitoring

- The block/unblock key events are not always displayed in [Online/Events](#). (32818)
 - 🔗 Remotely or physically audit the access points to confirm that block/unblock key events are received to confirm that Block/Unblock key actions have been performed on access points..
- [Online/Access Point Status](#). Upon clicking (Refresh) , the "Privacy enabled" column is not updated with the proper access point status. (32952)
 - 🔗 Navigate to a different tab then reselect [the Online/Access Point Status](#) tab or refresh the page.

Notification Management

- Notification groups that include the "Fire alarm deactivated" or "Request to exit close" notification, cannot be created. (32942)

Requirements

This section lists minimum system, network, device and interface requirements for installing and using Community. Additional resources may be required based on site configuration and usage.

System Requirements

The following table lists minimum requirements for the Community Server and Community workstation. Ancillary recommendations are listed at the end of the table.¹

Requirement	Community Server	Community Workstation
CPU	<ul style="list-style-type: none"> ■ 2GHz/64-bit/quad core ■ Dedicated server (recommended) 	2GHz/64-bit/dual core
RAM	16 GB or more	8GB
Disk Drive Free Space	30GB ²	50MB
Network Controller	Gigabit Ethernet - 1Gb/second	Gigabit Ethernet - 1Gb/second
USB 2.0 Port	Required to connect encoder	Required to connect encoder
Operating System	<ul style="list-style-type: none"> ■ Microsoft Windows Server 2019/2016/2012 R2 Standard (English)—Suitable for large and small-scale implementations. Required for online communication. ■ Windows 10 Pro/Enterprise (English)—Use for small-scale implementations only (recommended maximum of 1,000 access points and two encoders).³ 	<ul style="list-style-type: none"> ■ Microsoft Windows 10 Pro/Enterprise (English)
Database ⁴	<ul style="list-style-type: none"> ■ SQL Server Express 2014/2017 ■ SQL Server 2014/2016 	N/A
Web Browser ⁵	<ul style="list-style-type: none"> ■ Google Chrome (latest) ■ Microsoft Edge (latest) 	<ul style="list-style-type: none"> ■ Google Chrome (latest) ■ Microsoft Edge (latest)

¹Additional recommended hardware for the Community Server includes: UPS Backup, Integrated HD

Graphics Card, Keyboard/Mouse.

²Additional free space may be required depending on database backup and archiving settings.

³ Windows 10 Pro/Enterprise does not support Online Communication, the online functionality implemented by deploying gateways.

⁴The Microsoft OLE Database Driver for SQL Server is also required. Community prompts to install the driver if it is not detected. Microsoft reports issues that prevent SQL Server from installing successfully on a Domain Controller. Avoid installing SQL Server on a Domain Controller.

⁵Recommended Web browser resolution: 1366 x 768 or greater.

Network Requirements



If you have a firewall, configuration changes may be required to make ports accessible to the Community Server.

The following table lists the default Community Server port settings.

Port	Protocol	Description
80	HTTP	Community Web User Interface
443	HTTPS	Community Web User Interface
28000	TCP	KABA RFID IP encoder

Device Requirements

This section lists the embedded devices required to use Community and the latest supported firmware versions.



Community is backward compatible with all previous firmware versions.

Encoders

The following table shows the encoders that Community supports and the latest supported firmware version.

KABA RFID	1.012
-----------	-------

Maintenance Units

The following table shows the M-Units that Community supports and the latest supported firmware version.

HH6	2.30
-----	------



The latest supported firmware versions are required when using the Community No Touring feature and when programming units and suite units in Multi-Housing Toggle Mode.

Locks

The following table shows the locks that Community supports and the latest supported firmware versions.

	Boot	Main	Quantum	BLE	ZigBee
Saflok MT, Pixel, Saflok Quantum, RCU (Remote Controller Unit)	10.14.20.4	10.14.20.4	02.06.19.1	1.1.1.0	1.10x
Saflok RT+, Saffire LX (L, M&P / D&I), Nova	04.02.20.4	04.02.20.4	N/A	1.1.1.0	5.12
Saflok Confidant	09.03.19.2	09.03.19.2	N/A	1.1.1.0	1.10x
Saflok RT	06.14.18.2	06.14.18.2	N/A	1.1.1.0	1.10x
RAC5	10.07.20.4	10.07.20.4	N/A	N/A	N/A



The latest supported firmware versions are required when using the Community No Touring feature and when programming units and suite units in Multi-Housing Toggle Mode.

Elevator Controllers

The following table shows the elevator controllers that Community supports and the latest supported firmware versions.

	Boot	Main	Quantum	BLE	ZigBee
MFC	N/A	0.017	N/A	N/A	N/A
EMCC	N/A	20090929	N/A	N/A	N/A
MCC 8/12	N/A	0.031398	N/A	N/A	N/A
ECU/RCU4	11.20.19.2	11.20.19.2	02.06.19.1	1.1.1.0	1.10x
RAC5	10.07.20.4	10.07.20.4	N/A	N/A	N/A

ZigBee Gateways

The following table shows the ZigBee gateways that Community supports and the latest supported firmware versions.

	Boot	Main	Quantum	BLE	ZigBee
GWY I	0.221	0.221			
GWY II	.015	.015			

Interface Requirements

Community supports the following:

- **Aurora SDK**—v1.0.19 to v1.0.21
- **Aurora software**—v1.0.19 to v1.0.21

Online Communication Interfaces and Devices

The following table shows the Online Gateway combinations that Community supports. For example, the Gateway I device is compatible with RAC5 and MFC elevator controllers, one dormakaba interface and one third-party interface.

	GWY I Device (legacy)	GWY II Device	GWY II API
RAC5 Elevator Controller	Yes	Yes	No
MFC Elevator Controller	Yes	No	No

	GWY I Device (legacy)	GWY II Device	GWY II API
dormakaba interface			
Aurora	Yes	Yes	Yes
3rd-party interface ¹			
Inncom®	Yes	No	No
Interel®	Yes	No	No
¹ mutually exclusive			

No Touring Requirements

To use the Community No Touring feature, the following requirements must be met:

- MT/RCU Series locks must be installed at Resident Common Areas.
- The locks must be updated to the latest firmware.
- The M-Unit (HH6) must be updated to the latest firmware.



For information about the M-Unit, refer to the *Saflok HH6 User Reference Guide*.

Community Server Upgrades

The following upgrade paths are supported:

- 1.6 and above to 2.0



Take a backup of the database before performing an upgrade. For online systems, take backups of SQL Server and MongoDB databases.

After the upgrade, you must restart the Community Server.

After the upgrade, restart the Community Server and log in to Community. The upgrade process preserves the Community database.

CONFIDENTIAL: This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of dormakaba.

© dormakaba Canada, 2020, All rights reserved. dormakaba and Community are trademarks of dormakaba Canada. All other trademarks are property of their respective owners.

PK#: 3696 Rev 20201214