Community Release Notes

Supporting Community 2.4.2

What's new

Community 2.4.2 announces the following new feature:

Security enhancements

- Added support to block key sequences at *System Keys > Block Keys*. The feature is available for staff keys made using Staff, Staff (variable access), Vendor, and Limited Use credentials. The essential purpose of this feature is to block access to common areas and elevator controllers for keys with the status *Obsolete*. Previously, access to common areas and elevator controllers remained until key expiration.

Corrected issues

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

Reference	Description
Reports / Key Expiration Report	
SD-2985	Reports now display expiration details for resident keys when the Resident credential class is selected.
Aurora integration	
SD-3013	Corrected an issue that caused the connection between Community and Aurora to fail after upgrades from version 2.0.x to 2.4.1.

Known issues

This section lists known issues and provides detailed work-around instructions.

Reference	**Issue**	**Workaround**
Entry System API		
SD-3050	Resident data does not synchronize with the Comelit entry system.	Contact dormakaba Support.

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

Minimum requirements for the Community server are based on the number of access points. Additional notes are listed at the end of the table. [1]

ℹ A dedicated server is recommended but not required.

	Server		Workstation
	Small ≤500 access points	Medium 500-2k access points	not applicable
CPU [2]	2GHz/Intel x64-bit/4 core	2GHz/Intel x64-bit/8 core	2GHz/Intel x64-bit/dual core

RAM	16 GB or more	16 GB or more	8GB
Disk Drive Free Space [3]	30GB	60GB	50MB
Network Controller	Gigabit Ethernet - 1Gb/second	Gigabit Ethernet - 1Gb/second	Gigabit Ethernet - 1Gb/second
USB 2.0 Port	Required to connect encoder	Required to connect encoder	Required to connect encoder
Operating System [4]	▪ Microsoft Windows Server 2025/2022/2019 Standard ▪ Microsoft Windows 10 Pro/Enterprise ▪ Microsoft Windows 11 Pro/Enterprise [5]	▪ Microsoft Windows Server 2025/2022/2019 Standard	▪ Microsoft Windows 10 Pro/Enterprise ▪ Microsoft Windows 11 Pro/Enterprise [5]
	Note: Windows 10 Pro/Enterprise and Windows 11 Pro/Enterprise do not support Remote Lock Management due to Microsoft limitations on the number of concurrent network connections.		
.NET Framework	8.0.x	8.0.x	not applicable
Database [6]	▪ SQL Server Express 2022/2019/2017 ▪ SQL Server 2022/2019/2016	▪ SQL Server Express 2022/2019/2017 ▪ SSQL Server 2022/2019/2016	not applicable
Web Browser [7]	▪ Google Chrome (latest) ▪ Microsoft Edge (latest)	▪ Google Chrome (latest) ▪ Microsoft Edge (latest)	▪ Google Chrome (latest) ▪ Microsoft Edge (latest)

[1] Additional recommended hardware for the server includes: UPS Backup, Integrated HD Graphics Card, Keyboard/Mouse.

[2] Supported CPUs: Intel and AMD x64.

[3] Additional free space may be required depending on database backup and archiving settings.

[4] Community is localized for all supported operating systems. Languages: English, French. Note that browser language settings may affect on-screen text.

[5] TPM (Trusted Platform Module) 2.0 is required to run Windows 11.

[6] a) SQL Server Express 2022 is bundled with Community and can be selected to install during installation. b) IMPORTANT: For security reasons, dormakaba strongly recommends SQL Server 2022 (or SQL Server Express 2022). c) IMPORTANT: Due to SQL Server Express limitations, dormakaba recommends SQL Server Standard for medium and large deployments. For details, consult Microsoft documentation. d) For large deployments, dormakaba recommends using a dedicated server for the Community database. e) Microsoft reports issues that prevent SQL Server from installing successfully on a Domain Controller. Avoid installing SQL Server on a Domain Controller.

[7] Recommended Web browser resolution: 1366 x 768 or greater.

Network requirements

The Property IT is responsible for establishing and maintaining a secure network (Ethernet or Wi-Fi) environment on which the Community server, workstations, and integrated interfaces are deployed and used.

Deployment on virtual machine

If deploying Community on a cloud VM (virtual machine), a VPN (virtual private network) is required to secure the communication between the site and cloud VM.

Communication ports

The following table lists the default Community Server port settings. If you have a firewall, configuration changes may be required to make ports accessible to the Community Server. Inbound ports require a firewall rule to allow communication with the server.

Although dormakaba recommends a dedicated server for Community, the following port ranges are available for third-party monitoring and scanning: 10000-14999 and 30000-39000.

Inbound Port	Outbound Port	Protocol	Description
80/443		HTTP/S	Community Web User Interface
8083/443		HTTP/S	Community API
28000/28001		TCP	dormakaba RFID Encoder I (28000)/dormakaba RFID Encoder II (28001, required for Enhanced Security Mode)

27700	27701	TCP	ONLINE – Gateway I, Control 4 (27701 is the listening port on the hardware)
28002		TCP	ONLINE – Gateway II, RAC5-MFC/XT
	23211	TCP	ONLINE – INNCOM (23211 is the listening port on the INNCOM server)
40100		HTTP/S	Community Client and Maintenance Unit. No firewall rule required. This port is not exposed to external computer; it is localhost only.

Device requirements

This section lists the embedded devices required to use Community and the **latest** firmware versions. Community devices are backward compatible with all previous firmware versions.

RFID keys

The following table shows the RFID key types that Community supports.

Key type	Enhanced Key Security	Standard Key Security	Legacy Key Security
MIFARE DESFire EV2/EV3	✓	✓	Not Supported
dormakaba RFID ComID Cards / Fobs (treated as MIFARE DESFire, not listed in user interface)	✓	✓	Not Supported
MIFARE Plus	✓	Not Supported	✓
MIFARE Ultralight C	✓	✓	Not Supported

Encoders

The following table lists the encoders that Community supports and the **latest** firmware version.

Encoder type	Latest FW	Supported key types
dormakaba RFID ENCODER I (part 064-514822 or 74750) (not supported when enhanced security mode enabled)	1.015	MIFARE Plus MIFARE Ultralight C
dormakaba RFID ENCODER II (part 75720) (required when Enhanced Security Mode enabled)	3.002 Applet version: 1.003	MIFARE DESFire EV2/EV3 MIFARE Plus MIFARE Ultralight C

Encoders that shipped before September 2022 may not have the applet version required for enhanced key security. For more information, contact dormakaba Support.

Maintenance units

The following table lists the M-Units that Community supports and the **latest** firmware versions.

Programmer type	Latest supported FW	Minimum FW for enhanced security
M-Unit SAFLOK HH6	1.53	Not Supported
M-Unit SAFLOK HH6 NFC (required when Enhanced Security Mode enabled)	2.46	2.40

Locks

The following table lists supported locks and the **latest** firmware versions.

Toggle mode is not currently supported for RAC5 when enhanced security mode is enabled.

The latest firmware versions are required when programming units and suite units in multi-family housing toggle mode.

Lock profile	Boot & Main	Supported readers	Supported key types	BLE	Zigbee AVR
Use with Enhanced, Standard and Legacy security					
Confidant NFC	03.24.25.4	Integrated reader	MIFARE DESFire EV2/EV3 MIFARE Plus MIFARE Ultralight C	1.3.1.0	1.10x, 5.13x, 6.05x
MT4/Quantum (secure boot)	07.22.25.4	Quantum (secure boot): 08.12.25.5	MIFARE Plus MIFARE Ultralight C	1.3.1.0	1.10x, 5.13x, 6.05x
Quantum MT6 (secure boot)	06.06.25.4	LEGIC	MIFARE DESFire EV2/EV3 MIFARE Plus MIFARE Ultralight C	3.1.0.0	1.10x, 5.13x, 6.05x
Pixel +	06.06.25.4	LEGIC	MIFARE DESFire EV2/EV3 MIFARE Plus MIFARE Ultralight C	3.1.0.0	1.10x, 5.13x, 6.05x
Pixel	07.22.25.4	Quantum (secure boot): 08.12.25.5	MIFARE Plus MIFARE Ultralight C	1.3.1.0	1.10x, 5.13x, 6.05x
Nova	03.24.25.4	Integrated reader	MIFARE DESFire EV2/EV3 MIFARE Plus MIFARE Ultralight C	1.3.1.0	1.10x/ 5.13x
RAC5 XT/Lite (hardware for common areas)	03.18.25.4 (Main only)	NFC Wall Reader: 03.31.25.3	MIFARE DESFire EV2/EV3 MIFARE Plus MIFARE Ultralight C	1.3.1.0	N/A
RCU4	07.22.25.4	SR Wall Reader: 07.22.25.3	MIFARE DESFire EV2/EV3 MIFARE Plus MIFARE Ultralight C	1.3.1.0	1.10x, 5.13x, 6.05x
RT+	03.24.25.4	Integrated reader	MIFARE DESFire EV2/EV3 MIFARE Plus MIFARE Ultralight C	1.3.1.0	1.10x, 5.13x, 6.05x
Saffire LXD	03.24.25.4	Integrated reader	MIFARE DESFire EV2/EV3 MIFARE Plus MIFARE Ultralight C	1.3.1.0	1.10x/ 5.13x
Use with Standard and Legacy security					
Confidant	09.03.19.2	Integrated reader	MIFARE Plus MIFARE Ultralight C	1.3.1.0	1.10x/ 5.13x
MT4/Quantum	08.03.21.4	Quantum (secure boot): 02.06.19.1	MIFARE Plus MIFARE Ultralight C	1.3.1.0	1.10x, 5.13x, 6.05x
RT	06.14.18.2	Integrated reader	MIFARE Plus MIFARE Ultralight C	1.3.1.0	1.10x, 5.13x, 6.05x

All lock profiles support all previous firmware versions except RT; the RT lock supports firmware versions since 2015.

The RT and legacy Confidant lock models do not support the extended common areas feature.

Elevator controllers

The following table lists supported elevator controllers and the **latest** firmware versions.

	Boot & Main	Supported readers	Supported key types	BLE	Zigbee AVR
Enhanced, Standard and Legacy security					
ECU/RCU4	07.22.25.4	Quantum (secure boot): 08.12.25.5	MIFARE Plus MIFARE Ultralight C	1.3.1.0	1.10x
RAC5-MFC	03.18.25.4	NFC Wall Reader: 03.31.25.3	MIFARE DESFire EV2/EV3 MIFARE Plus MIFARE Ultralight C	1.3.1.0	N/A
Standard and Legacy security					
ECU/RCU4	08.03.21.4	Quantum (secure boot):02.06.19.1	MIFARE Plus MIFARE Ultralight C	1.3.1.0	1.10x
Legacy MFC	0.017 (Main only)	Integrated reader	MIFARE Plus MIFARE Ultralight C	1.3.1.0	N/A
EMCC	20090929 (Main only)	Integrated reader	MIFARE Plus MIFARE Ultralight C	1.3.1.0	N/A
MCC 8/12	0.031398 (Main only)	Integrated reader	MIFARE Plus MIFARE Ultralight C	1.3.1.0	N/A

Zigbee gateways

The following table shows the Zigbee gateways that Community supports and the **latest** firmware versions.

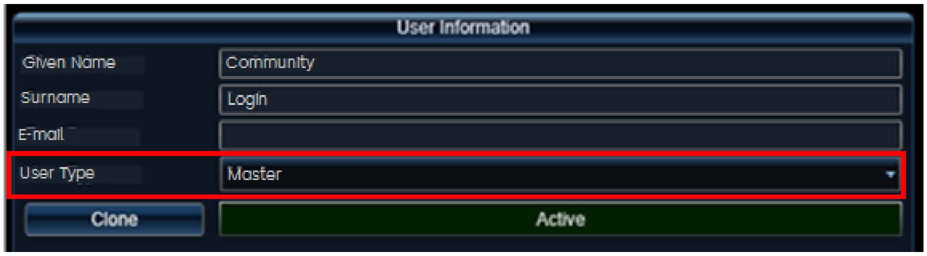
	Boot	BLE	Zigbee AVR
Gateway I	0.221	N/A	1.10x/5.13x
Gateway II	0.022	N/A	6.05x

Interface requirements

Community supports the following:

- Aurora licensed for SDK—v1.0.19 to v1.0.25

For sites with Aurora integrations, verify that the User Type is set to "Master" for the Community system user created in Aurora, per the Aurora Integration Manual. Other User Types will no longer work with Community 2.4.


User Information

Given Name: Community

Surname: Login

E-mail:

User Type: Master

For Aurora integrations, the following requirements apply when the Community license includes Visitor Management:

- Enable Extended PIN (7-digit), (Application)
- Enable Auto Generate PIN
- Enable Keyscan Credentials for Extended Card Format
- Enable KABA Integrated Mode
- Enable Auto Expiry mode
- Enable Card Count on ACUs
- Per ACU, select reader mode S - KABA Integration

For details, refer to the *Community Aurora Integration Deployment and Support Manual* (PK3769).

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 other Gateway I devices, RAC5 and MFC elevator controllers, and one third-party interface.

	Gateway I Device supported with	Gateway II Device supported with	Rx-Link supported with	RAC5-MFC/XT supported with
Gateway I Device	✓	Not Supported	Not Supported	✓
Gateway II Device	Not Supported	✓	✓	✓
Rx-Link	Not Supported	✓	✓	✓
RAC5-MFC	✓	✓	✓	✓
RAC5 XT	✓	✓	✓	✓
Legacy MFC	✓	Not Supported	Not Supported	Not Supported
Third-Party Interfaces (mutually exclusive)				
INNCOM®	✓	✓	✓	✓
INTEREL®	✓	Not Supported	Not Supported	Not Supported
Telkonet®	✓	Not Supported	Not Supported	Not Supported
Control4®	✓	Not Supported	Not Supported	Not Supported

Online communication lock support

The following table shows the locks supported with remote lock management (online communication).

	Gateway I / Legacy 3rd-Party Interfaces (Zigbee Gen I)	Gateway II / Rx-Link	
		Zigbee Gen II Phase 1	Zigbee Gen II Phase 2
Pixel	✓	✓	✓
Pixel+	✓	✓	✓
MT4	✓	✓	✓
MT6	✓	✓	✓
RCU4	✓	✓	✓
RT	✓	✓	Not Supported
RT+	✓	✓	✓

Saffire LX	✓	✓	✓
Nova	✓	✓	✓
Confidant	✓	✓	Not Supported
Confidant NFC	✓	✓	✓

No touring requirements

The No Touring feature cancels access to common areas when a resident key is canceled prior to the expiration date. To use the feature, the following requirements must be met:

- Supported lock profiles installed at resident common areas: MT/RCU series, Saffire series, Confidant NFC, RT+.
- The locks must be updated to the latest firmware versions.
- The M-Unit (HH6) must be updated to the latest firmware version.

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

General Data Protection Regulation (GDPR)

dormakaba's privacy policy statement can be found on the server at the following location: *\Community Server\GDPR*. Clients are encouraged to print a copy of the statement and have it available at your business premises for reference.

Upgrades

This chapter provides information and instructions for upgrading versions of Community and SQL Server.

Community upgrades

The following upgrade paths are supported:

- 1.6 and above to 2.4.2.

> Before upgrading, refer to *Community Enhanced Key Security* (PK3776) to learn about the requirements for enhanced security mode and for important information about upgrading without enabling enhanced security mode. The document is accessible at the root of the software download folder.

Pre-upgrade checklist

1	□	**IMPORTANT!** Server/Client. Verify that all Windows updates are installed.
2	□	Server. Take a backup of the database before performing an upgrade. For online systems, take backups of SQL Server and MongoDB databases.
3	□	Server/Client. Perform the installation as a **Local Administrator**.
4	□	Server. Make sure antivirus software is disabled before proceeding with server installation.
5	□	Server. If possible, disable Windows Defender for the duration of the installation.

Upgrade process

The upgrade is installed with the same options selected during the initial install.

1. In the dormakaba/Community folder, open the SERVER folder.
2. Double-click **CommunityServer.exe**. The installation wizard opens and prepares for setup.
3. On the Welcome page, click **Next**.
4. On the License Agreement page, accept the terms of the license agreement, then click **Next**. You can optionally print the agreement. The upgrade process starts.
5. When prompted, select whether to restart the server. Restart is required to complete the upgrade.

> The upgrade process includes upgrading the Community database.

Post-upgrade checklist

1	□	Restart the Community Server.
2	□	Server. Re-enable antivirus software.
3	□	Server. If necessary, re-enable Windows Defender.
4	□	Server. For installations using a remote SQL Server. On the Ambiance server, create a backup folder with the same name and directory that exists for backups on the remote server. For example, G:\backup must exist on both the Ambiance and remote servers.
5	□	Upgrade the Community Client installed on workstations. The server and client versions must be the same.
6	□	This step is recommended but not required for sites that do not enable enhanced security mode. Review RFID key type configurations at *System Settings > Advanced Settings > RFID key types*. Any change to settings requires reprogramming access points. Locks accept only those key types that are selected in System Settings.

ℹ To enable enhanced key security after upgrade, refer to *Community Enhanced Key Security* (PK3776). The document lists requirements and provides step-be-step instructions for enabling enhanced key security.

SQL Server upgrades

dormakaba strongly recommends using SQL Server 2022 (or SQL Server Express 2022).
To upgrade to SQL Server 2022:

1. Back up the Community database.
2. In Service Manager, stop all Community services.
3. Run the following command:

```
SQLEXPR_x64_ENU.exe /QS /ACTION=UPGRADE /INSTANCENAME=COMMUNITY /ISSVCAccount="NT Authority\Network Service"
/IACCEPTSQLSERVERLICENSETERMS
```

4. Restore backed up database.
5. Restart all Community services.

SQL Server 2022 (16.x) supports upgrade from the following versions of SQL Server:

- SQL Server 2012 (11.x) SP4 or later
- SQL Server 2014 (12.x) SP3 or later
- SQL Server 2016 (13.x) SP3 or later
- SQL Server 2017 (14.x)
- SQL Server 2019 (15.x)

Documentation

These release notes support Community 2.4.2. The information in these release notes supersedes all other documentation supporting this release.

The following core documents support this release:

- *Community Installation Guide* 2.4.0 PK3695
- *Community User Guide* 2.4.2 PK3706
- *Community Enhanced Key Security* 2.4.0 PK3776

Version 2.4.2 PK3696
9/18/2025