dormakaba

Community Release Notes

Supporting Community 2.5

What's new

Community 2.5 announces the following new features:

Security enhancements

- Implemented Single Sign-On support using the SAML protocol for more secure and simplified authentication.

Digital key usage

- Added feature to control and track the number of digital keys (mobile and wallet keys). See the Monitoring module. The licensed feature mobile keys must be enabled.

Mobile key payload support for Apple wallet

- You can now use the Community REST API to issue Apple wallet keys. The request returns a mobile key payload to be downloaded into a mobile app.

Corrected issues

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

Reference	Description
Remote unlock	
SD-2893	Remote unlock command can be sent to registered locks regardless of the status (online/offline) of the lock.
Entry System	
SD-2456	You can now generate authentication tokens during the Community - Entry System configuration.
SD-3050	Unit numbers are now visible in the COMELIT endpoint after data is synchronized.
Reports	
SD-2639	The Access Point Audit Report now refers to the following events: ■ "RELATCHED BY DEADBOLT" instead of "Unknown event (Level 27 / Type 7)" ■ "AUTO UNLATCH" instead of "Escape Return start"
SD-2907	The Key Expiration Report now includes all records that meet specified parameters when the report is generated for resident keys only.
Monitoring	
SD-2915	All keys are now listed by default at Monitoring / Keys.
Key Readback	
SD-2918	Resolved intermittent issue that caused key readback to fail for some resident keys.
MongoDB	
SD-3164	MongoDB v8.2.3 is recommended as a safe release.

Known issues

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

Reference	Issue	Workaround
Mobile keys		
55204	For fresh installs only. Mobile keys are not sent until the server is restarted after mobile key configuration in System Settings.	Restart the server after configuring mobile keys in System Settings.

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]

A dedicated server is recommended but not required.

	Server			Workstation
	Small < 500 access points	Medium 500-2k access points	Large > 2k access points	not applicable
CPU [2]	2GHz/Intel x64-bit/4 core	2GHz/Intel x64-bit/8 core	2GHz/Intel x64-bit/16 core	2GHz/Intel x64-bit/dual core
RAM	16 GB or more	16 GB or more	32 GB or more	8GB
Disk Drive Free Space [3]	30GB	60GB	100GB	50MB
Network Controller	Gigabit Ethernet - 1Gb/second	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	Required to connect encoder
Operating System [4]	▪ Microsoft Windows Server 2025/2022/2019 Standard ▪ Microsoft Windows 11 Pro/Enterprise [5]	▪ Microsoft Windows Server 2025/2022/2019 Standard	▪ Microsoft Windows Server 2025/2022/2019 Standard	▪ Microsoft Windows 11 Pro/Enterprise [5]
	Note: Microsoft Windows 11 Pro/Enterprise does not support Remote Lock Management due to MIcrosoft limitations on the number of concurrent network connections.			
.NET Framework	8.0.21.25475	8.0.21.25475	8.0.21.25475	not applicable
Database [6]	▪ SQL Server Express 2022/2019/2017 ▪ SQL Server 2022/2019/2016	▪ SQL Server Express 2022/2019/2017 ▪ SQL Server 2022/2019/2016	▪ SQL Server Express 2022/2019/2017 ▪ SQL 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)	▪ 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. Additional free space may be required depending on database backup and archiving settings.
[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 2022 Express is bundled with Community and can be selected to install during installation. b) IMPORTANT: For security reasons, dormakaba strongly recommends SQL Server 2022 (Standard or Express). 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. f) The storage media where SQL Server will be installed cannot exceed a sector size of 4096 bytes. Drives with larger sector sizes are not supported and will cause installation failure.
[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.

The Windows Sync Share service ports (80/443) conflict with the Community web user interface. dormakaba recommends to remove or disable this Windows feature.

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)
123	123	UDP	Open inbound and outbound access on UDP port 123 so that NTP (network time protocol) traffic is allowed and consistently reachable from the locks/gateways.
40100		HTTP/S	Community Client and Maintenance Unit. No firewall rule required. This port is not exposed to external computer; it is localhost only.

URL allow list

Establish an allow list for the following URLs:

- Licensing: https://api.simat.dormakaba-tech.com
- Mobile keys enabled: https://api.legicconnect.com

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	4.0.0.0	1.10x, 5.13x, 6.05x

Lock profile	Boot & Main	Supported readers	Supported key types	BLE	Zigbee AVR
Pixel +	06.06.25.4	LEGIC	MIFARE DESFire EV2/EV3 MIFARE Plus MIFARE Ultralight C	4.0.0.0	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	5.13x/ 6.05x
SRK (Secure Reader Keyscan)	09.19.25.3	LEGIC	MIFARE DESFire EV2/EV3 MIFARE Plus MIFARE Ultralight C	1.3.1.0	1.10x, 5.13x, 6.05x
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					

	Boot & Main	Supported readers	Supported key types	BLE	Zigbee AVR
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

SSO requirements

For sites that specify a server name (instead of IP address) during installation and plan to enable Single Sign-On, the server name specified when configuring the SSO ID provider must be all lowercase. For exmaple, using the SAML ID provider Okta, the following fields use the server name:

- Single sign-on URL
- Audience URI
- Other Requestable SSO URLs

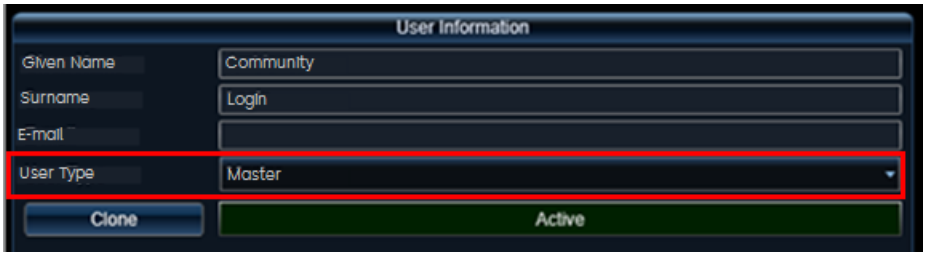
The server name specified during installation can use any character case.

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.



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
Telkonet Rhapsody	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*.

Third-party prerequisite components

The following table lists components installed with Community and validated for this release.

Third-Party Software	Version
Microsoft .NET Framework	4.8.1 Full
Microsoft .NET Desktop Runtime	8.0.21.25475
Microsoft ODBC Driver 17 for SQL Server	17.10.6.1
Microsoft Command Line Utilities 15 for SQL Server	15.0.4298.1
Microsoft OLE Database Driver for SQL Server	19.4.1.0
Microsoft OLE Database Driver for SQL Server	18.7.4.0
RabbitErlang	4.1.4
Redis on Windows	3.2.100
MongoDB	8.2.3 2008R2Plus SSL x64
Microsoft SQL Server Express (if selected)	2022 16.0.4215.2
Microsoft Visual C++ Redistributable	2013 12.0.40664.0 x86
Microsoft Visual C++ Redistributable	2015-2022 14.44.35112.1 x64
Microsoft Visual C++ Redistributable	2015-2022 14.44.35112.1 x86

Upgrades

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

In compliance with the GDPR (General Data Protection Regulation), when performing an upgrade with data encrypted with a generic symmetric key, all PII (Personally Identifiable Information) is re-encrypted with a site-specific symmetric key.

Community upgrades

The following upgrade paths are supported:

- 1.6 and above to 2.5

Community 2.3.0 introduced enhanced security mode to provide an additional layer of key security. Although the feature is disabled by default for upgrades, dormakaba strongly recommends enabling enhanced security mode.

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	☐	IMPORTANT! Server. For online-enabled sites, back up the MongoDB database. **This step is required to retain transaction data.**
3	☐	Server. Take a backup of the SQL Server database.
4	☐	Server/Client. Perform the installation as a Local Administrator.
5	☐	Server. Make sure antivirus software is disabled before proceeding with server installation.
6	☐	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	☐	For online-enabled properties that are upgrading from version 2.4.x and earlier to version 2.5 and later, and your SQL Server is remote, configure the backup location for MongoDB at *System Settings > Database Backup > MongoDB database backup settings*. If your SQL Server is local, the MongoDB backup continues to be saved in the MongoBackup folder where the SQL Server backups are stored, but you now have the option to configure a different location.
5	☐	Server. For online-enabled properties, restore the MongoDB database.
6	☐	Upgrade the Community Client installed on workstations. The server and client versions must be the same.
7	☐	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.

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 2.5. The information in these release notes supersedes all other documentation supporting this release.

The following core documents support this release:

- *Community Installation Guide* 2.5 PK3695
- *Community User Guide* 2.5 PK3706
- *Community Enhanced Key Security* 2.5 PK3776

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.

Version 2.5 PK3696
1/23/2026