

# Community Release Notes

## Community 2.3.1

### What's new

Community 2.3.1 is a maintenance release to deliver a corrected issue.

### Corrected issues

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

Reference	Description
System Settings	
SD-2457/48266	Can now issue resident keys with the disability option allowing for access points to remain in an unlocked state for a longer period of time after presenting the key.


### Known issues

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

Reference	Issue	Workaround
Upgrades		
47983	Community client service versions 2.2.3 and earlier are not compatible with Community server version 2.3.0.	Uninstall Community client service, download client service from Device Management and reinstall.
Community REST API		
47939	The Community REST API is unresponsive if HTTPS is enabled after installation using the Service Manager.	<ul style="list-style-type: none"> <li>▪ For fresh installs: Make sure to configure Community with an SSL certificate during installation.</li> <li>▪ For upgrades:               <ul style="list-style-type: none"> <li>▪ Backup Community database.</li> <li>▪ Uninstall Community.</li> <li>▪ Reinstall Community and configure an SSL certificate during installation.</li> <li>▪ Restore Community database.</li> </ul> </li> </ul>
Internationalization		
SD-2132/43715	Some strings may appear in English only.	None
System Settings		
38314	<a href="#">Advanced Settings/RFID key types</a> . MIFARE DESFire keys are accepted by access points regardless of the selected settings.	None
43387	<a href="#">Enhanced Security Mode</a> . Keys encoded prior to enabling enhanced security mode cannot be read in transition mode.	None

Reference	Issue	Workaround
44306	<a href="#">Security/Enhanced Security Mode and Advanced Settings/RFID key types</a> . Settings related to enhanced security may not display.	Clear browser cache and refresh page.
47590	<a href="#">Enhanced Security Mode</a> . After enabling enhanced security mode, all encoders must be reconnected before encoding and reading keys.	None
Device Management		
38741	<a href="#">Registered Gateways &amp; Paired Access Points</a> . The registered Saffire DX locks currently display as Saffire LX locks on the Access Points page. ( )	
40278	There is currently no warning flag displayed when the current Main RAC5 firmware version differs from the reference version to upgrade.	Proceed with the remote firmware upgrade.
Staff/Vendor Management		
35320/35321	The lost or defective keys replaced in Staff/Vendor Management > Assigned Keys are not displayed in the Key/User Assignment Report or at Monitoring > Keys.	View replaced, lost and defective keys at Staff/Vendor Management > Assigned Keys.
System Keys		
33490	Upon blocking a vendor or staff (variable access) key in access points, a new key is denied access in these access points.	Community UI: Create a new vendor or staff (variable access) credential in Credential Management and encode a new key with this credential.  Community API: Encode new vendor or staff (variable access) keys with a different credential.
Visitor Management		
35555	If multiple mobile devices running the BlueSky app request PINs or mobile key delegates concurrently, some requests may timeout and fail.	Using the BlueSky app, request the PIN or mobile key delegate again.
36355	Upon updating the mobile device with modified visitor management settings, the status remains "Updating mobile device...".	Refresh the page to view updated status.
Monitoring		
30784	<a href="#">Keys</a> . The operator name is currently not displayed for LGS SOAP API (PMS Web Service) AddSharedGuest requests.	None
Reports		
35391	Visitor Management Report. If a report is generated for one user type (residents or staff/vendors), then a second report is generated for the alternate user type, the second report includes data for both user types.	Refresh the browser page before generating the second report.

Reference	Issue	Workaround
Online Communication		
32987	<a href="#">Registered Gateways &amp; Paired Access Points</a> . The Verify Assignment command is currently not supported from the Gateways page.	Perform the Verify Assignment command on the desired access points from the Access Points page.
34012	<a href="#">Online Access Points Status Report</a> . The report currently displays an error when no access points have yet been paired.	Pair at least one access point then generate the report.
34900	<a href="#">Rx-Link</a> . The "Unpair all access points" and "Unpair access point" commands in Device Management/Registered Gateways & Paired Access Points /Gateways and Access Points are currently not supported for Rx-Link.	To unpair access points, use the "Pairing OFF" key in access points.
34961	<a href="#">Control4</a> . If the LUA driver that commissioned the gateway in Community is deleted, commands to the gateway sent from Community no longer work.	Delete the gateway in Device Management/Registered Gateways & Paired Access Points/ Gateways and recommission the Control4 controller.
Encoding		
None	An intermittent issue causes an encoder to go offline.	Enable WebSocket Protocol in Windows Features. The option is located at: Internet Information Services > World Wide Web Services > Application Development Features > WebSocket Protocol.
Community API		
33292	Upon requesting a resident key for an existing lease, the request must include all units already assigned to the lease plus any additional units.	None
Read key		
35043	Upon reading a MIFARE Mini or Ultralight C key, the <a href="#">View Guest Access Report</a> and <a href="#">View Staff Access Report</a> buttons are available in the Read Key dialog even though these key technologies do not support the guest and staff access tracking functionality.	None
Aurora		
29933	Remote unit assignment modifications in regards to Resident Common Areas are not synchronized to the Aurora server.	Create resident keys to synchronize new Resident Common Area access to the Aurora server.
35323	Perimeter FOB. Upon updating the expiration date for an expired perimeter FOB in Resident Management or Staff/Vendor Management, the previous records at Monitoring > Keys show the FOB as active instead of expired.	
Context Help		

Reference	Issue	Workaround
None	Product Help that displays on a separate browser tab is not automatically context-sensitive.	On the browser tab where the user interface displays, click (Help)  to update the Help content on the separate tab.

## 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. <sup>1</sup>

 A dedicated server is recommended but not required.

	Server		Workstation
	Small ≤ 500 access points	Medium 500-2k access points	not applicable
CPU	2GHz/64-bit/4 core	2GHz/64-bit/8 core	2GHz/64-bit/dual core
RAM	16 GB or more	16 GB or more	8GB
Disk Drive Free Space <sup>2</sup>	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 <sup>3</sup>	<ul style="list-style-type: none"> <li>▪ Microsoft Windows Server 2022/2019/2016</li> <li>▪ Microsoft Windows 10 Pro/Enterprise <sup>4</sup></li> <li>▪ Microsoft Windows 11 Pro/Enterprise <sup>5</sup></li> </ul>	<ul style="list-style-type: none"> <li>▪ Microsoft Windows Server 2022/2019/2016</li> </ul>	<ul style="list-style-type: none"> <li>▪ Microsoft Windows 10 Pro/Enterprise</li> <li>▪ Microsoft Windows 11 Pro/Enterprise <sup>4</sup></li> </ul>
.NET Framework	6.0.x	6.0.x	not applicable
Database <sup>6</sup>	<ul style="list-style-type: none"> <li>▪ SQL Server Express 2022/2019/2017/2014</li> <li>▪ SQL Server 2022/2019/2016/2014</li> </ul>	<ul style="list-style-type: none"> <li>▪ SQL Server Express 2022/2019/2017/2014</li> <li>▪ SQL Server 2022/2019/2016/2014</li> </ul>	not applicable
Web Browser <sup>7</sup>	<ul style="list-style-type: none"> <li>▪ Google Chrome (latest)</li> <li>▪ Microsoft Edge (latest)</li> </ul>	<ul style="list-style-type: none"> <li>▪ Google Chrome (latest)</li> <li>▪ Microsoft Edge (latest)</li> </ul>	<ul style="list-style-type: none"> <li>▪ Google Chrome (latest)</li> <li>▪ Microsoft Edge (latest)</li> </ul>

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

<sup>2</sup> Additional free space may be required depending on database backup and archiving settings.

<sup>3</sup> Community is localized for all supported operating systems. Languages: English, French. Note that browser language settings may affect on-screen text.

<sup>4</sup> Windows 10 Pro/Enterprise does not support Online Communication.

<sup>5</sup> a) Windows 11 Pro/Enterprise does not support Online Communication. b) TPM (Trusted Platform Module) 2.0 is required to run Windows 11.

<sup>6</sup> 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.

<sup>7</sup> 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 WiFi) 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.

Port	Protocol	Description
80	HTTP	Community Web User Interface
8083/443	HTTPS	Community Web User Interface, 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
28002	TCP	ONLINE – Gateway II, RAC5-MFC/XT
23211	TCP	ONLINE – INNCOM
40100	HTTP/S	Community Client and Maintenance Unit

## 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 Ultralight C®	✓	✓	Not Supported
MIFARE Plus®	✓	Not Supported	✓
MIFARE® DESFire EV2/EV3	✓	✓	✓

### 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, ULC
dormakaba RFID ENCODER II (part 75720) (required when Enhanced Security Mode enabled)	2.013 Applet version: 1.003	MIFARE DESFire, Plus, ULC

### 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	Supported key types
M-Unit SAFLOK HH6	1.53	Not Supported	MIFARE DESFire, Plus, ULC
M-Unit SAFLOK HH6 NFC (required when Enhanced Security Mode enabled)	2.40	2.40	MIFARE DESFire, Plus, ULC

**Locks**

The following table lists supported locks and the **latest** firmware versions. The BLE version for all locks is 1.3.1.0.



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



Toggle mode is supported for standard and legacy security. The latest firmware versions are required when programming units and suite units in multihousing toggle mode.

Lock profile	Boot & Main	Supported readers	Supported key types	Zigbee AVR
<b>Use with Enhanced, Standard and Legacy security</b>				
Confidant NFC	11.21.23.4	Integrated reader	MIFARE DESFire, Plus, ULC	1.10x/5.13x / 6.05x
MT4 (secure boot)	06.13.23.4	<ul style="list-style-type: none"> <li>Quantum (secure boot): 05.26.23.1</li> </ul>	MIFARE Plus, ULC	1.10x/5.13x/6.05x
Quantum MT6 (secure boot)	01.12.24.4	<ul style="list-style-type: none"> <li>Quantum (secure boot): 05.26.23.1</li> </ul>	MIFARE DESFire, Plus, ULC	1.10x/5.13x/6.05x
Nova	11.21.23.4	Integrated reader	MIFARE DESFire, Plus, ULC	5.13x / 6.050
Pixel	06.13.23.4	<ul style="list-style-type: none"> <li>Quantum (secure boot): 05.26.23.1</li> </ul>	MIFARE Plus, ULC	1.10x/5.13x/6.05x
Quantum (secure boot)	06.13.23.4	<ul style="list-style-type: none"> <li>Quantum (secure boot): 05.26.23.1</li> </ul>	MIFARE Plus, ULC	1.10x/5.13x/6.05x
RAC5 XT/Lite (hardware for common areas)	08.22.23.4(Main only)	<ul style="list-style-type: none"> <li>SRK (NFC Wall) Reader: 11.10.23.4</li> </ul>	MIFARE DESFire, Plus, ULC	N/A
RCU4	06.13.23.4	<ul style="list-style-type: none"> <li>Quantum (secure boot): 05.26.23.1</li> </ul>	MIFARE Plus, ULC	1.10x/5.13x/6.05x
RT+	11.21.23.4	Integrated reader	MIFARE DESFire, Plus, ULC	1.10x/5.13x / 6.05x
Saffire LX	11.21.23.4	Integrated reader	MIFARE DESFire, Plus, ULC	5.13x / 6.05x
Saffire LXD	11.21.23.4	Integrated reader	MIFARE DESFire, Plus, ULC	5.13x / 6.05x
<b>Use with Standard and Legacy security</b>				
Confidant	09.03.19.2	Integrated reader	MIFARE Plus, ULC	1.10x/5.13x
MT4	08.03.21.4	<ul style="list-style-type: none"> <li>Quantum (secure boot): 02.06.19.1</li> </ul>	MIFARE Plus, ULC	1.10x/5.13x/6.05x
Quantum	08.03.21.4	<ul style="list-style-type: none"> <li>Quantum (secure boot): 02.06.19.1</li> </ul>	MIFARE Plus, ULC	1.10x/5.13x/6.05x
RT	06.14.18.2	Integrated reader	MIFARE Plus, ULC	1.10x/5.13x/6.05x



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

## Elevator controllers

The following table lists supported elevator controllers and the **latest** firmware versions. The BLE version for all elevator controllers is 1.3.1.0.

	Boot & Main	Supported readers	Supported key types	Zigbee AVR
<b>Enhanced, Standard and Legacy security</b>				
ECU/RCU4	06.13.23.4	Quantum (secure boot): 05.26.23.1	MIFARE Plus, ULC	1.10x
RAC5-MFC	08.22.23.4	<ul style="list-style-type: none"> <li>▪ Integrated reader</li> <li>▪ SRK (NFC Wall) Reader: 11.10.23.4</li> </ul>	DESFire, MIFARE Plus, ULC	N/A
<b>Standard and Legacy security</b>				
ECU/RCU4	08.03.21.4	Quantum (secure boot): 02.06.19.1	MIFARE Plus, ULC	1.10x
Legacy MFC	0.017 (Main only)	Integrated reader	MIFARE Plus, ULC	N/A
EMCC	20090929 (Main only)	Integrated reader	MIFARE Plus, ULC	N/A
MCC 8/12	0.031398 (Main only)	Integrated reader	MIFARE Plus, ULC	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 SDK](#)—v1.0.19 to v1.0.24
- [Aurora software](#)—v1.0.19 to v1.0.24



(Aurora integrations only) In Aurora, the following requirements apply when Community license includes Visitor Management:

- Minimum Aurora version is 1.0.24.
- 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	✓	✓	✓
MT4	✓	✓	✓
MT6	✓	✓	✓
RCU4	✓	✓	✓
RT	✓	✓	Not Supported
RT+	✓	✓	✓
Saffire LX	✓	✓	✓
Nova	✓	✓	✓
Confidant	✓	✓	Not Supported
Confidant NFC	✓	✓	✓

## 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 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*.



## 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 2.3.1.



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	<input type="checkbox"/>	<b>IMPORTANT!</b> Server/Client. Verify that all Windows updates are installed.
2	<input type="checkbox"/>	Server. Take a backup of the database before performing an upgrade. For online systems, take backups of SQL Server and MongoDB databases.
3	<input type="checkbox"/>	Server/Client. Perform the installation as a <b>Local Administrator</b> .
4	<input type="checkbox"/>	Server. Make sure antivirus software is disabled before proceeding with server installation.
5	<input type="checkbox"/>	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.

#### Post-upgrade checklist

1	<input type="checkbox"/>	Restart the Community Server.
2	<input type="checkbox"/>	Server. Re-enable antivirus software.
3	<input type="checkbox"/>	Server. If necessary, re-enable Windows Defender.
4	<input type="checkbox"/>	Upgrade the Community Client installed on workstations. The server and client versions must be the same.
5	<input type="checkbox"/>	This step is recommended but not required for sites that do not enable enhanced security mode. Review RFID key type configurations at <a href="#">System Settings &gt; Advanced Settings &gt; RFID key types</a> . Any change to settings requires reprogramming access points. Locks accept only those key types that are selected in <a href="#">System Settings</a> .



To enable enhanced key security after upgrade, refer to *Community Enhanced Key Security (PK3776)*. The document lists requirements and provides step-by-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 2.3.1. The information in these release notes supersedes all other documentation supporting this release.

The following core documents support this release:

- *Community Installation Guide 2.3.x-x* PK3695
- *Community User Guide 2.3.x-x* PK3706
- *Community Enhanced Key Security 2.3.x-x* PK3776

**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, 2024, All rights reserved. dormakaba and Community are trademarks of dormakaba Canada. All other trademarks are property of their respective owners. MIFARE, MIFARE Classic, MIFARE Plus, MIFARE Ultralight, and MIFARE DESFire EV2/EV3 are registered trademarks of NXP B.V.

PK#: 3696 Rev 5/1/2024