

[Ambiance 2.12.5 - download link](#)

What's new

Ambiance 2.12.5 is a maintenance release to deliver corrected issues.

Corrected issues


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

Reference	Description
Installation	
SD-2798/SD-2786/ SD-2765	A problem that caused certain services to fail to start after updating Windows is now resolved.
PMS	
SD-2855	LGS REST API. Keys are issued with the appropriate guest common area access, as specified in the LGS REST API requests and defined in the common area profile.
Guest Registration	
SD-2817	Pre-registered guest keys can now be issued with the correct check-in and check-out dates/times when using Ambiance in French.

Known issues

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

Reference	Issue	Workaround
Internationalization		
SD-2132/43715	Some strings may appear in English.	None
34627	Upon printing or downloading a report in Chinese, some characters are not displayed correctly.	None
PMS		
52270	LGS SOAP API. After upgrading Ambiance to this version, a 15-minute waiting period may be required before API requests can be processed.	None
System Settings / Enhanced Security Mode		
43387	Keys encoded prior to enabling enhanced security mode cannot be read in transition mode.	None
50317	After enabling enhanced security mode, encoders do not automatically reinitialize.	Disconnect and reconnect all encoders after enabling enhanced security mode.
Device Management		
40278	No warning flag displays when the RAC5 firmware version differs from the reference version.	Proceed with the remote firmware upgrade.

Reference	Issue	Workaround
Staff Management		
35320/35321	The lost or defective keys replaced in StaffManagement > Assigned Keys are not displayed in the Key/User Assignment Report or at Monitoring > Keys.	View replaced, lost and defective keys at Staff Management > Assigned Keys.
Guest Registration		
None	When the operator selects a Check Out date that is the same day as the Check In date, the system initially reverts to the default Check Out date.	Reselect the desired Check Out date and time.
Online Communication		
32987	Registered Gateways & Paired Access Points . 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	Online Access Points Status Report . 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	Rx-Link . 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	Control4 . If the LUA driver that commissioned the gateway in Ambiance is deleted, commands to the gateway sent from Ambiance 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.
Aurora / MATRIX		
29933	Remote unit assignment modifications in regards to Guest Common Areas are not synchronized to the Aurora server or MATRIX server.	Create guest keys to synchronize new GuestCommon Area access to the Aurora server or MATRIX server.
Context Help		
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 Ambiance. Additional resources may be required based on site configuration and usage.

System Requirements

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



Ambiance requires a dedicated server.

	Server			Workstation
	Small ≤ 500 access points	Medium 500-3k access points	Large ≥ 3k access points	not applicable
CPU ²	2GHz/x64-bit/4 core	2GHz/x64-bit/8 core	2GHz/x64-bit/16 core	2GHz/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	<ul style="list-style-type: none"> Microsoft Windows Server 2022/2019/2016 Standard Microsoft Windows 10 Pro/Enterprise⁵ Microsoft Windows 11 Pro/Enterprise^{5, 6} 	<ul style="list-style-type: none"> Microsoft Windows Server 2022/2019/2016 Standard 	<ul style="list-style-type: none"> Microsoft Windows Server 2022/2019/2016 Standard 	<ul style="list-style-type: none"> Microsoft Windows 8.1 Pro/Enterprise Microsoft Windows 10 Pro/Enterprise Microsoft Windows 11 Pro/Enterprise⁵
.NET Framework	8.0.x	8.0.x	8.0.x	not applicable
Database ⁷	<ul style="list-style-type: none"> SQL Server Express 2022/2019/2017 SQL Server 2022/2019/2016 	<ul style="list-style-type: none"> SQL Server Express 2022/2019/2017 SQL Server 2022/2019/2016 	<ul style="list-style-type: none"> SQL Server Express 2022/2019/2017 SQL Server 2022/2019/2016 	not applicable
Web Browser ⁸	<ul style="list-style-type: none"> Google Chrome (latest) Microsoft Edge (latest) 	<ul style="list-style-type: none"> Google Chrome (latest) Microsoft Edge (latest) 	<ul style="list-style-type: none"> Google Chrome (latest) Microsoft Edge (latest) 	<ul style="list-style-type: none"> 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 data retention settings.

⁴ Ambiance is localized for all supported operating systems. Languages: English, German, Spanish, French, Italian, Japanese, Polish, Brazilian Portuguese, Russian, and Chinese. Note that browser language settings may affect on-screen text.

⁵ Windows 10 Pro/Enterprise and Windows 11 Pro/Enterprise do not support Online Communication due to Microsoft limitations on the number of concurrent network connections.

⁶ TPM (Trusted Platform Module) 2.0 is required to run Windows 11.

⁷ a) SQL Server 2022 Express is bundled with Ambiance 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 Ambiance database. e) Microsoft reports issues that prevent SQL Server from installing successfully on a Domain Controller. Avoid installing SQL Server on a Domain Controller.

⁸ 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 Ambiance server, workstations, and integrated interfaces are deployed and used.

Deployment on Virtual Machine

If deploying Ambiance 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 Ambiance Server port settings. If you have a firewall, configuration changes may be required to make ports accessible to the Ambiance Server. Inbound ports require a firewall rule to allow communication with the server.

Inbound Port	Outbound Port	Protocol	Description
80/443		HTTP/S	Ambiance Web User Interface, PMS – LGS SOAP API (80 for HTTP/443 for HTTPS)
28000/28001		TCP	dormakaba RFID Encoder I (28000)/dormakaba RFID Encoder II (28001, required for Enhanced Security Mode)
5120/5121		HTTP/S	PMS – LGS REST API (5120 for HTTP/5121 for HTTPS)
8265		TCP	PMS – Oracle FIAS
9898		HTTP	PMS – BART (configurable in PMS.BART.Service.Host.exe.Config)
8264		TCP	PMS – SAFLOK IRS
9090		HTTP/S	PMS – LGS REST API (KF2)
5020/5021		HTTP/S	PMS – SkyTouch (5020 for HTTP/5021 for HTTPS)
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	Ambiance 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 Ambiance and the **latest** firmware versions. Ambiance devices are backward compatible with all previous firmware versions.

RFID keys

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



The MIFARE Ultralight AES key type requires compatible lock and encoder firmware. Contact dormakaba Support for more information.

Key type	Enhanced Key Security	Standard Key Security	Legacy Key Security
MIFARE DESFire EV2/EV3	✓	✓	Not Supported
MIFARE Ultralight AES	✓ (with additional requirements)	Not Supported	Not Supported
MIFARE Ultralight C	✓	✓	Not Supported
MIFARE Plus	✓	Not Supported	✓

The following table shows the RFID key type support for folio data formats. For more information about the limitations, see *Folio Data Format Specifications* PK3758.

Key type	Auto-Format	Custom layout (PMS and/or user interface)		
		ASCII	BCD Format 1	BCD Format 2
MIFARE Ultralight AES	Not Supported	✓ (with limitations)	✓ (with limitations)	✓ (with limitations)
MIFARE Ultralight C	Not Supported	✓ (with limitations)	✓ (with limitations)	✓ (with limitations)
MIFARE Plus	✓	✓	✓	✓

Encoders

The following table lists the encoders that Ambiance 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)	3.001 Applet version: 1.003	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 Ambiance 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. The BLE version for all locks is 1.3.1.0.

Lock profile	Boot & Main	Supported readers	Supported key types	Zigbee AVR
Use with Enhanced, Standard and Legacy security				
Confidant NFC	04.29.24.4	Integrated reader	MIFARE Plus MIFARE Ultralight C	1.10x/5.13x / 6.05x
MT4 (secure boot)	06.28.24.4	▪ Quantum (secure boot): 06.18.24.5	MIFARE Plus MIFARE Ultralight C	1.10x/5.13x/6.05x
Quantum MT6 (secure boot)	10.03.24.4	LEGIC	MIFARE Plus MIFARE Ultralight C	1.10x/5.13x/6.05x
Pixel	06.28.24.4	▪ Quantum (secure boot): 06.18.24.5	MIFARE Plus MIFARE Ultralight C	1.10x/5.13x/6.05x
Quantum (secure boot)	06.28.24.4	▪ Quantum (secure boot): 06.18.24.5	MIFARE Plus MIFARE Ultralight C	1.10x/5.13x/6.05x
RAC5 XT/Lite (hardware for common areas)	08.22.23.4 (Main only)	▪ SRK (NFC Wall) Reader: V_07.04.24.3	MIFARE Plus MIFARE Ultralight C	N/A

Lock profile	Boot & Main	Supported readers	Supported key types	Zigbee AVR
RCU4	06.28.24.4	■ Quantum (secure boot): 06.18.24.5	MIFARE Plus MIFARE Ultralight C	1.10x/5.13x/6.05x
RT+	04.29.24.4	Integrated reader	MIFARE Plus MIFARE Ultralight C	1.10x/5.13x / 6.05x
Saffire LX	04.29.24.4	Integrated reader	MIFARE Plus MIFARE Ultralight C	5.13x / 6.05x
Use with Standard and Legacy security				
Confidant	09.03.19.2	Integrated reader	MIFARE Plus MIFARE Ultralight C	1.10x/5.13x
MT4	08.03.21.4	■ Quantum (secure boot): 02.06.19.1	MIFARE Plus MIFARE Ultralight C	1.10x/5.13x/6.05x
Quantum	08.03.21.4	■ Quantum (secure boot): 02.06.19.1	MIFARE Plus MIFARE Ultralight C	1.10x/5.13x/6.05x
RT	06.14.18.2	Integrated reader	MIFARE Plus MIFARE Ultralight C	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
Enhanced, Standard and Legacy security				
ECU/RCU4	06.28.24.4	Quantum (secure boot): 05.26.23.1	MIFARE Plus MIFARE Ultralight C	1.10x
RAC5-MFC	08.22.23.4	■ Integrated reader ■ SRK (NFC Wall) Reader: V_07.04.24.3	MIFARE Plus MIFARE Ultralight C	N/A
Standard and Legacy security				
ECU/RCU4	08.03.21.4	Quantum (secure boot): 02.06.19.1	MIFARE Plus MIFARE Ultralight C	1.10x
Legacy MFC	0.017 (Main only)	Integrated reader	MIFARE Plus MIFARE Ultralight C	N/A
EMCC	20090929 (Main only)	Integrated reader	MIFARE Plus MIFARE Ultralight C	N/A
MCC 8/12	0.031398 (Main only)	Integrated reader	MIFARE Plus MIFARE Ultralight C	N/A

Zigbee Gateways

The following table shows the Zigbee gateways that Ambiance 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

Ambiance supports the following:

- [Aurora SDK](#)—v1.0.19 to v1.0.24
- [Aurora software](#)—v1.0.19 to v1.0.24
- [MATRIX](#)—v4.1.2

Online Communication Interfaces and Devices

The following table shows the Online Gateway combinations that Ambiance 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	✓	✓	✓
Confidant	✓	✓	Not Supported
Confidant NFC	✓	✓	✓

General Data Protection Regulation (GDPR)

dormakaba's privacy policy statement can be found on the server at the following location: `\Ambiance 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 Ambiance and SQL Server.

Ambiance upgrades

The following upgrade paths are supported:

- 1.4 and above to 2.12.5.



Ambiance 2.10.0 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 *Ambiance Enhanced Key Security* (PK3777) 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"/>	IMPORTANT! For sites that use MIFARE Classic keys and plan to either upgrade without enabling enhanced security mode or plan to upgrade using the transitional approach, follow the instructions provide in <i>Ambiance Enhanced Key Security for Upgrades</i> (PK3777). All MIFARE Classic keys must be remade using a supported RFID key type.
2	<input type="checkbox"/>	IMPORTANT! Server/Client. Verify that all Windows updates are installed.
3	<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.
4	<input type="checkbox"/>	Server/Client. Perform the installation as a Local Administrator .
5	<input type="checkbox"/>	Server. Make sure antivirus software is disabled before proceeding with server installation.
6	<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/Ambiance folder, open the SERVER folder.
2. Double-click **AmbianceServer.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 Ambiance 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 Ambiance 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 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 *Ambiance Enhanced Key Security for Upgrades* (PK3777). 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 Ambiance database.
2. In Service Manager, stop all Ambiance services.
3. Run the following command:
`SQLXPR_x64_ENU.exe /QS /ACTION=UPGRADE /INSTANCENAME=AMBIANCE/ISSVCAccount="NT Authority\Network Service" /IACCEPTSQLSERVERLICENSETERMS`
4. Restore backed up database.
5. Restart all Ambiance 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 Ambiance 2.12.5. The information in these release notes supersedes all other documentation supporting this release.

The following core documents support this release:

- *Ambiance Installation Guide 2.12.0* PK3701
- *Ambiance User Guide 2.12.0* PK3722
- *Ambiance Enhanced Key Security for Upgrades 2.12.0* PK3777

Amendments to product documentation

System Settings / Security

For the Login Protection setting [Failed login threshold for account suspension](#), the valid values are 3-30.

System Settings / PMS

Localized Help only. Refer to the following instructions for configuring LGS REST API (KF2).

The screenshot shows a configuration window titled 'LGS REST API (KF2)'. It contains four settings:

- Maximum RFID keys per request:** A numeric input field with a value of 6, flanked by minus and plus buttons.
- Enable HTTPS:** A checkbox with a blue 'YES' button.
- TCP/IP port:** A numeric input field with a value of 9090, flanked by minus and plus buttons.
- Web service URL:** A text input field containing 'https://*:9090/'.

- Select the maximum number of RFID keys per request. Valid values: 1-25. Default: 6.
- Select whether to enable HTTPS for secure communication between the PMS and servers. Default: YES. When HTTPS is enabled, go to [System Settings > Security > HTTPS Certificate](#), and set [Enable automatic CAPI store certificate renewal](#) to YES.
- Specify the port number. Default: 9090. The default value is good for both HTTP and HTTPS. After saving the settings, bind the certificate to the port.
- Specify the Web service URL for REST requests.

System Settings / Failsafe Keys

Localized Help only. Refer to the following information about Failsafe keys.

Failsafe keys are backups of individual guest room keys that are made in advance and maintained in complete sets to be issued to guests in the event of a system or power failure. The recommendation is to create and maintain two sets of three keys for each guest room and suite door. After one set of Failsafe keys is issued and used, make another set of Failsafe keys to replace the used set. Locks only accept keys from the two most recent Failsafe key sets.

Using a Failsafe key invalidates previous guest key access to guest rooms, suite common doors and suite inner doors.

System Settings / Advanced / RFID key types

Localized Help only. Refer to the following information about RFID key types.

- Enhanced Key Security—Only available when enhanced security mode is enabled. When enabled, options in Standard and Legacy Key Security are disabled.
 - MIFARE Ultralight AES—Selected by default for new installations. For upgrades, selected if previously selected or upon enabling Enhanced Security Mode if previously selected in Standard Key Security.
 - MIFARE Ultralight C—Selected by default for new installations. For upgrades, selected if previously selected or upon enabling Enhanced Security Mode if previously selected in Standard Key Security. When selected, MIFARE Ultralight AES is required.
 - MIFARE Plus—Selected by default for new installations. For upgrades, selected if previously selected or upon enabling Enhanced Security Mode if previously selected in Legacy Key Security.
- Standard Key Security—Disabled when enhanced security mode is enabled. MIFARE DESFire EV2/EV3—Default selection for new installations.
 - MIFARE Ultralight AES—Selected by default for new installations. For upgrades, selected by default if previously selected.
 - MIFARE Ultralight C—Selected by default for new installations. For upgrades, selected by default if previously selected. When selected, MIFARE Ultralight AES is required.
- Legacy Key Security—Disabled when enhanced security mode is enabled. Selecting an option in this section prompts a security reminder message.
 - MIFARE Plus—Unselected by default for new installations. For upgrades, selected by default if previously selected.
 - MIFARE Classic—Not supported for new installations. For upgrades, only displays if previously selected. Contact dormakaba Support.

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, 2025, All rights reserved. dormakaba and Ambiance 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.

Version 2.12.5-0 PK3702