

Ambiance

Installation Guide

dormakaba Canada, Inc.
105 Marcel-Laurin Blvd
Montreal, Quebec H4N 2M3
T: +1 866-dormakaba (1-866-367-6252)

www.dormakaba.com

Copyright © dormakaba 2026
All rights reserved.

No part of this document may be reproduced or used in any form or by any means without prior written permission of dormakaba Canada .

All names and logos of third-party products and services are the property of their respective owners. MIFARE, MIFARE Classic, MIFARE Plus, MIFARE Ultralight, and MIFARE DESFire are registered trademarks of NXP B.V.

Subject to technical changes.

Table of contents

1 About this document	6
1.1 Validity	6
1.2 Target audience	6
1.3 Purpose and objective	6
1.4 Additional documents	6
2 Welcome	7
3 Security overview	8
3.1 Enhanced security mode	8
3.2 Physical security	8
3.2.1 Hardware selection	9
3.2.2 Installation / upgrades	9
3.3 Network security	9
3.3.1 Installation	9
3.3.2 Configuration	9
3.4 Application security	10
3.4.1 Data standards	10
3.4.2 Security features	10
3.4.3 Proprietary design decisions	11
3.5 User security	11
4 Requirements	12
4.1 System Requirements	12
4.2 Network Requirements	13
4.2.1 Deployment on Virtual Machine	13
4.2.2 Communication Ports	13
4.3 Device Requirements	13
4.3.1 RFID keys	14
4.3.2 Encoders	14
4.3.3 Maintenance Units	14
4.3.4 Locks	15
4.3.5 Elevator Controllers	16
4.3.6 Zigbee Gateways	17
4.4 SSO requirements	17
4.5 Interface Requirements	17
4.6 Online Communication Interfaces and Devices	17

4.7 Online Communication Lock Support	18
4.8 Third-party prerequisite components	18
5 Pre-installation checklist	20
5.1 Requirements	20
5.2 Recommendations	20
6 Prepare for using an existing SQL Server instance	21
6.1 Configure a Windows firewall for database engine access	24
7 Ambiance server installation	30
7.1 Choose Setup Language page	30
7.2 Welcome page	31
7.3 License Agreement page	32
7.4 Choose Destination Location page	33
7.5 IP Address / Server Name Selection page	34
7.6 Setup Type page	35
7.7 SQL Database Server page	36
7.8 Setup Status page	37
7.9 SSL Certificate Selection page	38
7.9.1 Choose SSL certificate	38
7.9.2 Password page	39
7.10 Installation Complete page	40
8 Ambiance client installation	41
8.1 Welcome page	42
8.2 License Agreement page	43
8.3 Choose Destination Location page	44
8.4 Setup Status page	45
8.5 Installation Complete page	46
9 Post-installation checklist	47
10 Ambiance upgrades	48
10.1 Pre-upgrade checklist	48
10.2 Upgrade process	48
10.3 Post-upgrade checklist	49
10.4 SQL Server upgrades	49
11 Getting started with Ambiance	50
11.1 Product activation	50
11.2 Site configuration workflow	51
11.3 Remember to ...	51

A Appendix A: Service Manager	52
A.1 Installing / renewing SSL certificate after installation	52
A.1.1 Server	52
A.1.2 Client	53
A.2 Changing server IP address	53
A.2.1 Server	54
A.2.2 Client	54
A.3 Restore online database	54
A.4 Disable/enabling Watchdog	55
B Appendix B: Polling service	56
C Appendix C: Database restore	57
C.1 Required preparatory steps	57
C.1.1 Install the Ambiance server on a reserve machine	57
C.1.2 Identify database backups	57
C.1.3 Copy backup files to the new server	57
C.1.4 Obtain and configure the dormakaba restore tool	58
C.2 Restore the SQL Server database	58
C.3 Restore the MongoDB database	61
C.4 Static IP address only. Update IP address	66
C.5 Ambiance with polling feature only. Additional configurations	66
C.6 Update Ambiance workstations	66
C.7 Ambiance only. Update PMS server	66

1 About this document

1.1 Validity

This document describes the product:

Product designation:	Ambiance
Version:	2.15.0

1.2 Target audience

This document is for IT specialists responsible for all tasks related to installing the Ambiance Server and Ambiance Client.

1.3 Purpose and objective

The purpose of this document is to provide information and instructions to support all tasks related to installing Ambiance. The document lists requirements and includes pre-installation and post-installation checklists for fresh installs and upgrades.

1.4 Additional documents

Ambiance User Guide 2.15.0 (PK3722-EN)

Ambiance Release Notes 2.15.0 (PK3702)

Ambiance Enhanced Key Security for Upgrades 2.15.0 (PK3777)

2 Welcome

Ambiance® is the leading-edge access management software for the hospitality industry. Developed for security and designed for users, the application streamlines access control management and integrates seamlessly into any hotel IT infrastructure. Ambiance provides an efficient and user-friendly method to establish and manage multisite property access .

Flexible configuration and integration options showcase a robust feature set. Guided workflows simplify property configuration, staff management, key issuance, and guest registration. Configurable user permissions secure system access. Lock and system data collection supports detailed access point audits and reporting. Remote lock management provides immediate and convenient control of access points. An extensive library of web services and APIs are available for third-party integrations. Ambiance also supports market-demand technologies including Bluetooth® and enhanced key security.

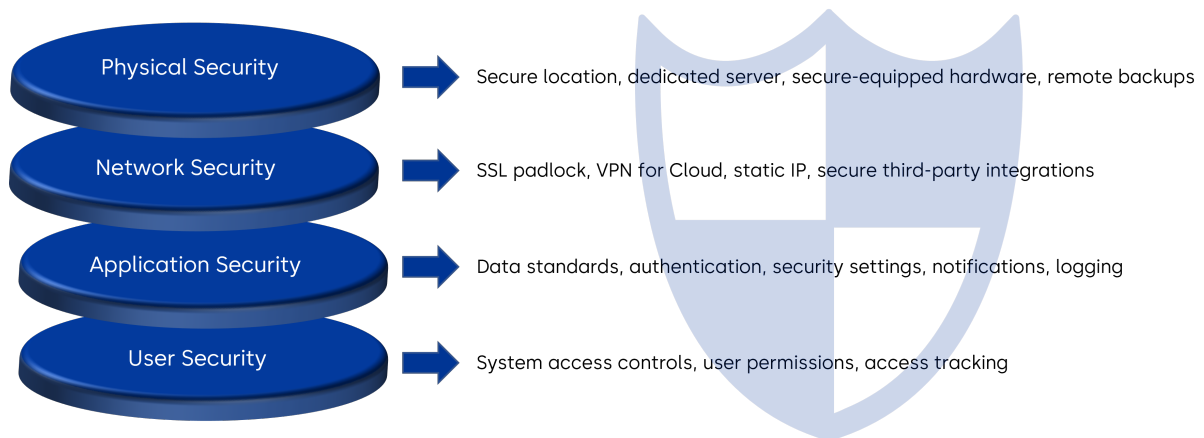
The browser-based Ambiance Client provides system access 24/7 from any device on the property network.

3 Security overview

As a leader in the access control industry, dormakaba recognizes the continuously evolving nature of security technology. We strive to make ongoing improvements in our products, and we encourage our customers to implement enhanced authentication and encryption protocols. Moreover, dormakaba recommends configuring security-related options available in Ambiance and adopting standard best practices.

This chapter presents security-related options and best practices based on the relevant layer of security. Enhanced security mode is prioritized as the principal and strongest recommendation to ensure end-to-end security.

Ambiance Enhanced Security Mode



3.1 Enhanced security mode

Enabling enhanced security mode introduces an additional layer of security for protecting data on RFID keys. The technological shift increases the integrity of the entire access management system. With enhanced key security:

- All keys include enhanced security.
- Data encoded on keys is protected using global encryption standards.
- Encoders support advanced encryption standards.
- Lock programming is protected with stronger encryption and authentication.
- Locks are programmed to accept only high-security keys.

Enhanced key security requires devices that are compliant with advanced encryption standards and authentication protocols. Locks, encoders, Maintenance Units, RFID keys and elevator controllers must meet minimum requirements. For details, refer to the relevant sections in [Device requirements](#).

Implementing enhanced key security involves establishing device requirements and enabling Enhanced security mode in System Settings. For new installations, security mode is enabled by default and all devices are preconfigured to meet requirements. For upgrades, security mode is disabled by default and requires preparation and manual steps to enable. Lastly, some sites may need to upgrade yet delay using enhanced key security.

In all cases except new installations that proceed with security mode enabled, refer to the document *Ambiance Enhanced Key Security for Upgrades* accessible at the root of the software download folder. The document describes options and provides step-by-step instructions for enabling enhanced security mode. The document also contains important information for sites that upgrade without enhanced key security.

3.2 Physical security

Physical security is the foundation upon which all additional layers of security depend.

3.2.1 Hardware selection

When planning an initial deployment or upgrade, use hardware that supports enhanced security:

- **Server**—A dedicated server is required for Ambiance.
- **Locks**—All lock profiles in Ambiance support enhanced security except RT and Confidant.
- **M-Units**—(Maintenance Units) Use only type M-Unit Saflok HH6 NFC. Required for enhanced security mode.
- **Encoders**—Use only type dormakaba RFID Encoder II, part number 75720. Required for enhanced security mode.
- **RFID keys**—Please be advised that many access cards utilized in RFID systems have become susceptible to cloning and related attacks over the years. Notably, certain legacy card technology has been the subject of published vulnerability reports.. dormakaba recommends using credentials utilizing MIFARE Ultralight AES to provide an additional layer of security for the installed version of Ambiance.
 - For guest credentials—Select the more secure credentials MIFARE Ultralight AES which have security features that offer additional protection against cloning.
 - For staff credentials—Our recommendation is to also use Ultralight AES. This will offer an additional layer of security for the access management software presently installed at your property. Our implementation of the MIFARE Plus credential was designed to provide compatibility with legacy solutions, specifically MIFARE Classic. As a result, for this particular application MIFARE Plus will not provide the same level of security as Ultralight AES.

3.2.2 Installation / upgrades

- Install the Ambiance server in a secure physical location.
- dormakaba strongly recommends scheduling automated backups to a remote server and storing backup and archival data in a secure location off-site. Requirements apply to back up to a remote server. For upgrades, take a backup of the database before performing the upgrade. For online systems, take backups of Ambiance SQL Server and MongoDB databases. See System Settings > Database Backup.

3.3 Network security

Prior to deployment, a dormakaba technician works with site IT to discuss network requirements. Review the following best practices and security-related options.

3.3.1 Installation

- Prior to starting the installation, verify that all Windows updates are installed.
- Configure the Ambiance server with a static IP address.
- dormakaba strongly recommends installing an SSL certificate to enable the HTTPS protocol. The SSL certificate to enable HTTPS mode must be provided by a well-known and trusted certificate authority. If you opt to install an SSL certificate post-installation, use the Service Manager for a streamlined transition.
- 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.
- Versioning controls dictate that Ambiance workstations are required to be at the same version as the Ambiance server to program locks and encode/read keys.

3.3.2 Configuration

- **Communication ports**—Default secure ports are listed in product release notes. When necessary, consult a dormakaba technician for customizing ports. See [Communication ports](#).
- **HTTPS Browser Certificate**—When Ambiance is deployed with an SSL certificate, specify the number of days before the certificate expires to start receiving a daily warning. See System Settings > Security > HTTPS Browser Certificate.
- **Secure email notifications**—When SSL is enabled and security certificates are valid, all email data sent from the email server to mail clients is private and secure. See System Settings > Email Configuration.
- **Integrations**—Integrate only with third-party applications that support secure communication. See [Communication ports](#) and obtain integration documentation from dormakaba Customer Service.

3.4 Application security

Ambiance supports industry data standards and recommends taking advantage of security-related options. See also [Proprietary design decisions](#).

3.4.1 Data standards

- **PCI-DSS**—Select whether to enable PCI-DSS (Payment Card Industry Data Security Standard), an information security standard for organizations that handle credit cards. Recommended value: YES. When you enable PCI-DSS, the Enable security questions option in Password Reset is set to YES and cannot be disabled.
- **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.

3.4.2 Security features

- **Enhanced security mode**—This setting enables enhanced encryption for encoding data on keys. Default: YES for fresh installations, NO for upgrades. See System Settings > Security > Enhanced Security Mode.
- **Single Sign-On**—This licensed option is disabled by default. SSO centralizes authentication enabling organizations to implement stronger security controls.
- **Staff key validation**—This licensed option reinforces access control by validating staff keys daily.
- **RFID key types**—dormakaba recommends enabling enhanced security mode which supports MIFARE Ultralight AES (recommended), MIFARE Ultralight C, and MIFARE Plus. When enhanced security mode is not enabled, dormakaba recommends MIFARE Ultralight C (Standard Security). See System Settings > Advanced > RFID key types.
- **Device security**—This setting is enabled by default for new installations. Service-side and client-side SSL certificates secure communication for encoders, gateway II devices, and MFC devices. For upgrades, the certificates need to be manually activated.
- **M-Unit authentication**—Select whether to require M-Unit authentication. When authentication is enabled, M-Unit credentials are required to program and audit locks. When authentication is enabled, M-Unit credentials must be configured in Staff Management for at least one operator. Required for enhanced security mode. See System Settings > Security > Maintenance Unit.
- **M-Unit security code**—When enhanced security mode is enabled, a security code is required to program locks with the M-Unit. See System Settings > Security > Enhanced Security Mode.
- **PMS authentication**—Select whether to require authentication for PMS requests. When authentication is enabled, PMS credentials must be configured in Staff Management for at least one operator. See System Settings > Security > PMS.
- **Lock access**—Review settings for [Escape return](#), [Quick relatch](#), and [Disability mode](#) to fine-tune lock access after a door opens. See System Settings > Security > Lock Access.
- **Data security**—dormakaba strongly recommends scheduling automated backups to a remote server and storing backup and archival data in a secure location off-site. Requirements apply to back up to a remote server. See System Settings > Database Backup.
- **Data privacy**—In compliance with the GDPR (General Data Protection Regulation), dormakaba encrypts all PII (Personally Identifiable Information) with a site- specific symmetric key.
- **PPK/SPK**—Primary and secondary programming keys can be made in advance in System Keys to prepare for disaster recovery. The PPK is essential to recover from database corruption or total loss.
- **Failsafe keys**—Failsafe Keys are backups of individual guest room keys that are made in advance and maintained in complete sets to be issued in the event of a system or power failure. See System Settings > Failsafe Keys.
- **Staff/System keys**—Always specify a key holder when making staff and system keys. Although it is not required, identifying the key holder is useful for tracking and accountability. See Staff Keys and System Keys.
- **Invalidate access** when appropriate:
 - Use the Block and Deactivate functions in Staff Management to restrict operator access when necessary. See Staff Management.
 - Use the System Keys at locks to invalidate staff and guest access. See System Keys.
 - Use the Erase key function (from Read Key dialog) to invalidate keys. See the Ambiance toolbar.
- **Access tracking**—Staff and guest access tracking reports can be generated from the Read Key dialog.

- **Notifications**—Configure notification groups, then assign subscriptions for staff members in Staff Management. See Notifications and Staff Management.
- **Logging**—Extensive logging is produced to facilitate troubleshooting.
- **Firmware upgrades**—Establish a schedule to upgrade devices with the latest supported firmware.
- **Reports**—Establish a schedule to run and review Ambiance reports. See Reports.

3.4.3 Proprietary design decisions

A security-focused approach to site configuration involves detailed planning.

- **Property Builder**—Thoughtfully plan, create and maintain access points. Establish standards for creating restricted area and foyer door access point types, and when selecting the limited access option for guest and staff common areas. See Property Builder.
- **Access Management**—Thoughtfully plan, create and maintain access management controls utilizing schedules, credentials, and common area access. See Access Management.
 - **Credentials**—Carefully configure all credentials paying particular attention to Connector credentials, which is a guest-level credential class that associates guest room access point types. If the guest rooms are associated with a foyer group, then the Connector class is implicitly applied to the foyer group.
 - **Emergency Keys**—When necessary, obtain a license for Emergency Keys. Only Emergency keys *always* override a projected dead bolt or active privacy switch.

3.5 User security

System access controls include the following options and best practices:

- **Password, login, and account settings**—Customize global settings to prevent unauthorized operator access. See System Settings > Security.
- **Single Sign-On**—This licensed option is disabled by default. SSO simplifies access for users and minimizes credential maintenance.
- **Role Management**—Operator roles determine the level of access to Ambiance features and functions. Thoughtfully plan and assign operator roles. When necessary, create custom roles. See Role Management.
- **Staff Management**—Staff profiles are designed to store details about all staff. Specify all available details on the **Staff Info** tab. For operators, create PMS operator credentials on the **Operator Info** tab. The credentials are validated when M-Unit and PMS authentication are enabled. See Staff Management.
- **Default Admin account**—After installation, log in to the default Admin01 account to change the default password. Create strong passwords using at least eight characters that include uppercase and lowercase letters, numbers, and special characters.

4 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.

4.1 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/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 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	8.0.25.26112	8.0.25.26112	8.0.25.26112	not applicable
Database ⁶	- SQL Server Express 2022/2019/2017 - SQL Server 2022/2019/2016			
Web Browser ⁷	- 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 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 TPM (Trusted Platform Module) 2.0 is required to run Windows 11.

⁶ 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. 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.

4.2 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.

4.2.1 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.

4.2.2 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.



Although Ambiance requires a dedicated server, use the following port ranges for third-party monitoring and scanning: 10000-14999 and 30000-39000.



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

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)
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	Ambiance 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>

4.3 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.

4.3.1 RFID keys

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

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

4.3.2 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 Ultralight C MIFARE Plus
dormakaba RFID ENCODER II (part 75720) (required when Enhanced Security Mode enabled)	3.003 Applet version: 1.003	MIFARE Ultralight AES MIFARE DESFire EV2/EV3 MIFARE Ultralight C MIFARE Plus



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

4.3.3 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

4.3.4 Locks

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

Lock profile	Boot & Main	Supported readers	Supported key types	BLE	Zigbee AVR
Use with Enhanced, Standard and Legacy security					
Confidant NFC	03.09.26.4	Integrated reader	Apple Wallet, Google Wallet, BLE MIFARE Ultralight AES MIFARE DESFire EV2/EV3 MIFARE Ultralight C MIFARE Plus	2.0.1.0	1.10x, 5.13x, 6.05x
MT4/Quantum (secure boot)	07.22.25.4	Quantum (secure boot): 08.12.25.5	BLE MIFARE Ultralight C MIFARE Plus	1.3.1.0	1.10x, 5.13x, 6.05x
Quantum MT6 (secure boot)	11.13.25.04	LEGIC	Apple Wallet, Google Wallet, BLE MIFARE Ultralight AES MIFARE DESFire EV2/EV3 MIFARE Ultralight C MIFARE Plus	4.0.0.0	1.10x, 5.13x, 6.05x
Pixel +	11.13.25.04	LEGIC	Apple Wallet, Google Wallet, BLE MIFARE Ultralight AES MIFARE DESFire EV2/EV3 MIFARE Ultralight C MIFARE Plus	4.0.0.0	1.10x, 5.13x, 6.05x
Pixel	07.22.25.4	Quantum (secure boot): 08.12.25.5	BLE MIFARE Ultralight C MIFARE Plus	1.3.1.0	1.10x, 5.13x, 6.05x
RAC5 XT/Lite (hardware for common areas)	08.12.25.4 (Main only)	NFC Wall Reader: 11.19.25.3	Apple Wallet, Google Wallet, BLE MIFARE Ultralight AES MIFARE DESFire EV2/EV3 MIFARE Ultralight C MIFARE Plus	2.0.1.0	N/A
RCU	07.22.25.4	SR Wall Reader: 07.22.25.3	Apple Wallet, Google Wallet, BLE MIFARE Ultralight AES MIFARE DESFire EV2/EV3 MIFARE Ultralight C MIFARE Plus	1.3.1.0	1.10x, 5.13x, 6.05x
RT+	03.09.26.4	Integrated reader	Apple Wallet, Google Wallet, BLE MIFARE Ultralight AES MIFARE DESFire EV2/EV3 MIFARE Ultralight C MIFARE Plus	2.0.1.0	1.10x, 5.13x, 6.05x
Saffire LX	03.09.26.4	Integrated reader	Apple Wallet, Google Wallet, BLE MIFARE Ultralight AES MIFARE DESFire EV2/EV3 MIFARE Ultralight C MIFARE Plus	2.0.1.0	5.13x/ 6.05x

Lock profile	Boot & Main	Supported readers	Supported key types	BLE	Zigbee AVR
SRK (Secure Reader Keyscan)	09.19.25.3	LEGIC	Apple Wallet, Google Wallet, BLE MIFARE Ultralight AES MIFARE DESFire EV2/EV3 MIFARE Ultralight C MIFARE Plus	2.0.1.0	1.10x, 5.13x, 6.05x
Use with Standard and Legacy security					
Confidant	09.03.19.2	Integrated reader	BLE MIFARE Ultralight C MIFARE Plus	1.3.1.0	1.10x/ 5.13x
MT4/Quantum	10.11.19.2	Quantum (secure boot): 09.17.16.1	BLE MIFARE Ultralight C MIFARE Plus	1.3.1.0	1.10x, 5.13x, 6.05x
RT	06.14.18.2	Integrated reader	BLE MIFARE Ultralight C MIFARE Plus	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.

4.3.5 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	BLE MIFARE Ultralight C MIFARE Plus	1.3.1.0	1.10x
RAC5-MFC	08.12.25.4	NFC Wall Reader: 11.19.25.3	Apple Wallet, Google Wallet, BLE MIFARE Ultralight AES MIFARE DESFire EV2/EV3 MIFARE Ultralight C MIFARE Plus	2.0.1.0	N/A
Standard and Legacy security					
ECU/RCU4	10.11.19.2	Quantum (secure boot): 09.17.16.1	BLE MIFARE Ultralight C MIFARE Plus	1.3.1.0	1.10x
Legacy MFC	0.017 (Main only)	Integrated reader	BLE MIFARE Ultralight C MIFARE Plus	1.3.1.0	N/A
EMCC	20090929 (Main only)	Integrated reader	BLE MIFARE Ultralight C MIFARE Plus	1.3.1.0	N/A
MCC 8/12	0.031398 (Main only)	Integrated reader	BLE MIFARE Ultralight C MIFARE Plus	1.3.1.0	N/A

4.3.6 Zigbee Gateways

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

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

4.4 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 example, 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.

4.5 Interface Requirements

Ambiance supports the following:

- [MATRIX](#)—v4.1.2
- [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 Ambiance system user created in Aurora, per the Aurora Integration Manual. Other User Types will no longer work with Ambiance 2.15.0.

4.6 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)				

	Gateway I Device supported with	Gateway II Device supported with	Rx-Link supported with	RAC5-MFC/XT supported with
INNCOM	✓	✓	✓	✓
INTEREL	✓	Not Supported	Not Supported	Not Supported
Telkonet	Not Supported	Not Supported	✓	Not Supported
Control4	✓	Not Supported	Not Supported	Not Supported

4.7 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	✓	✓	✓
Confidant	✓	✓	Not Supported
Confidant NFC	✓	✓	✓

4.8 Third-party prerequisite components

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

Third-Party Software	Version
Microsoft .NET Framework	4.8.1 Full
Microsoft .NET Desktop Runtime	8.0.25.26112
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	4.2.5
Erlang	27.3.4.9
Microsoft SQL Server Express (if selected)	2022 16.0.4215.2
SQL Server kumulative Updates	KB5080999
Redis on Windows	3.2.100

MongoDB	8.2.6 2008R2Plus SSL x64
Mongosh	2.8.2
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

5 Pre-installation checklist

The following items apply to initial installations only.

5.1 Requirements

1	☐	Server/Client. Verify that all applicable requirements are met.
2	☐	Server. Verify that the Date/Time and Time Zone settings are correct. (The Ambiance Server and the locks installed at access points must be configured for the same time zone.)
3	☐	IMPORTANT! Server/Client. Verify that all Windows updates are installed.
4	☐	Server. Verify that Windows PowerShell 4.0 is installed.
5	☐	Server. Verify that the following programs are NOT installed:
6	☐	SQL Server (only if not connecting to an existing SQL instance)
7	☐	Redis
8	☐	RabbitMQ
9	☐	Web Server IIS
10	☐	Server. Verify that you have an activation key for Ambiance 2.15.0.
11	☐	Disable Windows USB power saving settings (to ensure encoders connected via USB function properly).
12	☐	Remove or disable the Windows Sync Share service. The feature uses ports in conflict with Ambiance.
13	☐	Server/Client. Verify that the operating system is up and activated.
14	☐	Server/Client. Perform the installation as a Local Administrator .
15	☐	If applicable, prepare to connect to an existing SQL Server instance .
16	☐	Server. Make sure antivirus software is disabled before proceeding with server installation.
17	☐	Server. If the language used for the user interface is different from the server operating system language, it is required to install the Microsoft Windows language pack matching the user interface language for Ambiance reports to display the appropriate information.
18	☐	Verify that the storage media where SQL Server will be installed is does not exceed a sector size of 4096 bytes. Drives with larger sector sizes are not supported and will cause installation failure.

5.2 Recommendations

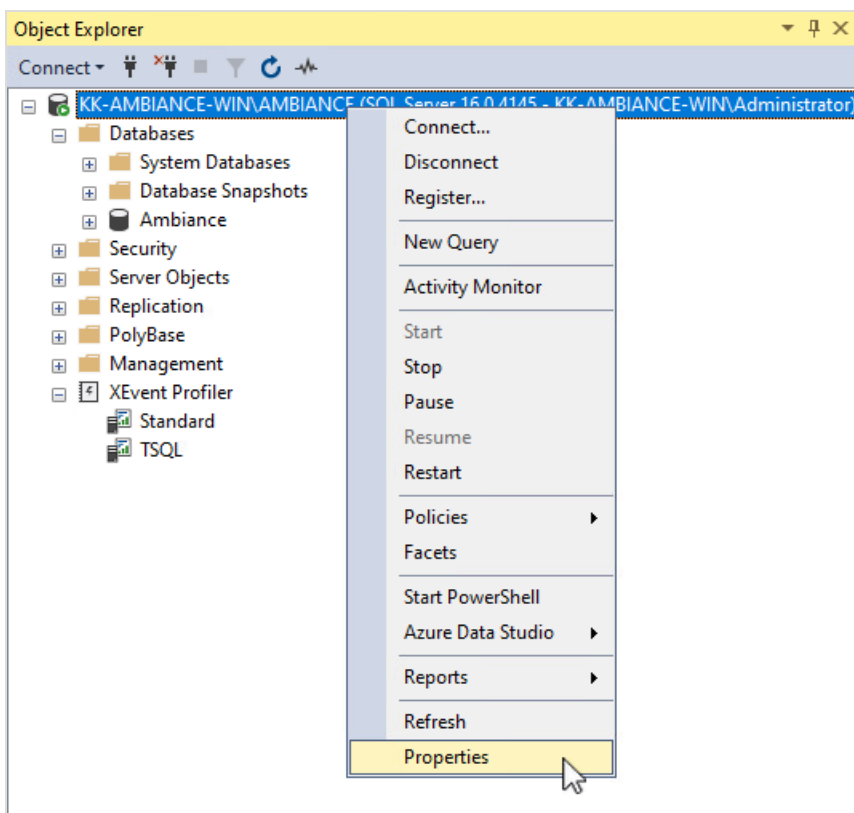
1	☐	IMPORTANT! Install the Ambiance Server in a secure physical location.
2	☐	IMPORTANT! Ensure that the edition of SQL Server meets organizational requirements.
3	☐	Server. If deploying on a cloud VM, set up a VPN to secure the communication between the site and cloud VM.
4	☐	Server. Verify that the server where SQL Server is installed is not a Domain Controller.
5	☐	Server. If possible, disable Windows Defender for the duration of the installation.
6	☐	Server. Configure the Ambiance Server with a static IP address.
7	☐	Make sure that you have your Windows OS Installer available.

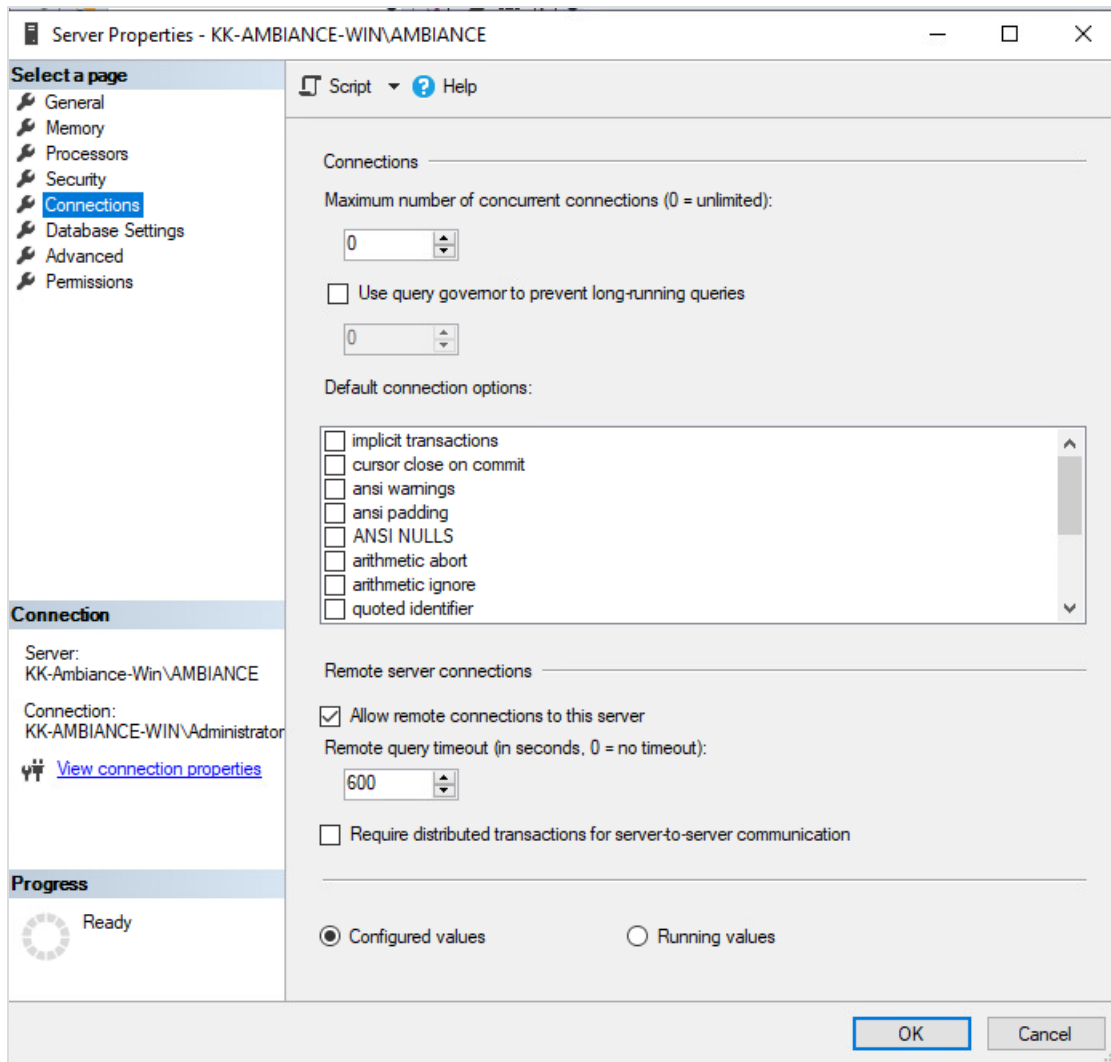
6 Prepare for using an existing SQL Server instance

If you plan to connect to an existing SQL Server database (local or remote), you must prepare before starting the installation.

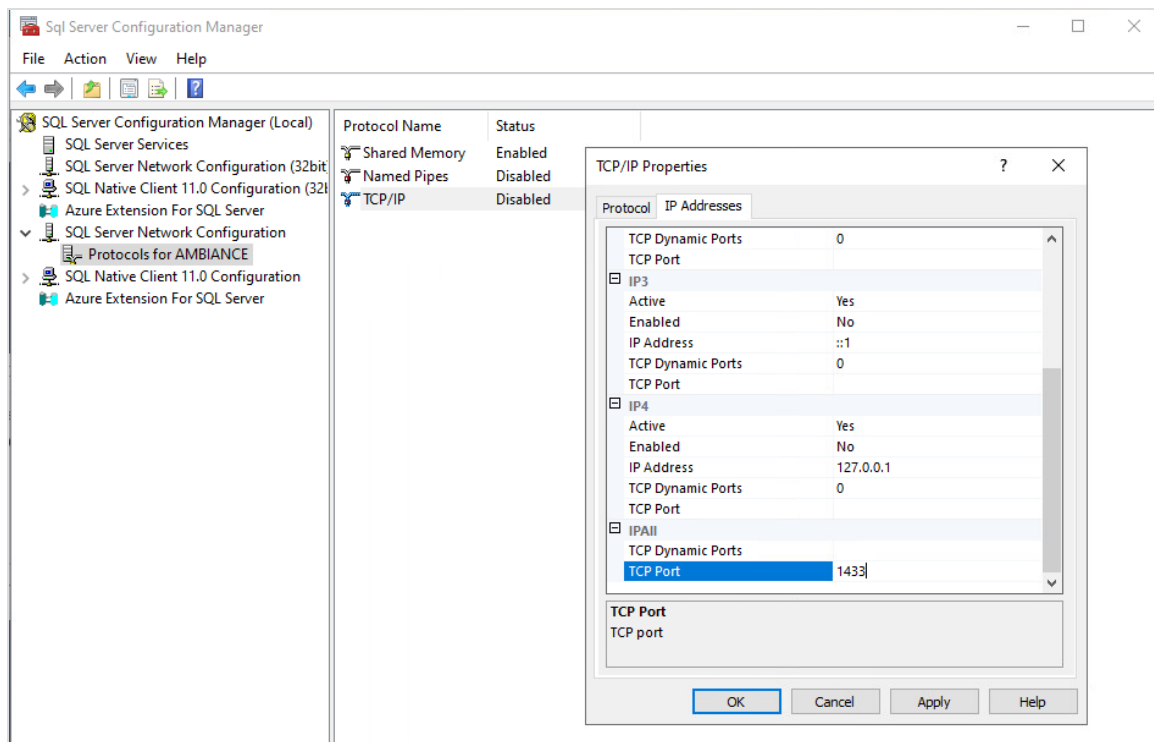
1. In the Ambiance installation package, go to the [AMBIANCE_PREREQUIS](#) folder and copy the master database file (Ambiance.mdf) to the remote computer where Microsoft SQL Server is installed. Recommended path: C:\Program Files\Microsoft SQL Server\MSSQL $version.instanceName$ \MSSQL\DATA\.
2. Right-click the database file and select **Properties**. Deselect the [Read-Only](#) attribute, then click **Apply > OK**.
3. Attach the database:
 - a. Open SQL Server Management Studio.
 - b. Connect to an instance of the SQL Server Database Engine.
 - c. In Object Explorer, expand the instance view.
 - d. Right-click **Databases** and select **Attach**.
 - e. In the Attach Databases dialog box, click **Add**.
 - f. In the Locate Database Files dialog box, navigate to and select the .mdf file (previously pasted in step 1).
 - g. Click **OK**.

4. Right-click the server and select **Properties**.





5. For **Connections**, select the **Allow remote connections to this server**, then click **OK**.
6. Open the SQL Server Configuration Manager.
7. Navigate to SQL Server Network Configuration > Protocols for instanceName (AMBIANCE).



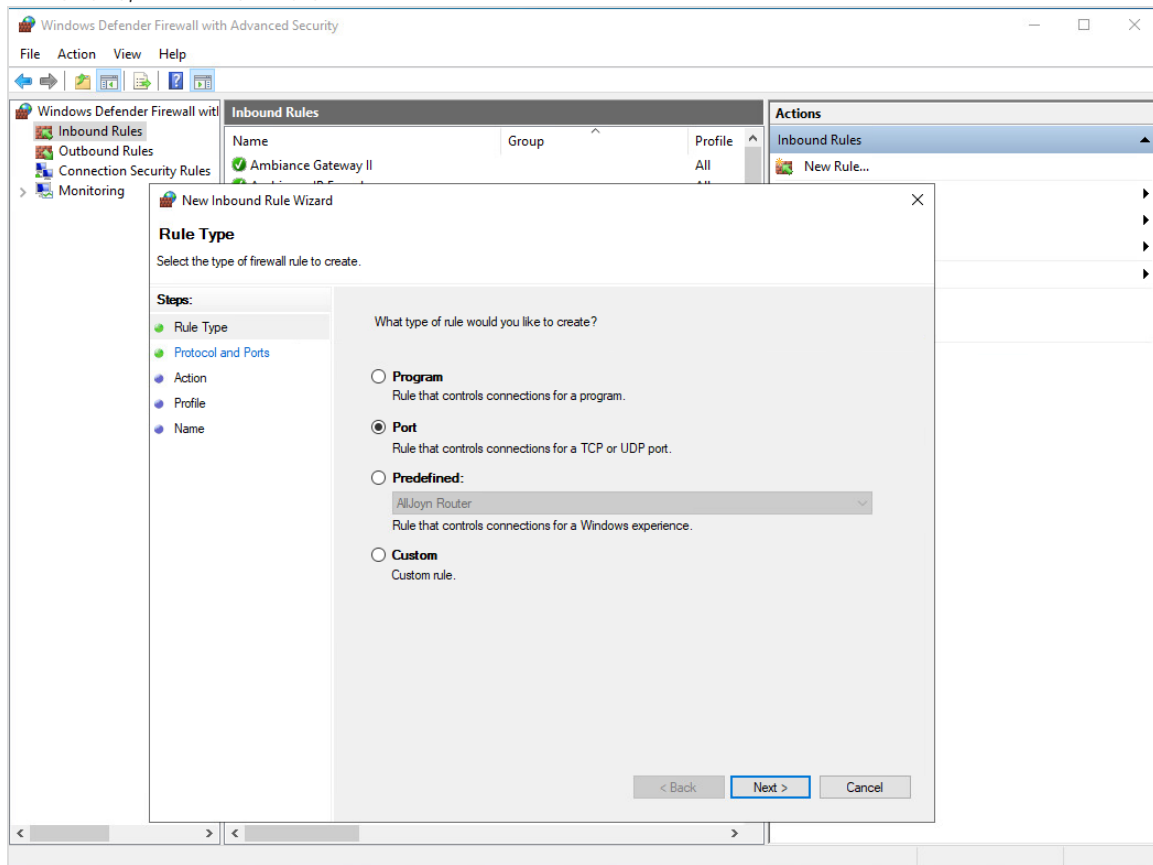
8. Right-click **TCP/IP** and select **Properties**.
9. In the TCP/IP Properties dialog, select the **IP Addresses** tab and scroll to **IPAll**.
10. Set the **TCP Dynamic Ports** to blank and **TCP Port** to **1433**. (Port 1433 is the default instance that SQL Server uses.)
11. Click **Apply** > **OK**.

If using a firewall, continue to the next section to open access for the database engine.

6.1 Configure a Windows firewall for database engine access

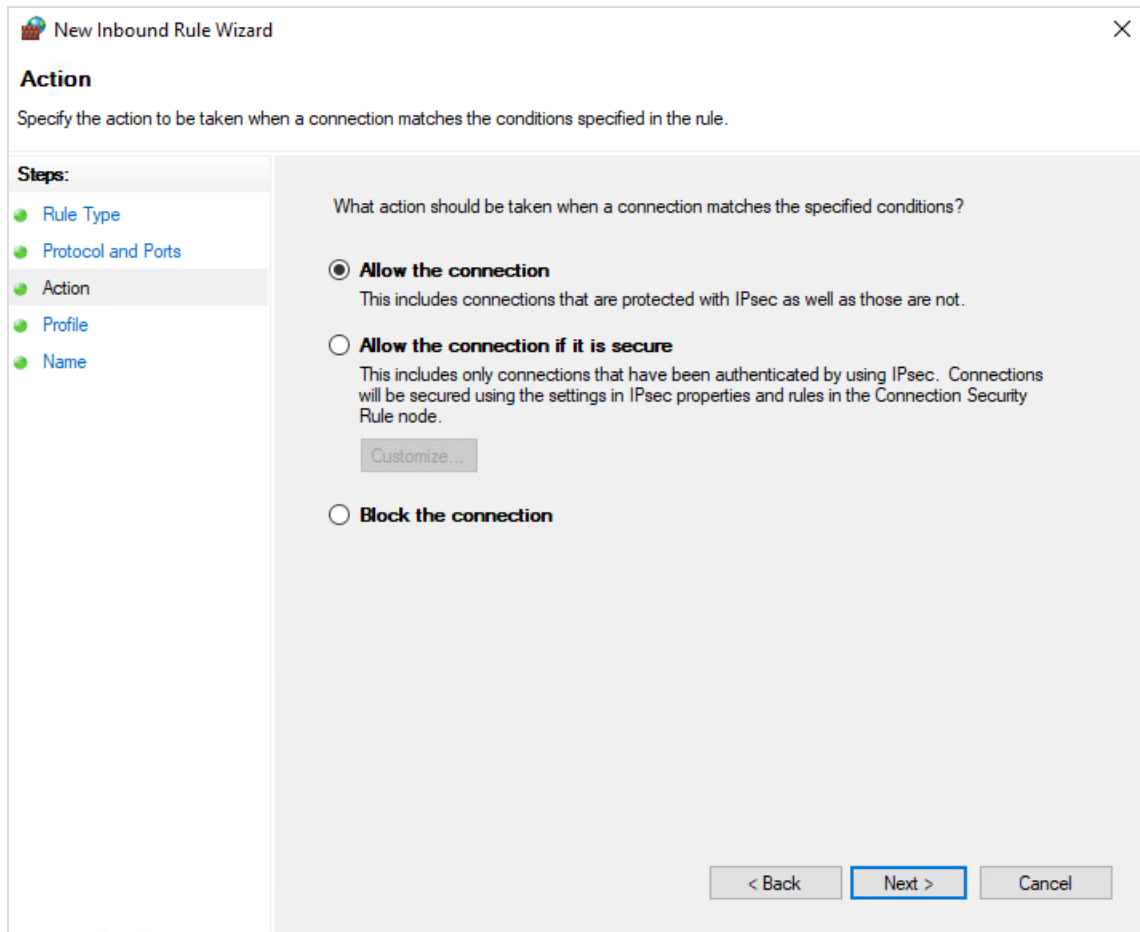
If the firewall is turned on, you need to add an exception for the 1433 port to allow TCP/IP traffic on Port 1433 and UDP traffic on Port 1434.

1. In the Windows Search bar, search for and open Administrative Tools.
2. Open Windows Defender Firewall with Advanced Security.
3. Select **Inbound Rules**.

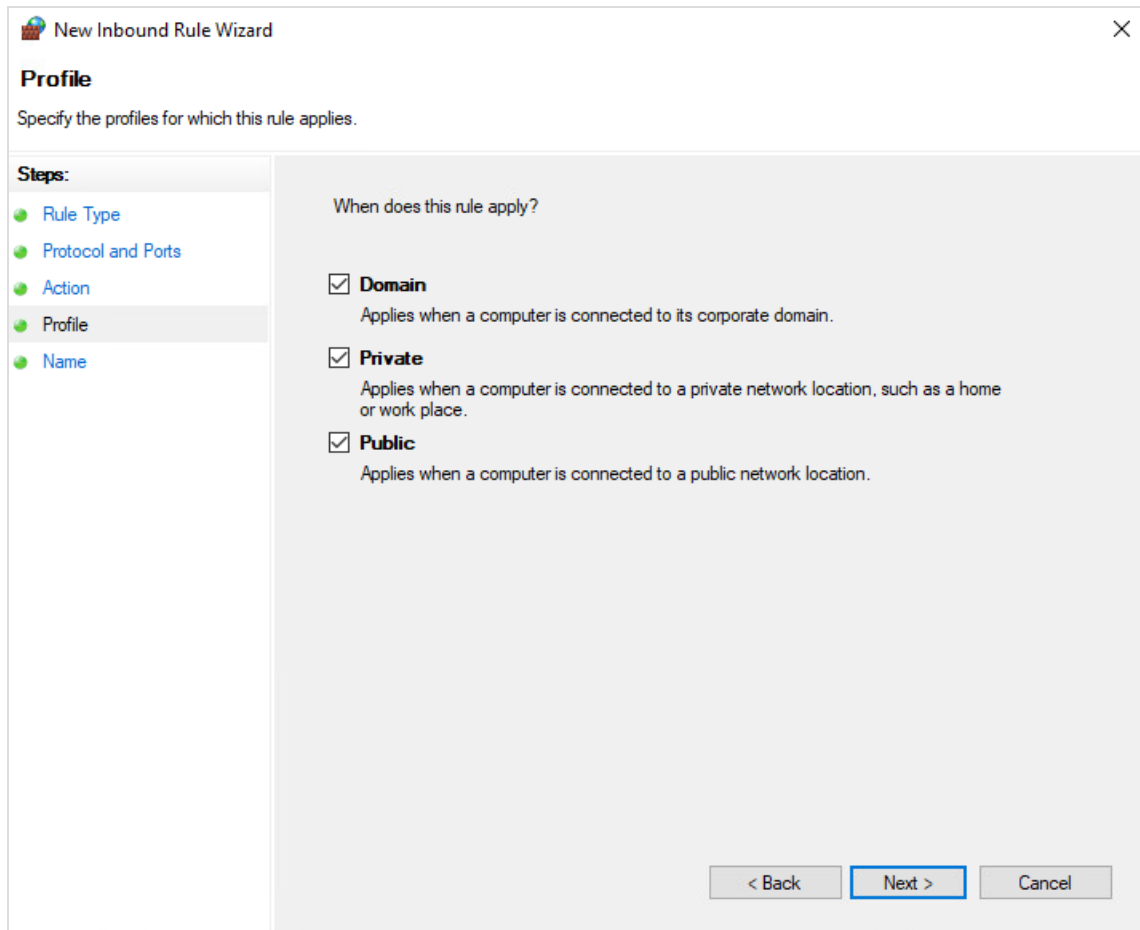
4. Under **Actions**, select **New Rule**.5. For Rule Type, select **Port**, then click **Next**.6. For Protocols and Ports, select **TCP** and specify **1433** for **Specific local ports**, then click **Next**.

The screenshot shows the 'New Inbound Rule Wizard' window, specifically the 'Protocol and Ports' step. The window title is 'New Inbound Rule Wizard'. The subtitle is 'Protocol and Ports'. Below the subtitle, it says 'Specify the protocols and ports to which this rule applies.' On the left, there is a 'Steps:' list with five items: 'Rule Type', 'Protocol and Ports' (which is highlighted), 'Action', 'Profile', and 'Name'. The main area of the wizard contains two questions. The first question is 'Does this rule apply to TCP or UDP?' with two radio button options: 'TCP' (which is selected) and 'UDP'. The second question is 'Does this rule apply to all local ports or specific local ports?' with two radio button options: 'All local ports' and 'Specific local ports:' (which is selected). Below the 'Specific local ports:' option, there is a text input field containing the value '1433'. Below the input field, there is a small text example: 'Example: 80, 443, 5000-5010'. At the bottom right of the wizard, there are three buttons: '< Back', 'Next >' (which is highlighted with a blue border), and 'Cancel'.

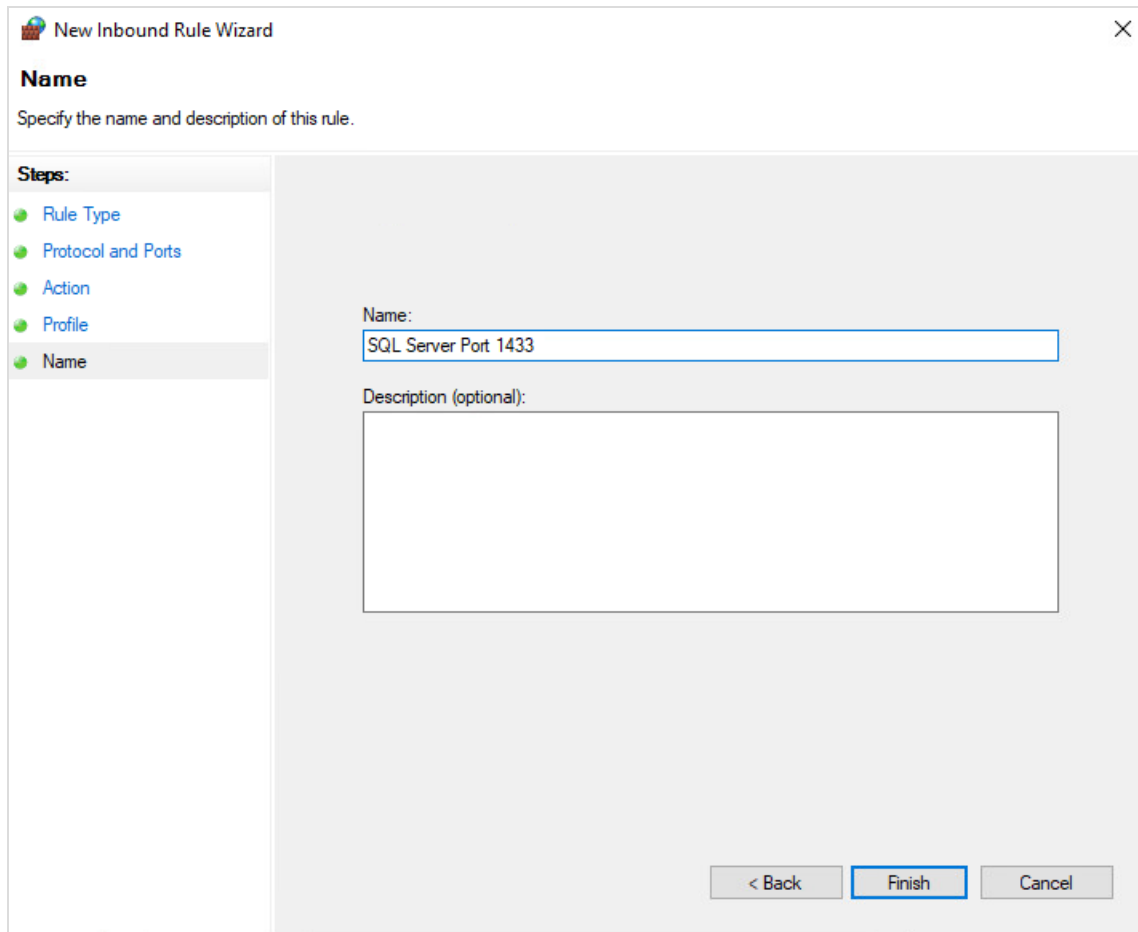
7. For Action, select **Allow the connection** (to specify the action to be taken when a connection matches the conditions specified in the rule).



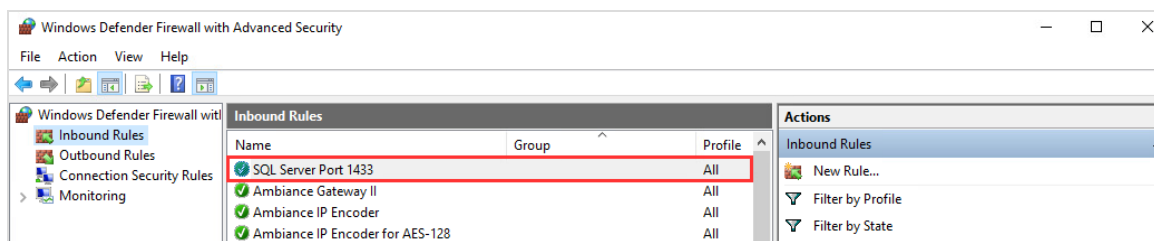
8. For Profiles, select the profiles to which the rule applies, then click **Next**.



9. For Name, specify the name of the new rule, then click **Finish**.



You can now see the created rule in the list of inbound rules.



10. Repeat the same steps to add UDP port 1434.

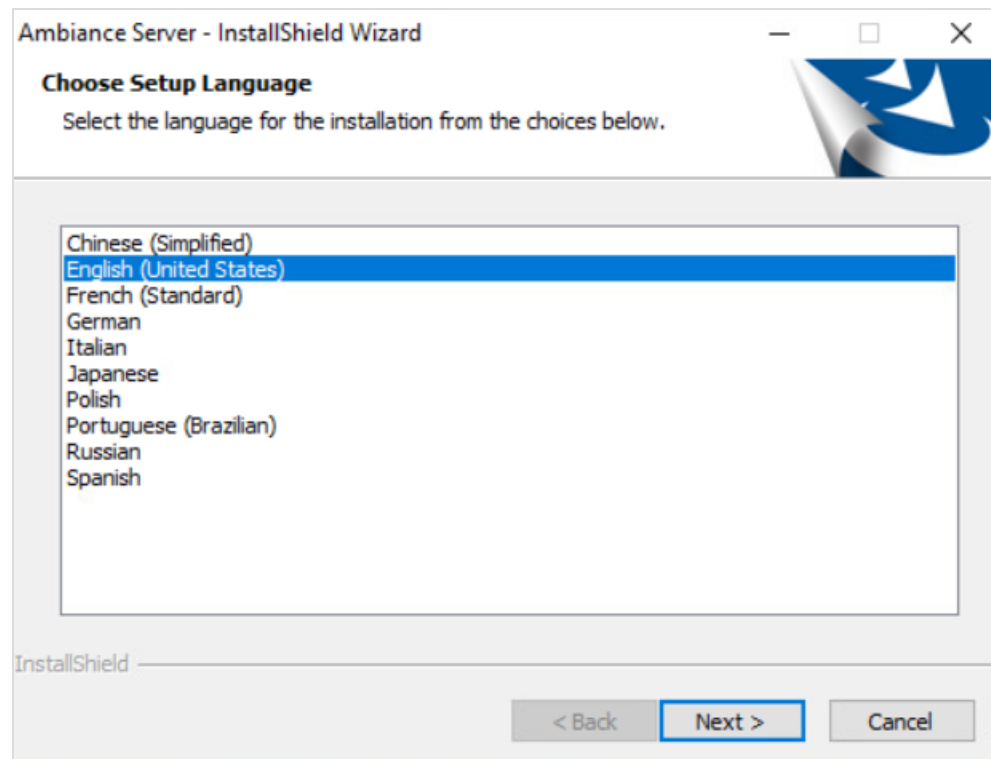
7 Ambiance server installation

This chapter is for first-time installations. If the installation is an upgrade, refer to *Ambiance Upgrades*.

To install the Ambiance Server:

1. In the dormakaba/Ambiance folder, open the SERVER folder.
2. Double-click **AmbianceServer.exe**. The installation wizard opens and prepares for setup. Depending on the server, you may be prompted to install third-party prerequisite components.
3. Follow the instructions for each of the following wizard pages. When a restart is required, confirm to proceed with the installation.

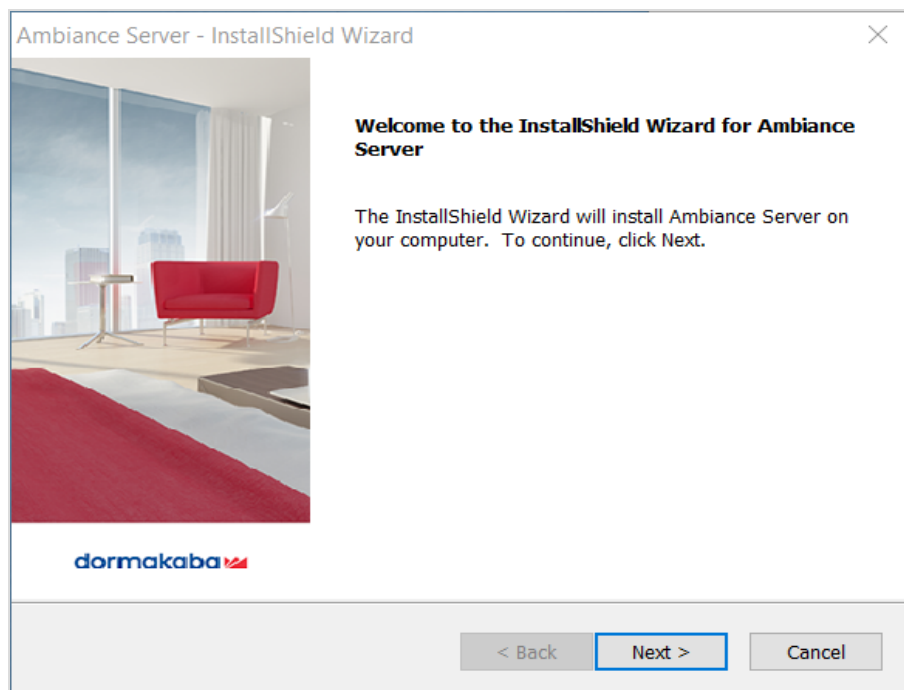
7.1 Choose Setup Language page



On the Choose Setup Language page:

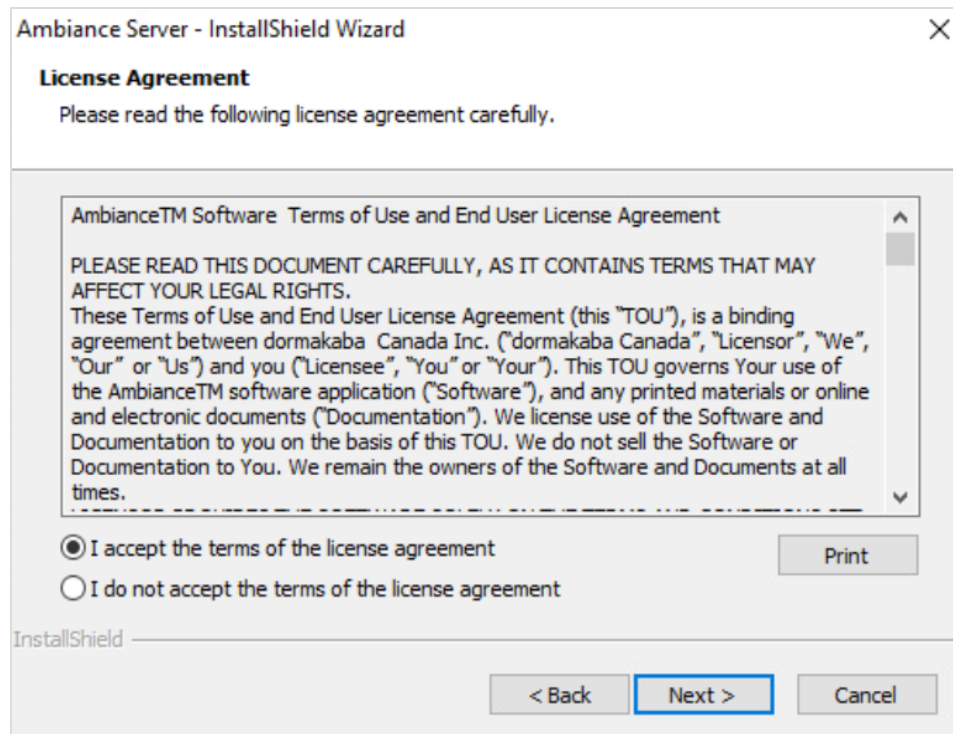
1. Select **English (United States)**.
2. Click **Next**.

7.2 Welcome page



On the Welcome page click **Next**.

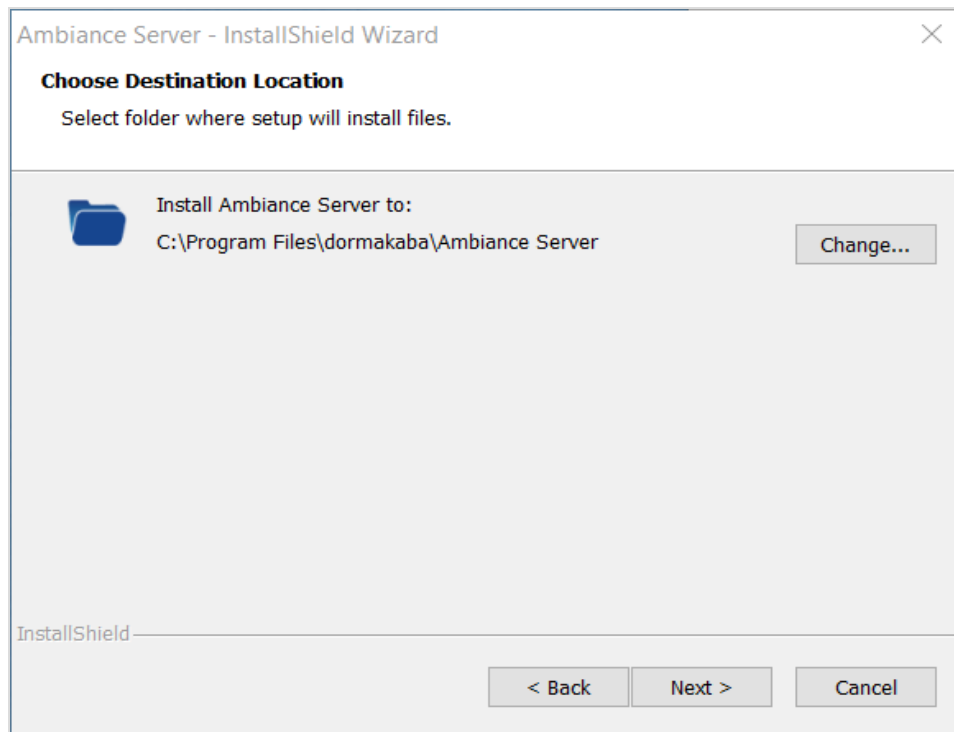
7.3 License Agreement page



On the License Agreement page:

1. Accept the terms of the license agreement.
You can optionally print the agreement.
2. Click **Next**.

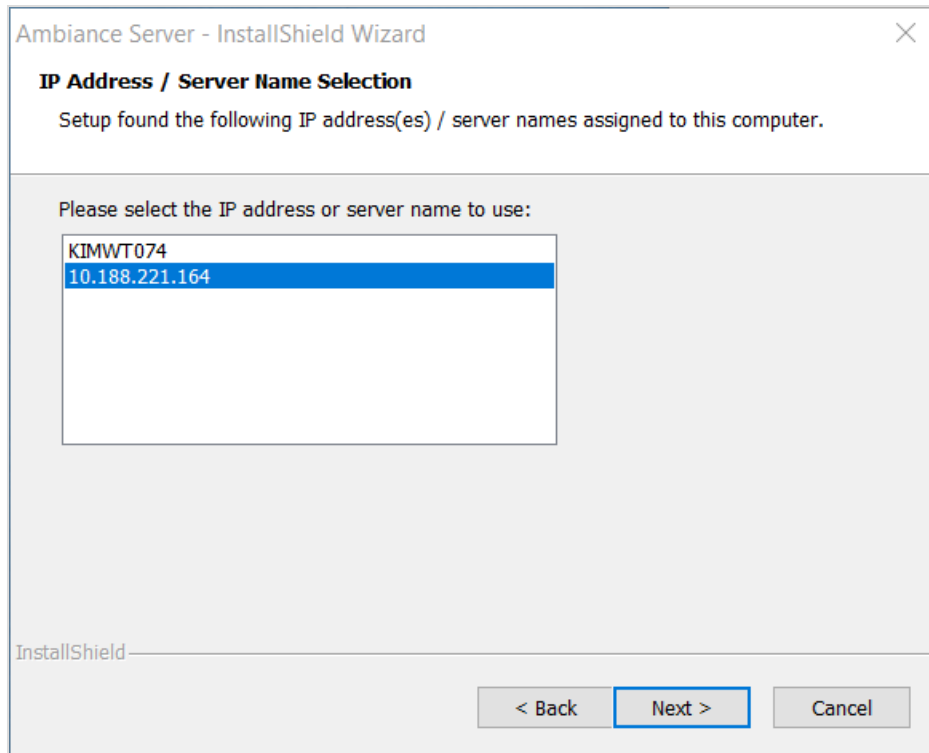
7.4 Choose Destination Location page



On the Choose Destination Location page:

1. Choose where to install Ambiance Server files:
 - Accept the default location (recommended).
 - Click **Change** and navigate to a location on the server.
2. Click **Next**.

7.5 IP Address / Server Name Selection page



On the IP Address / Server Name Selection page:

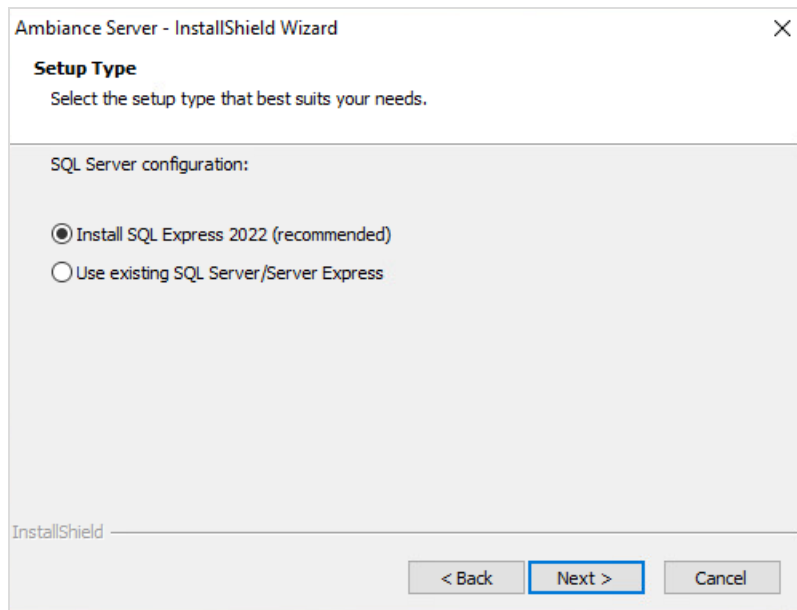
1. Select the IP address or host name to use for the installation.
2. Click **Next**.



Ambiance must be installed using a static IP address (not a hostname) for Single Sign-On to function properly.

7.6 Setup Type page

This page only displays if the installer detects an existing instance of SQL Server.

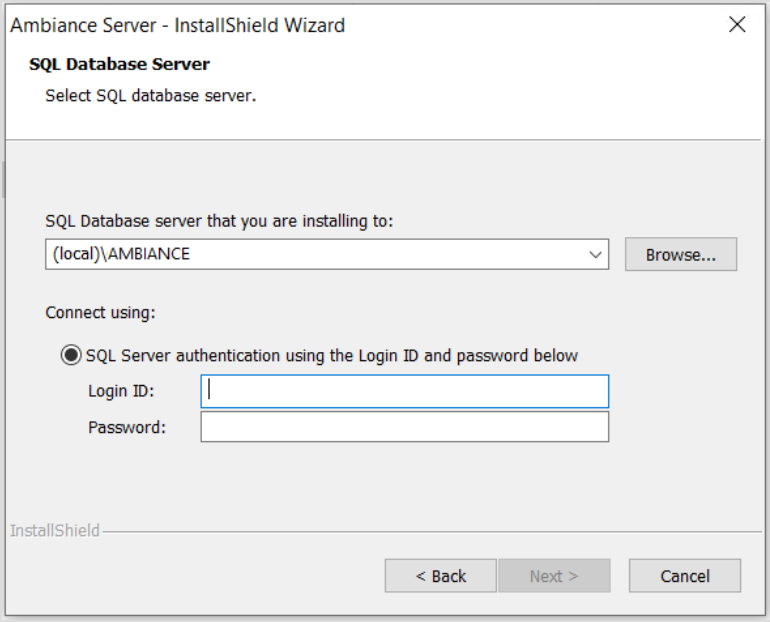


On the Setup Type page:

Select whether to install a new instance of SQL Server or connect to an existing local or remote SQL Server/Server Express database instance. If installing a new instance, SQL Server Express 2022 is installed. Any instance to which you connect must be a supported version (see *Requirements*).

- If installing a new instance, click **Next** and proceed to *Setup Status Page*.
- If connecting to an existing instance, click **Next** and proceed to *SQL Database Server Page*.

7.7 SQL Database Server page



On the SQL Database Server page:

- 1. Click [Browse](#), navigate to select the correct SQL instance.
- 2. Specify valid SQL Server credentials
- 3. Click **Next**.

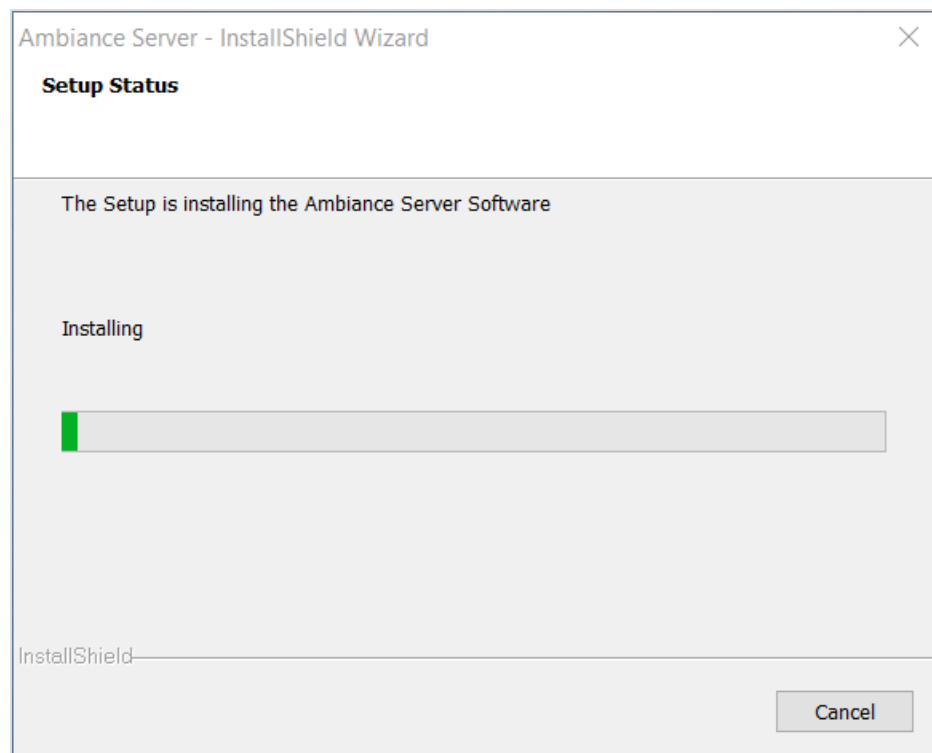


If there is no database attached to the selected instance, a message informs to prepare for using an existing SQL Server instance. For instructions, see the previous chapter.

Refer to the following default locations.

Data	Location Stored	Backup Option	Frequency	Retention
SQL Server	Specified directory (local or remote)	On-demand	On-demand	Current backup
	Default: C:\Program Files\Microsoft SQL Server\MSSQL16.AMBIANCE\MSSQL\Backup	Per schedule	Per schedule	Per setting
	Default for upgrades: existing setting persists			
GDPR symmetric key	ProgramData\DormaKaba\Ambiance\backup (local only)	Per site policy		
MongoDB	MongoDB folder in specified directory (local only)	Per schedule	Per schedule	Latest backup
	Default for new installations and upgrades with remote SQL Server: none			
	Default for upgrades with local SQL Server: existing setting persists			
Archive	Specified directory (local allowed but external hard drive, network drive, or remote server recommended)	Per schedule	Per schedule	Indefinite
	Default: C:\Program Files\dormakaba\Ambiance Server\Archive			
	Default for upgrades: existing setting persists			

7.8 Setup Status page



The Setup Status page displays the installation status. When prompted, click **Next**.

7.9 SSL Certificate Selection page



Security is your responsibility. dormakaba strongly recommends installing an SSL certificate to enable the HTTPS protocol. The SSL certificate to enable HTTPS mode must be provided by a well-known and trusted certificate authority.

On the Setup Type page:

1. Select whether to install an SSL certificate.
 - Select [Install a PFX certificate](#), then click [Browse](#) and navigate to select a file.
 - Select an existing certificate from the CAPI certificate store. Certificates in the Personal and Web Hosting folders display. The [Friendly name](#) can be modified in [System Settings](#).



An advantage to selecting a certificate from the CAPI store is that Ambiance detects and rebinds a new certificate based on the friendly name and Valid from dates. Options are configured in [System Settings](#).

- Select [Install without a certificate \(HTTP\)](#).
2. Click **Next**. If you proceed without installing a certificate, a warning displays.



To install an SSL certificate after installation, use the Service Manager (on the server); use the Service Manager (on workstations) to change the server IP/name to https://.

7.9.1 Choose SSL certificate

In File Explorer:

1. Navigate to and select the SSL certificate to install.
2. Click **Open**.

7.9.2 Password page

Ambiance Server - InstallShield Wizard

Password

This setup has been password protected.

If applicable, enter the password for the SSL certificate, to use the HTTPS protocol.

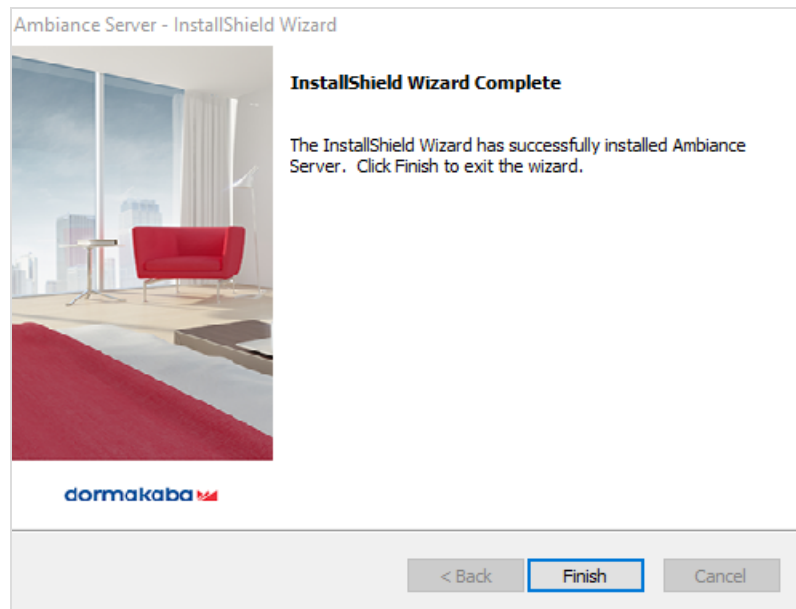
InstallShield

< Back **Next >** Cancel

On the Password page:

1. Specify the password for the SSL certificate that you selected.
2. Click **Next**.

7.10 Installation Complete page



When notified the installation is complete, click **Finish**.



After the Ambiance Server is installed, upgraded or restarted, wait two to three minutes before using Ambiance.

8 Ambiance client installation

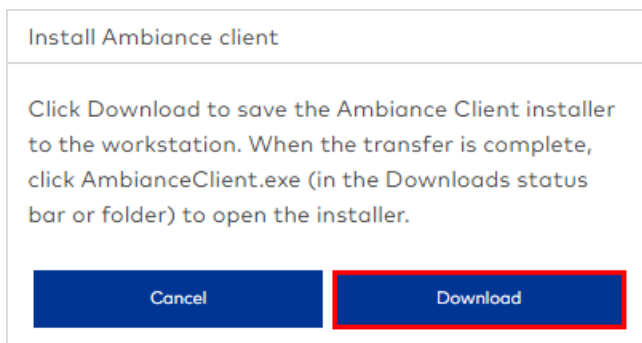
This chapter guides you through the Ambiance Client installation. You must install the Client on every workstation where a USB encoder and / or Maintenance Unit is required.

To install the Ambiance Client:

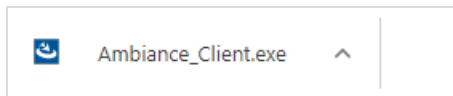
1. In a supported browser, go to the IP address of the Ambiance server.
2. Log in.
3. Go to [Device Management](#).



4. In the toolbar, click to install the Ambiance client.

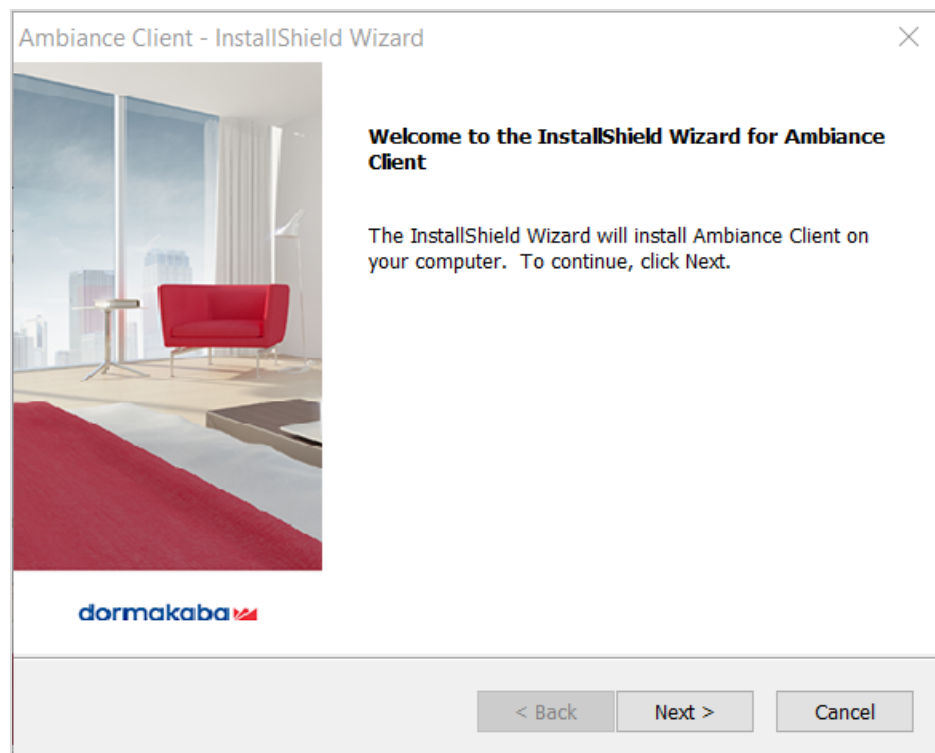


5. Click [Download](#). A total of three files are required `Ambiance_Client.exe`, `serverURL.config`, and `token.txt`.



6. Open **Ambiance.exe**. The installation wizard opens and prepares for setup. Depending on the computer, the following step may occur during installation:
 - The wizard checks for Microsoft .NET 8.0, and installs it if not found.
7. Follow the instructions for each of the following wizard pages.

8.1 Welcome page



On the Welcome page:

- Click **Next**.

8.2 License Agreement page

Ambiance Client - InstallShield Wizard

License Agreement

Please read the following license agreement carefully.

AmbianceTM Software Terms of Use and End User License Agreement

PLEASE READ THIS DOCUMENT CAREFULLY, AS IT CONTAINS TERMS THAT MAY AFFECT YOUR LEGAL RIGHTS.

These Terms of Use and End User License Agreement (this "TOU"), is a binding agreement between dormakaba Canada Inc. ("dormakaba Canada", "Licensor", "We", "Our" or "Us") and you ("Licensee", "You" or "Your"). This TOU governs Your use of the AmbianceTM software application ("Software"), and any printed materials or online and electronic documents ("Documentation"). We license use of the Software and Documentation to you on the basis of this TOU. We do not sell the Software or Documentation to You. We remain the owners of the Software and Documents at all times.

☒ I accept the terms of the license agreement

☐ I do not accept the terms of the license agreement

Print

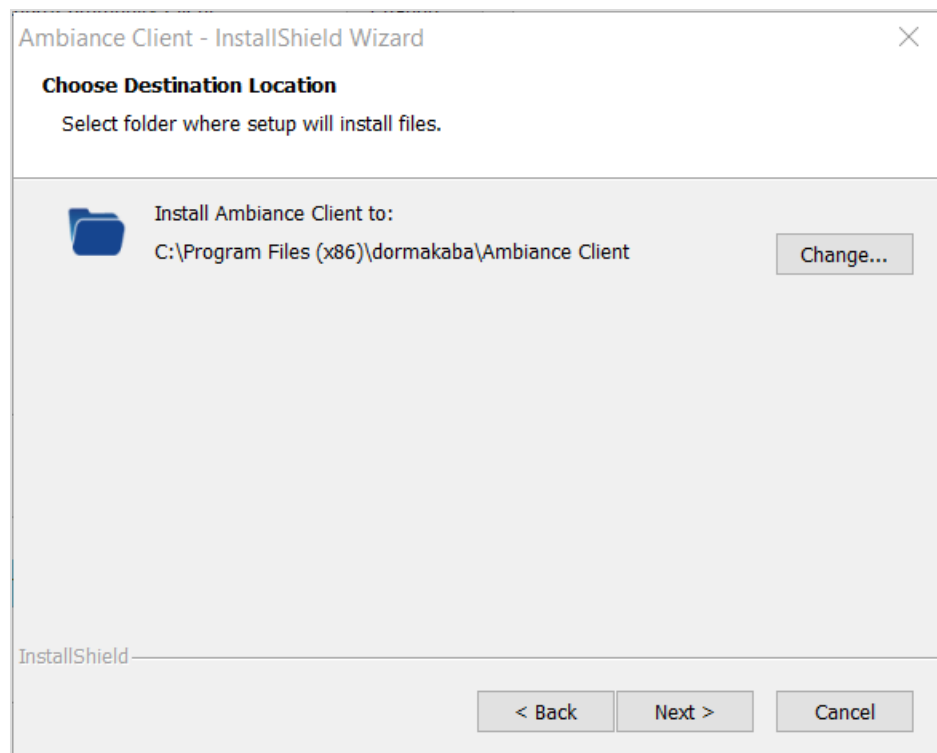
InstallShield

< Back Next > Cancel

On the License Agreement page:

1. Accept the terms of the license agreement.
You can optionally print the agreement.
2. Click **Next**.

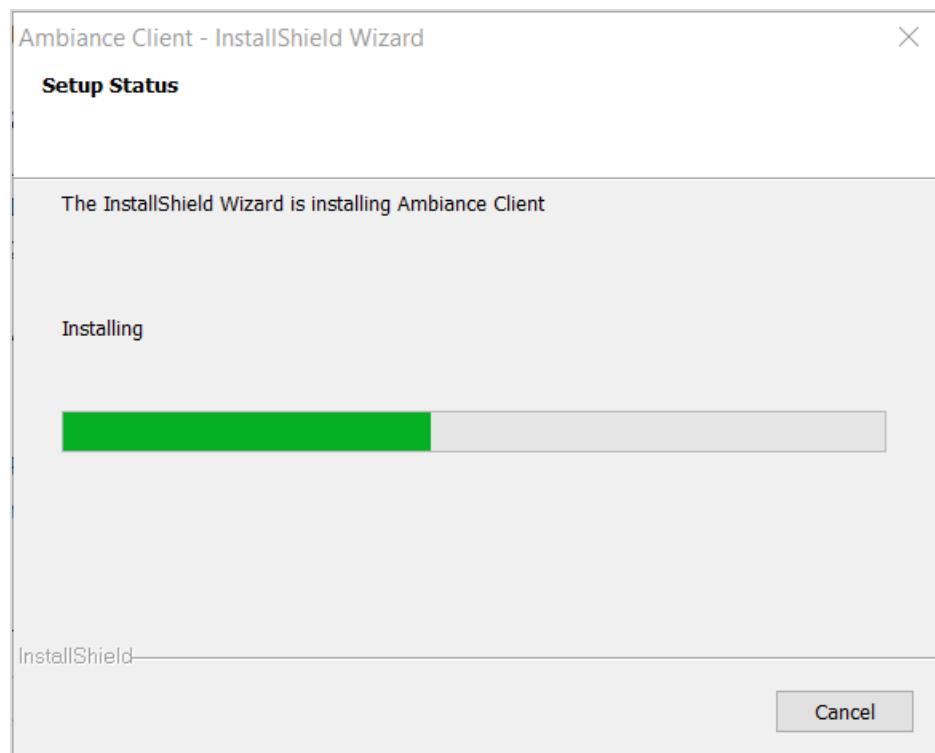
8.3 Choose Destination Location page



On the Choose Destination Location page:

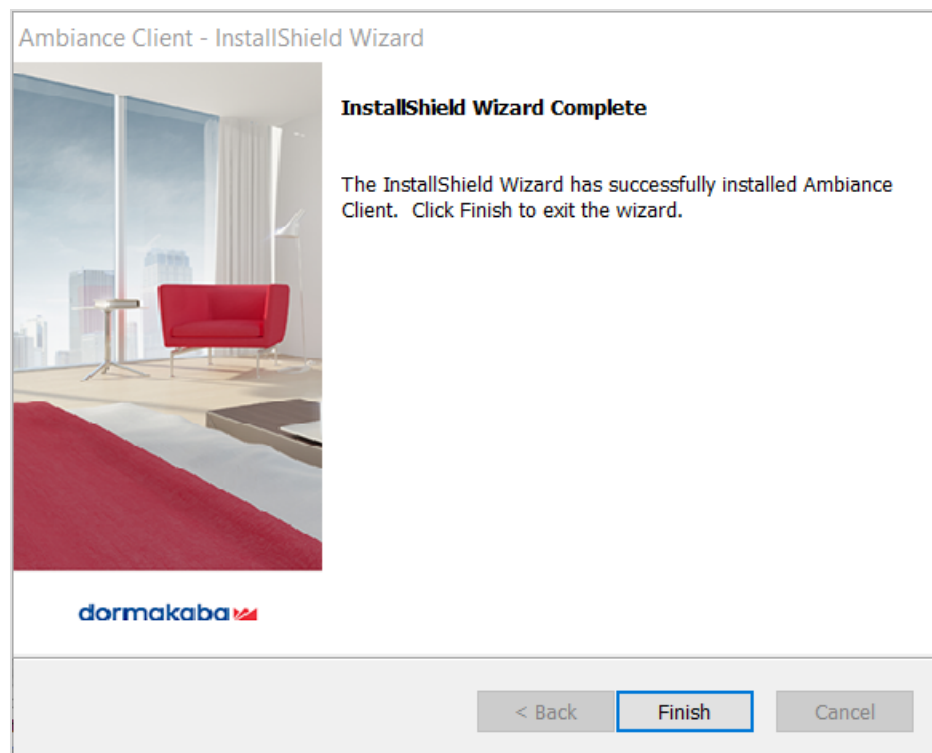
1. Choose where to install Ambiance Client files:
 - Accept the default location (recommended).
 - Click **Change** and navigate to a location on the server.
2. Click **Next**.

8.4 Setup Status page



The Setup Status page displays the installation status. When prompted, click **Next**.

8.5 Installation Complete page



When notified the installation is successful, click [Finish](#).

9 Post-installation checklist

The following items apply to initial installations only.

1	☐	Server. Re-enable antivirus software.
2	☐	Server. If necessary, re-enable Windows Defender.
3	☐	Server. Activate the product. Open Ambiance in a supported browser and specify a valid activation key for Ambiance 2.15.0.
4	☐	Server or Client. Change the default password.
5	☐	Server (Online Installations only). Make sure gateway and access point firmware versions are updated to the latest versions as per "Device Requirements."
6	☐	Microsoft Edge. A Windows issue prevents the Edge browser from detecting/connecting to the Maintenance Unit. Consequently, access points cannot be programmed or audited without intervention. Open the Command prompt and issue the following command: <code>C:\windows\system32\CheckNetIsolation.exe LoopbackExempt -a -n=Microsoft.MicrosoftEdge_8wekyb3d8bbwe</code>
7	☐	Microsoft Edge. Add the Ambiance Server IP address as a trusted site. Go to Control Panel > Network and Internet > Internet Options > Security > Trusted Sites . Click Sites and add the Ambiance Server IP address.
8	☐	Microsoft Edge. Default Windows 10 Edge browser security blocks access to the local host thus disallowing Maintenance Unit communication for access point programming and auditing operations. Use Chrome or run the following command from the Windows console: - Windows 10 Build 10158 or above: CheckNetIsolationLoopbackExempt-a-n=Microsoft.MicrosoftEdge_8wekyb3d8bbwen - For previous builds: CheckNetIsolationLoopbackExempt-a-n=Microsoft.Windows.Spartan_cw5n1h2txyewy
9	☐	Server. Go to ProgramData\DormaKaba\Ambiance\backup, make a copy of the GDPR symmetric key file, and store the key file at a secure location.
10	☐	Server (Online Installations only). For Saflok to Ambiance conversions, upgrade firmware remotely with Saflok S6000/LENS before transitioning to Ambiance.

10 Ambiance upgrades

This chapter provides information and instructions for upgrading versions of Ambiance 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.

The following upgrade paths are supported:

- versions 1.4.0 and later → 2.9.0
- versions 2.9.0 and later → 2.15.0



Ambiance 2.10.0 introduced enhanced security mode to provide an additional layer of key security. Although the feature is disabled by default, dormakaba strongly recommends enabling enhanced security mode.

Before upgrading, refer to *Ambiance Enhanced Key Security for Upgrades* 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.

10.1 Pre-upgrade checklist

1	☐	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	☐	IMPORTANT! Server/Client. Verify that all Windows updates are installed.
3	☐	IMPORTANT! Server. For online-enabled sites, back up the MongoDB database. This step is required to retain transaction data.
4	☐	Server. Take a backup of the SQL Server database before performing an upgrade.
5	☐	Server. Ensure that a backup of the GDPR symmetric key is saved at a separate secure location. The default location is: ProgramData\DormaKaba\Ambiance\backup.
6	☐	Server/Client. Perform the installation as a Local Administrator .
7	☐	Server. Make sure antivirus software is disabled before proceeding with server installation.
8	☐	Server. If possible, disable Windows Defender for the duration of the installation.

10.2 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.



If Ambiance is configured to use the MIFARE Classic RFID key type, a warning displays with important security information and instructions to modify RFID key type settings.



The upgrade process includes upgrading the Ambiance database.

10.3 Post-upgrade checklist

1	☐	Restart the Ambiance Server.
2	☐	Server. Re-enable antivirus software.
3	☐	Server. If necessary, re-enable Windows Defender.
4	☐	Server. For online-enabled properties that are upgrading from version 2.13.x and earlier to version 2.14.x 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	☐	IMPORTANT! Server. Restore the MongoDB database.
6	☐	Upgrade the Ambiance 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 .
8	☐	If upgrading from Ambiance 2.10.x or 2.11.x for properties already enabled with Enhanced Key Security and using TCP/IP encoders, delete then re-add all TCP/IP encoders.



To enable enhanced key security after upgrade, refer to *Ambiance Enhanced Key Security for Upgrades* (PK3777). The document lists requirements and provides step-by-step instructions for enabling enhanced key security.

10.4 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)

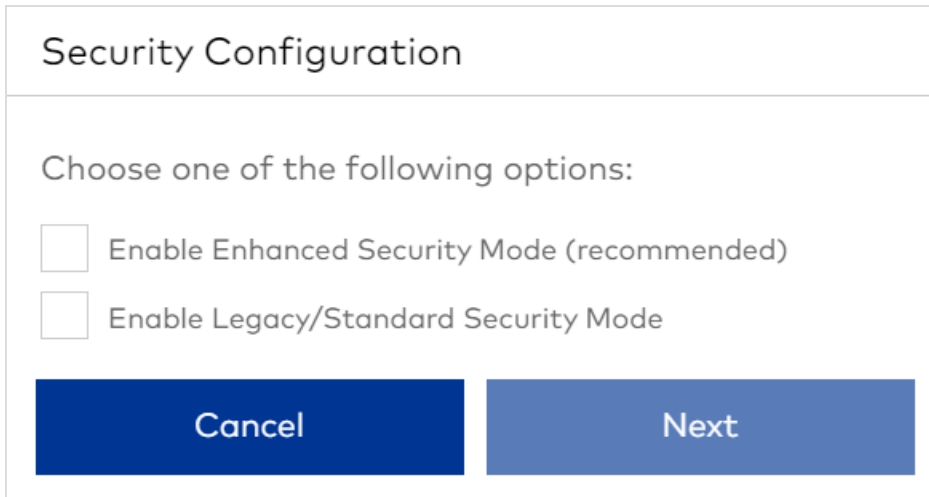
11 Getting started with Ambiance

This chapter provides basic information for getting started with Ambiance.

11.1 Product activation

Ambiance must be activated to access, configure and use the product.

1. Go to the IP address of the Ambiance server in the location bar of a supported browser.
2. Specify a valid activation key. dormakaba provides the activation key with the product purchase or upon request when a new activation key is required.
3. Log in using the Admin01 account. The default password is provided with the product purchase. Ambiance prompts require changing the password for the Admin01 account.
 - For new installation initial logins, proceed to the next step.
 - For all other logins, the Home page displays. Proceed to configure the product.
4. Select whether to enable enhanced security mode, then click [Next](#).



Security Configuration

Choose one of the following options:

☐ Enable Enhanced Security Mode (recommended)

☐ Enable Legacy/Standard Security Mode

Cancel Next

- If the option [Enable Enhanced Security Mode](#) was selected, proceed to the next step.
 - If the option [Enable Legacy/Standard Security Mode](#) was selected, the Home page displays. Proceed to configure the product.
5. Acknowledge that requirements to enable enhanced security mode are established, then click [Next](#).

Security Configuration

IMPORTANT: The Enhanced Security Mode option cannot be disabled once configured.

Before enabling this mode, confirm the following:

- ☒ All active keys in circulation are MIFARE Ultralight AES, MIFARE Ultralight C and/or MIFARE Plus. (MIFARE Classic keys are not supported in this mode).
- ☒ All encoders are dormakaba RFID encoder II (part number 75720) and meet the minimum firmware version requirement. Refer to Ambiance Release Notes.
- ☒ All Maintenance Units are type HH6 NFC and meet the minimum firmware version requirement. Refer to Ambiance Release Notes.
- ☒ All locks, elevator controllers meet minimum firmware version requirements. Refer to Ambiance Release Notes.

Back

Next

The Home page displays. Proceed to configure the product.

11.2 Site configuration workflow

The Ambiance workflow is an excellent resource to guide your deployment. The document provides an overview of the application flow and the first steps to take in each module to set up Ambiance.

The *Ambiance User Guide* is a new resource that provides information and instructions for all Ambiance Operators.

- The "Site Configuration" section provides an easy-to-follow workflow and step-by-step instructions for setting up Ambiance.
- The "Using Ambiance" section provides instructions for day-to-day work after Go Live and includes *Troubleshooting* and *Working with ...* topics that address some of the more complicated situations.

Look for the guide in the software download folder.

11.3 Remember to ...

- Go to [System Settings > Database Backup](#) to configure regularly scheduled backups and data retention for the Ambiance SQL Server database and for online systems, the MongoDB database. The recommendation is to store backups at a secure external location.
- Go to ProgramData\DormaKaba\Ambiance\backup, make a copy of the GDPR symmetric key file, and store the key file at a secure location.
- If not licensed for PPK/SPK Storage, go to [System Keys](#) and make primary and secondary program keys.

A Appendix A: Service Manager

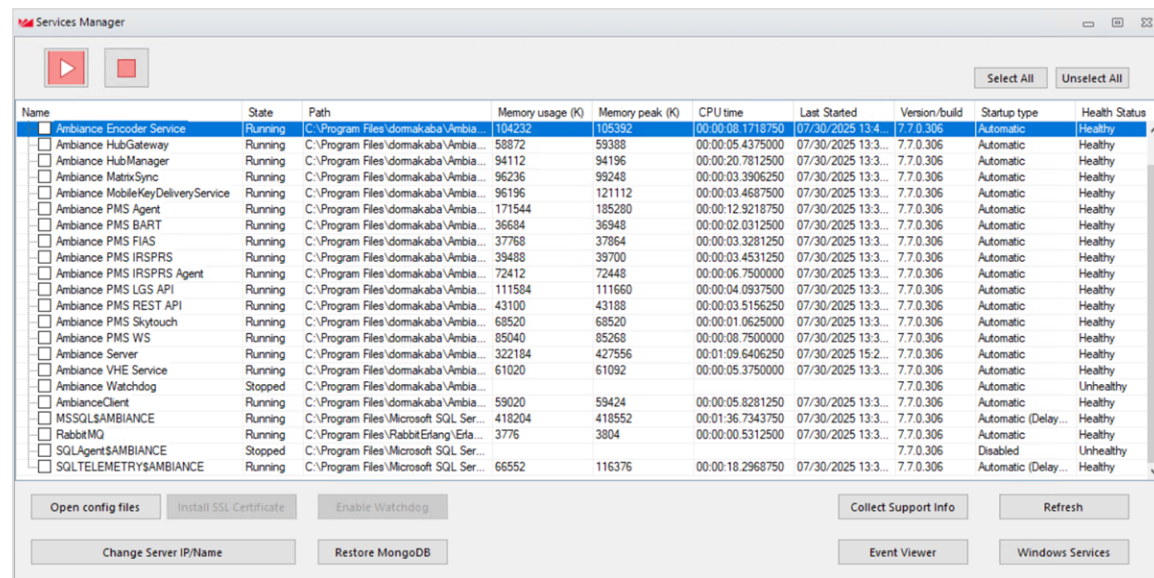
The Service Manager provides convenient access to post-installation configuration options. Access the Service Manager at the following locations:

- On the Ambiance server:

C:\Program Files\dormakaba\Ambiance Server\Services\Service Manager\ServiceManager.exe

- On the Ambiance client:

C:\Program Files (x86)\dormakaba\Ambiance Client\Services\Service Manager\ServiceManager.exe



A.1 Installing / renewing SSL certificate after installation

Use the Service Manager to install or renew an SSL certificate on the Ambiance server after installation. Each Ambiance workstation must be updated to use the HTTPS protocol.



This feature applies to the certificate for the browser, LGS REST API, and LGS REST KF2 API.

A.1.1 Server

- On the Ambiance server, open the Service Manager.
- Click [Install SSL Certificate](#).
- Disregard the warning message and click [Yes](#) to proceed.



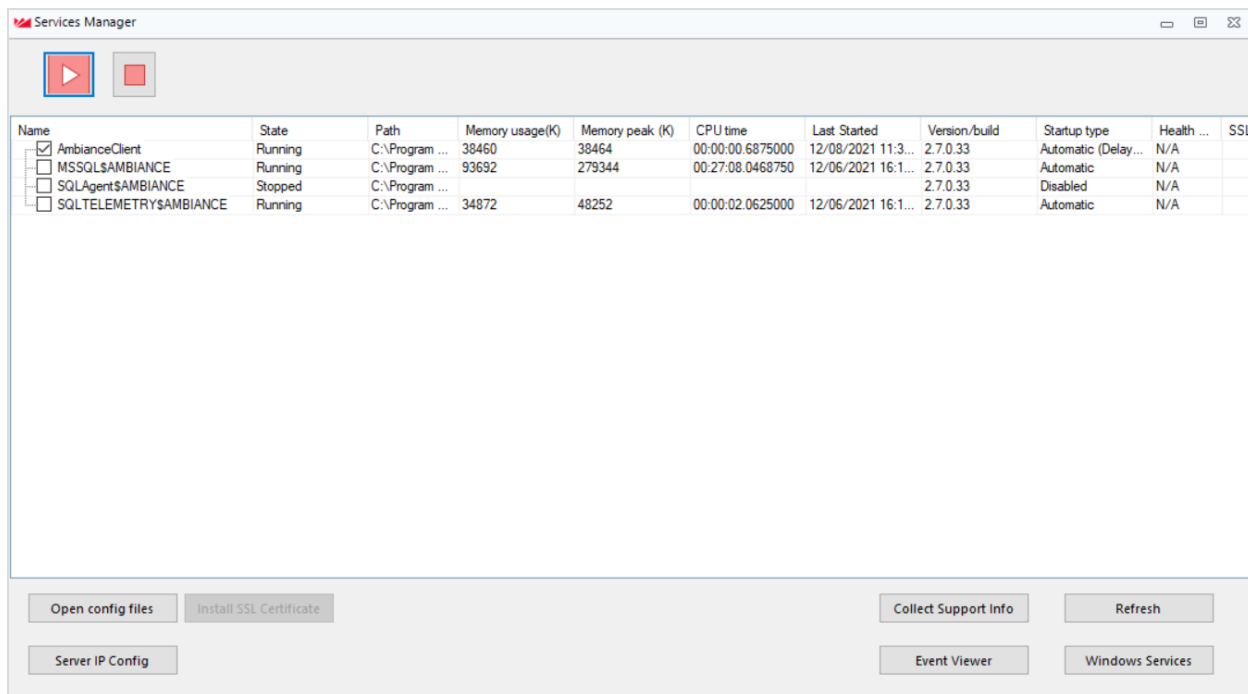
- If applicable, specify the password for the certificate.
- Click [Select File](#).

6. Navigate to and select the certificate (.pfx).
7. When notified the certificate was installed successfully, click **OK**.

A.1.2 Client

The following steps must be performed on each Ambiance workstation.

1. Open the Service Manager.



2. Select the **AmbianceClient** service and click  to stop the service.
3. Click **Open Config files**.
4. Change "WebAPIUrl" and "signalrURL" values to point to **https**:
 - From:


```
<add key="WebAPIUrl" value="http://<Ambiance Server IP>/WebAPI/" />
<add key="signalrURL" value="http://<Ambiance Server IP>/WebAPI/signalr/" />
```
 - To:


```
<add key="WebAPIUrl" value="https://<Ambiance Server IP>/WebAPI/" />
<add key="signalrURL" value="https://<Ambiance Server IP>/WebAPI/signalr/" />
```
5. Save and close the configuration file.

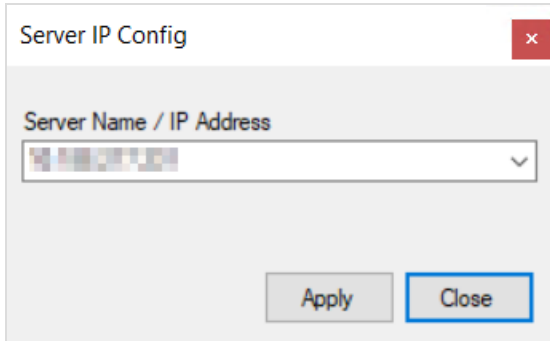
6. Click  to restart the AmbianceClient service.

A.2 Changing server IP address

Use the Service Manager to change the Ambiance server IP address after installation. Changing the IP address requires that the Ambiance client be uninstalled and reinstalled on each workstation.

A.2.1 Server

1. On the Ambiance server, open the Service Manager.
2. Click [Server IP Config](#).
3. Disregard the warning and click [Yes](#) to proceed.
4. Specify the new IP address, then click [Apply](#).



5. Restart the Ambiance Server.

A.2.2 Client

The following steps must be performed on each Ambiance workstation.

1. Open the Service Manager.



2. Select the [AmbianceClient](#) service and click  to stop the service.
3. Click [Open Config files](#).
4. Change "WebAPIUrl" and "signalrURL" values to point to the new IP address.
 - From:

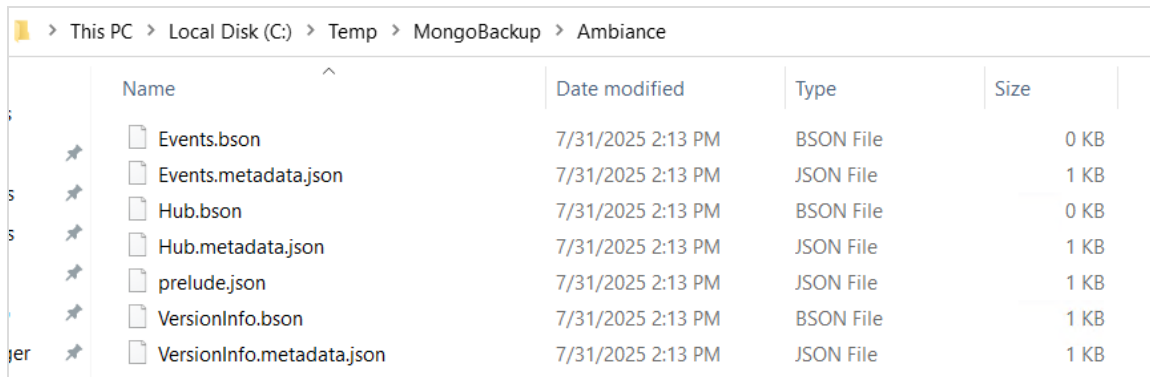

```
<add key="WebAPIUrl" value="https://<Ambiance Server IP>/WebAPI/" />
<add key="signalrURL" value="https://< Ambiance Server IP>/
WebAPI/signalr/" />
```
 - To:


```
<add key="WebAPIUrl" value="https://< Ambiance NewServer IP>/WebAPI/" />
<add key="signalrURL" value="https://< Ambiance NewServer IP>/
WebAPI/signalr/" />
```
5. Save and close the configuration file.
6. Click  to restart the AmbianceClient service.

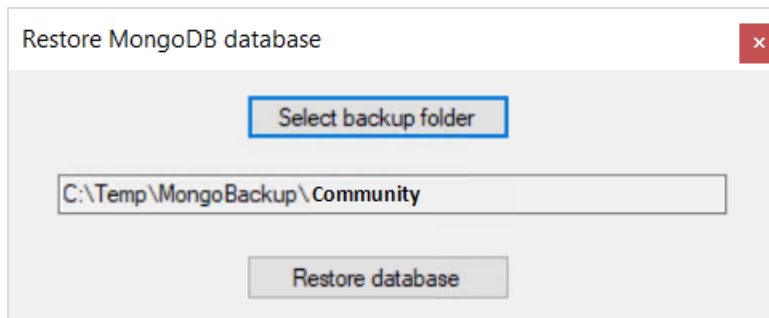
A.3 Restore online database

Use the Service Manager to restore the MongoDB database when online communication is enabled.

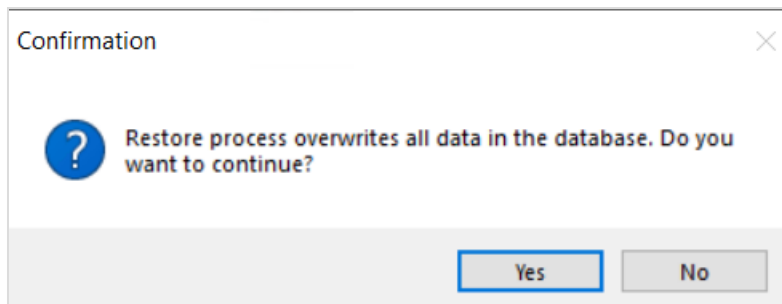
1. On the Ambiance server, open the Service Manager.
2. Click [Restore MongoDB](#).
3. Click [Select backup folder](#), then navigate to and select the MongoDB backup collection folder [Ambiance](#)(which contains the .json files).



Name	Date modified	Type	Size
Events.bson	7/31/2025 2:13 PM	BSON File	0 KB
Events.metadata.json	7/31/2025 2:13 PM	JSON File	1 KB
Hub.bson	7/31/2025 2:13 PM	BSON File	0 KB
Hub.metadata.json	7/31/2025 2:13 PM	JSON File	1 KB
prelude.json	7/31/2025 2:13 PM	JSON File	1 KB
VersionInfo.bson	7/31/2025 2:13 PM	BSON File	1 KB
VersionInfo.metadata.json	7/31/2025 2:13 PM	JSON File	1 KB



- Click **Restore database**. A message indicates whether the restore was successful.



- Restart the Ambiance server.

A.4 Disable/enabling Watchdog

The Service Manager includes a Watchdog feature that performs regular healthchecks on server. The Watchdog is enabled by default. To disable / enable Watchdog, open Service Manager and click the appropriate button.

B Appendix B: Polling service

Ambiance offers a feature that polls third-party servers to detect requests for mobile keys. The feature requires an SSL certificate. When enabled, the Ambiance Service Manager automatically renews the certificate.

For initial installations, consult the site IT Administration to configure the following polling service settings:

1. On the Ambiance server, go to:
`\dormakaba\AmbianceServer\Services\MobileKeyDeliveryService`.
2. Open the file `MobileKeyDeliveryService.exe.Config`.
3. Specify key values for the certificate:
 - `<add key="PollingServiceCertificateThumbprint" value="customValue" />`
 - `<add key="PollingServiceCertificateIssuerName" value="customValue" />`
4. Specify key values for the polling service URL:
 - `<add key="PollingServiceApiEndpoint" value="customValue" />`
 - `<add key="PollingServiceSiteName" value="customValue" />`
 - `<add key="PollingServiceRequestToken" value="/digitalKeyDetails_MPG" />`
 - `<add key="PollingServiceResponseToken" value="/digitalKeyDetails_MPG" />`
5. Specify the authentication settings for Ambiance to communicate with the polling service:
 - `<add key="PollingServiceMpgUserName" value="customValue" />`
 - `<add key="PollingServiceSecurityToken" value="customValue" />`
 - `<add key="PollingServiceIsSecurityEnabled" value="true" />`
6. Enable the polling service:
 - `<add key="PollingServiceEnabled" value="true" />`
7. Select whether to enable the automatic renewal of the SSL certificate:
 - `<add key="PollingCertificateManagerEnabled" value="true" />`

The following key values are read from the certificate thumbprint and auto-populated:

 - `<add key="CertIssuedTo" value="auto_populates" />`
 - `<add key="CertFriendlyName" value="auto_populates" />`
8. Save the file.



The certificate friendly name must also be specified at System Settings/Security/HTTPS Certificate.

To manually change the SSL certificate, use the Ambiance Service Manager (at Program Files\dormakaba\Ambiance Server\Services\ServiceManager).

C Appendix C: Database restore

This document contains instructions for restoring the Ambiance SQL Server and MongoDB databases. The encryption key (added in Ambiance 2.13) requires an additional restore step using an internal tool accessible only by dormakaba Support. All customers using Ambiance 2.13 or later must contact Support to restore the SQL Server database and when online communication is enabled, the MongoDB database.

The restore process includes the following steps:

1. [Perform required preparatory steps](#):
 - Install the Ambiance server on a reserve machine.
 - Identify database backups. When conditions allow, take an on-demand backup. Go to [System Settings/Database Backup](#), scroll to the bottom of the page, then click [Back Up Database](#).
 - Copy the SQL Server backup and secure key files to the new server.
 - Obtain and configure the dormakaba restore tool [RestoreSiteSpecGDPRKeyRelease](#).
 - Delete the empty Ambiance database on the reserve machine.
 - If MongoDB data already exists, copy all MongoDB collections to the reserve machine.
2. [Restore the SQL Server database](#).
3. When Online Communication is enabled, [restore the MongoDB database](#). When there is no back up for the MongoDB database, all gateways must be reconfigured after restoring the SQL Server database.
4. When the Ambiance server uses a static IP address, [update IP addresses](#) at [System Settings > Online Communication and Device Management > Registered Gateways and Paired Access Points](#).
5. For Ambiance deployments that use the Polling feature, [update server configurations](#).
6. [Update the server IP address on workstations](#). Alternatively, uninstall and re-install the client on each workstation to ensure all references to the Ambiance server are updated.
7. [Update the PMS server](#) with the current IP address.
8. Start all Ambiance Windows services.
9. Restart the Ambiance server.

This following sections list the minimum steps to restore the SQL Server database after a total system failure.

C.1 Required preparatory steps

Perform all of the following steps in preparation to restore the SQL Server database, and when online communication is enabled, the MongoDB database.

C.1.1 Install the Ambiance server on a reserve machine

Re-install the Ambiance server on a new or reformatted machine. For instructions, refer to *Ambiance Installation Guide*. Wait until after the restore to activate Ambiance|Community.

C.1.2 Identify database backups

If database backups are stored off-site, retrieve the backup files; or, if conditions permit, take an on-demand backup.

- Go to [System Settings > Database Backup](#), scroll to the bottom and click [Back Up Database](#).

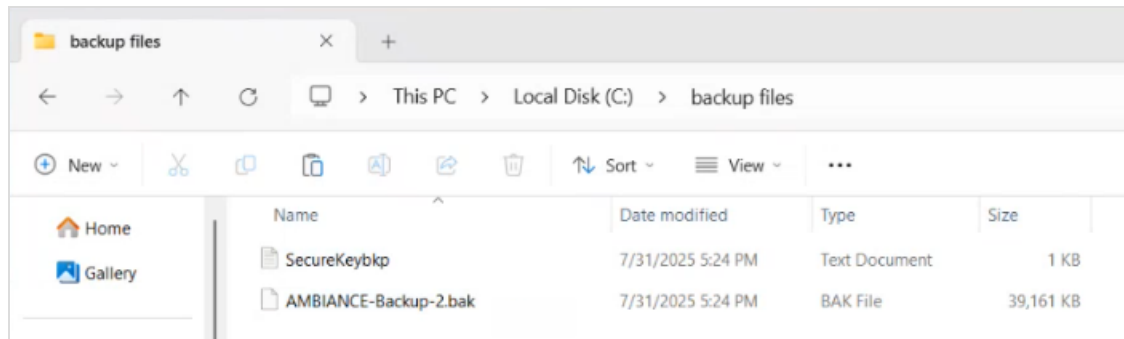


If Online Communication is enabled and there is no backup of the MongoDB database, be prepared to reconfigure the entire online environment.

C.1.3 Copy backup files to the new server

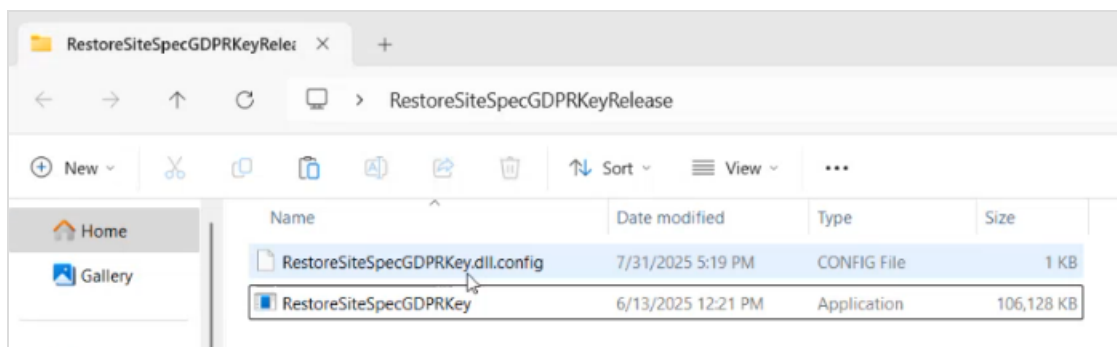
Copy the following backup files to the new server:

- AMBIANCE-backup.bck or COMMUNITY-backup.bck
- SecureKeybkp

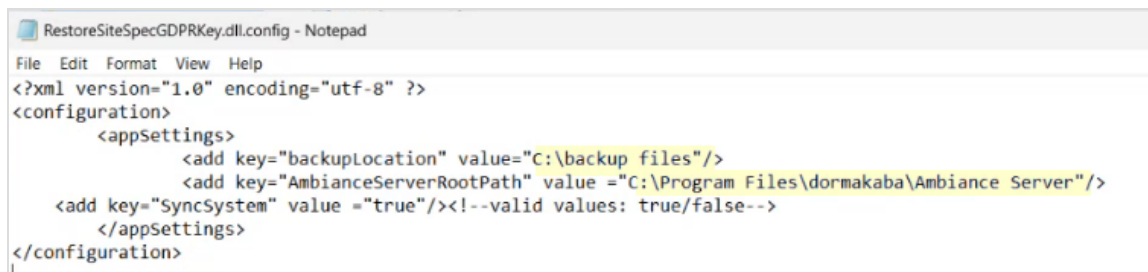


C.1.4 Obtain and configure the dormakaba restore tool

1. Obtain the tool RestoreSiteSpecGDPRKeyRelease.



2. Open the RestoreSiteSpecGDPRKey.dll.config file, then configure backupLocation and AmbianceServerRootPath.

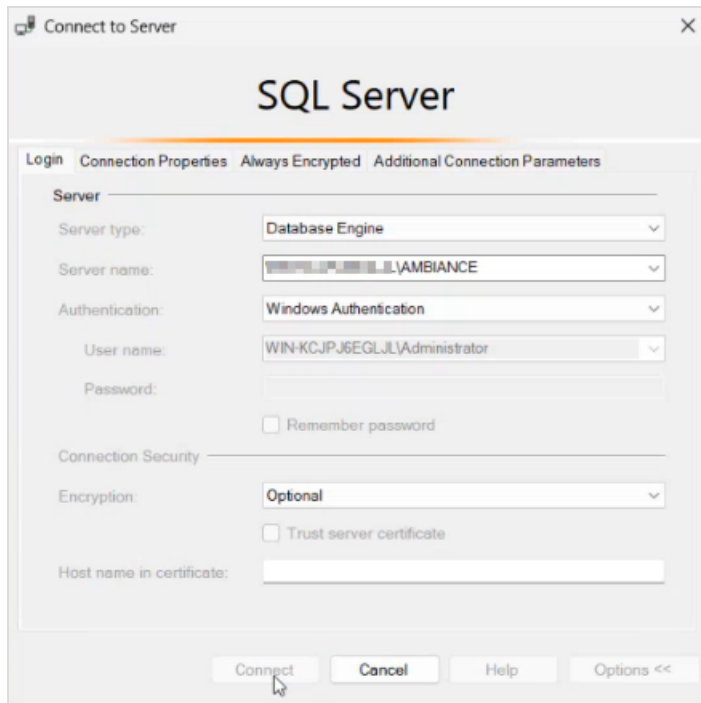


C.2 Restore the SQL Server database

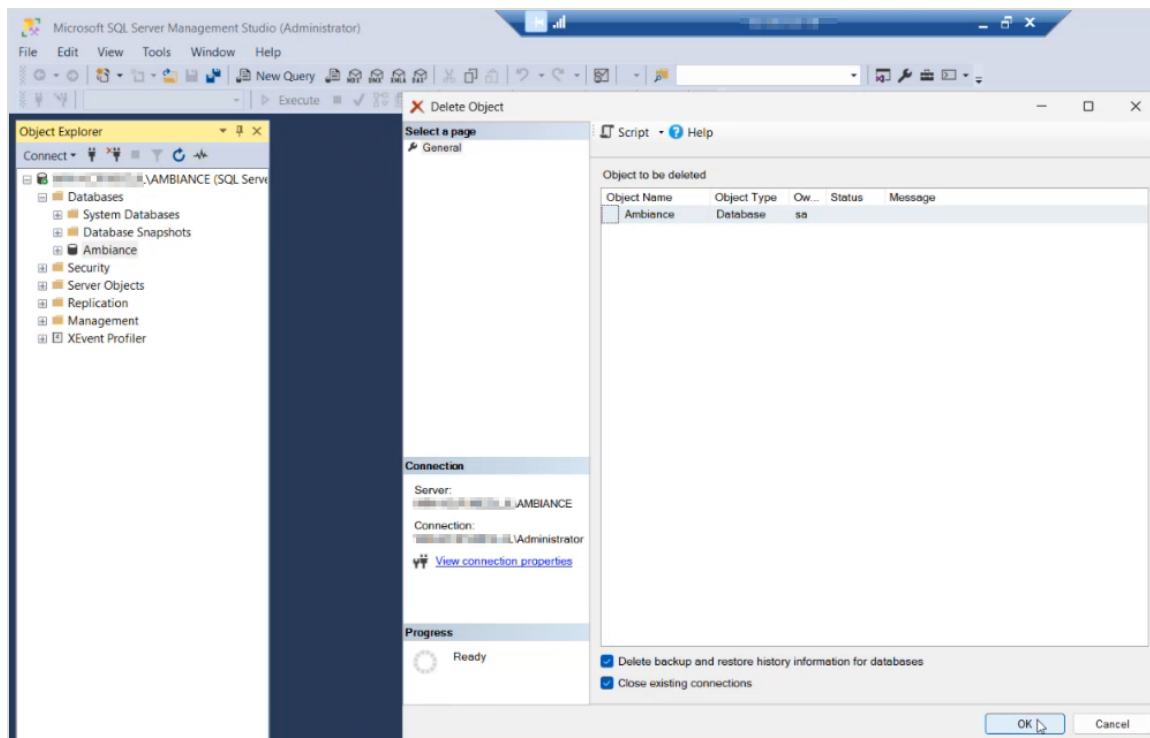
All sites must restore the Ambiance SQL Server database.

Perform the following steps when the Ambiance database has been corrupt or when transferring the database to a different machine:

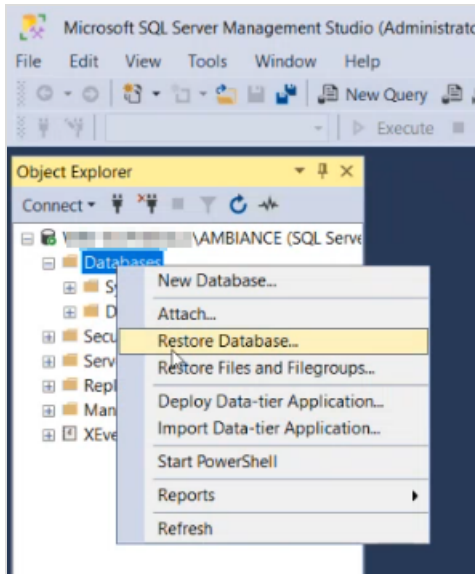
1. Install SQL Server Management Studio. Go to the installation folder `\SERVER\Ambiance_PREREQUIS\` and run `SSMS-Setup-ENU.exe`.
2. Open SQL Server Management Studio.
3. Connect to the server using Windows Authentication and Encryption Optional.



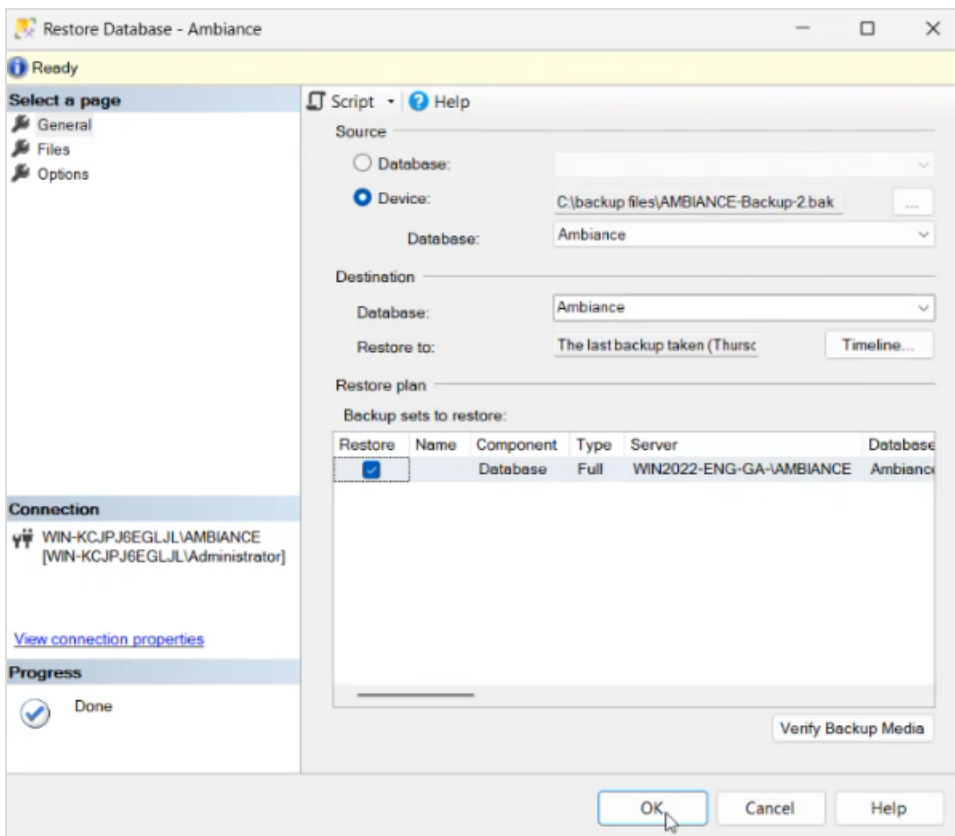
4. Delete the empty Ambiance database. Expand the **Databases** folder, right-click the **AMBIANCE** database, then select **Delete**. On the Delete Object screen, click **OK**.



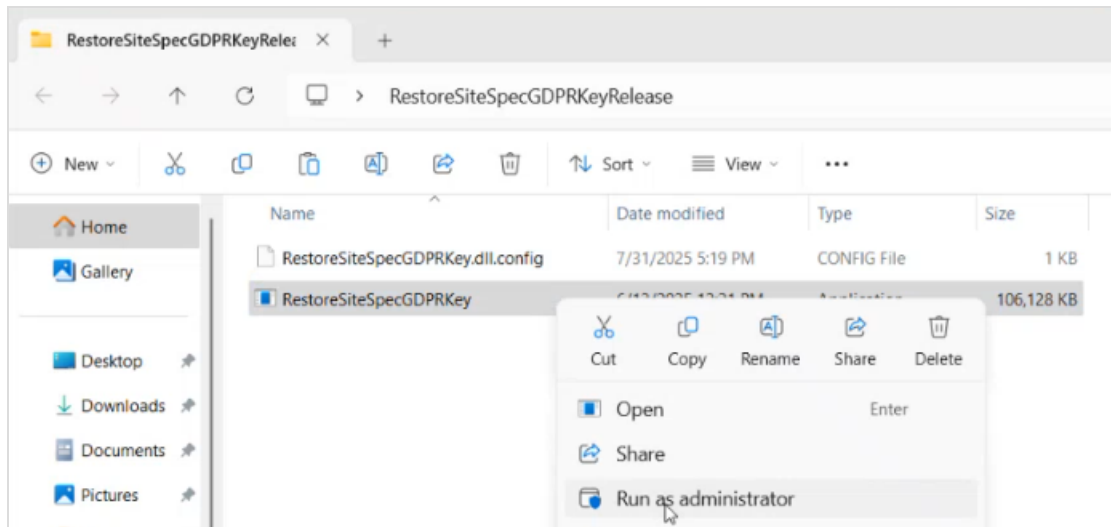
5. After the empty database is deleted, right-click the **Databases** folder again and select **Restore Database**.



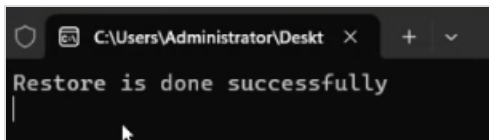
6. On the Restore Database screen, select **Device**. For **Database**, click **...** to navigate to and select the SQL Server backup file. Click **OK**.



7. When the database is successfully restored, click **OK**.
8. Navigate to the RestoreSiteSpecGDPRKeyRelease tool.



9. Right-click `RestoreSiteSpecGDPRKey` and select `Run as administrator`. The program runs and notifies when the restore is successful. Press any key to close the tool.



10. Restart the Ambiance|Community server.
11. Go the Ambiance login page to find the SQL Server database is restored. No activation is required.

Please enter your login information

Username

Password

☐ Remember me

[Forgot your password?](#)

C.3 Restore the MongoDB database

Sites where Online Communication is enabled must restore the MongoDB database.

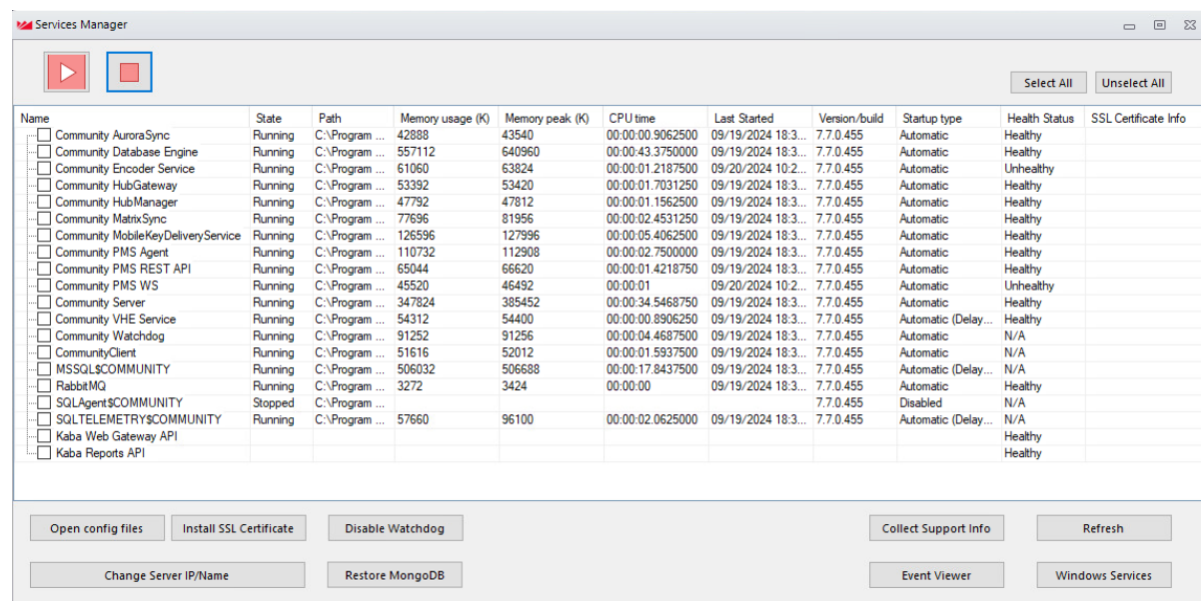
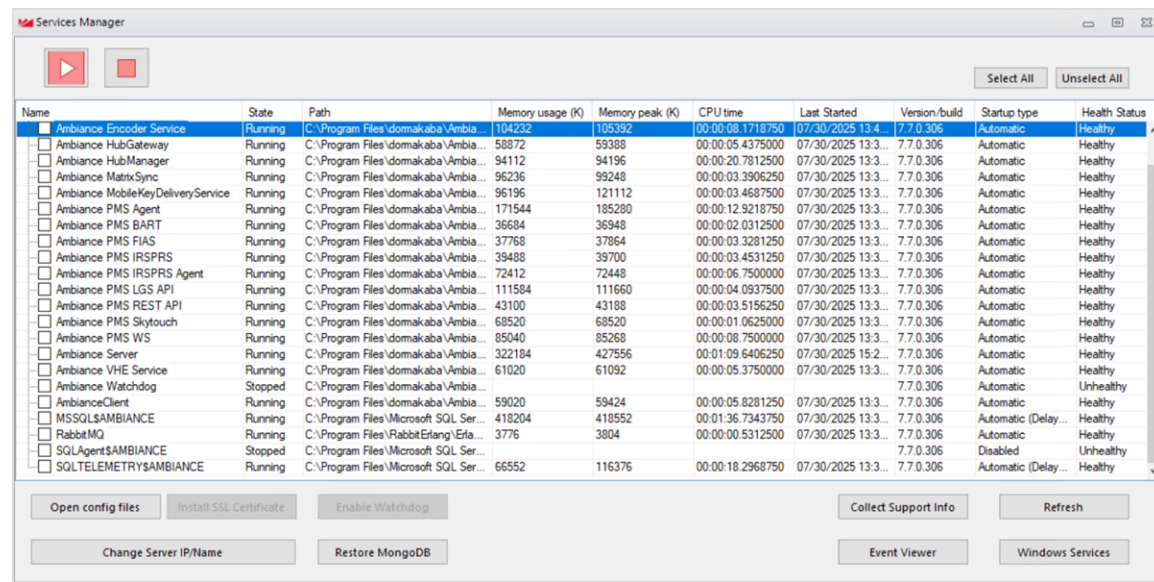


For sites where Online Communication is enabled and no backup of the MongoDB exists, all gateways must be reconfigured. After restoring the SQL Server database, go to [Device Management](#) and refer to Context Help or "[Remote Lock Management](#)" in the the *Ambiance User Guide* for instructions how to set up gateways and pair access points.

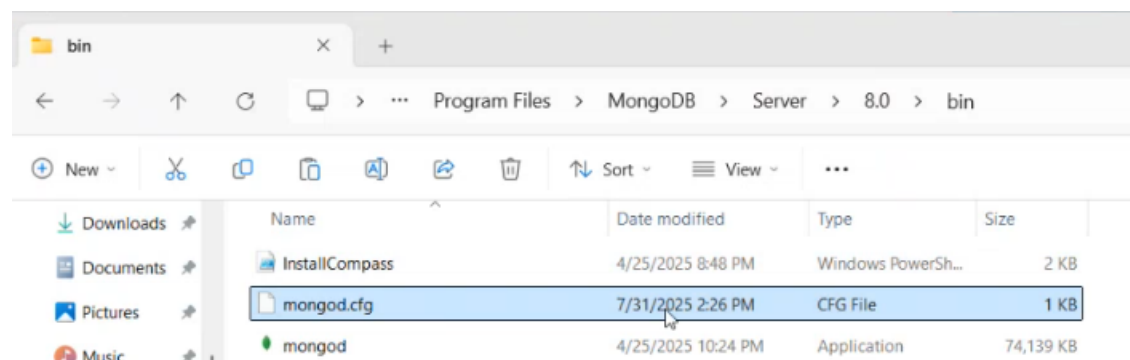
Use the Service Manager to restore the MongoDB database.

- On the Ambiance server:

C:\Program Files\dormakaba\Ambiance Server\Services\Service Manager\ServiceManager.exe



1. On the Ambiance server, navigate to the MongoDB configuration file [mongod.cfg](#).

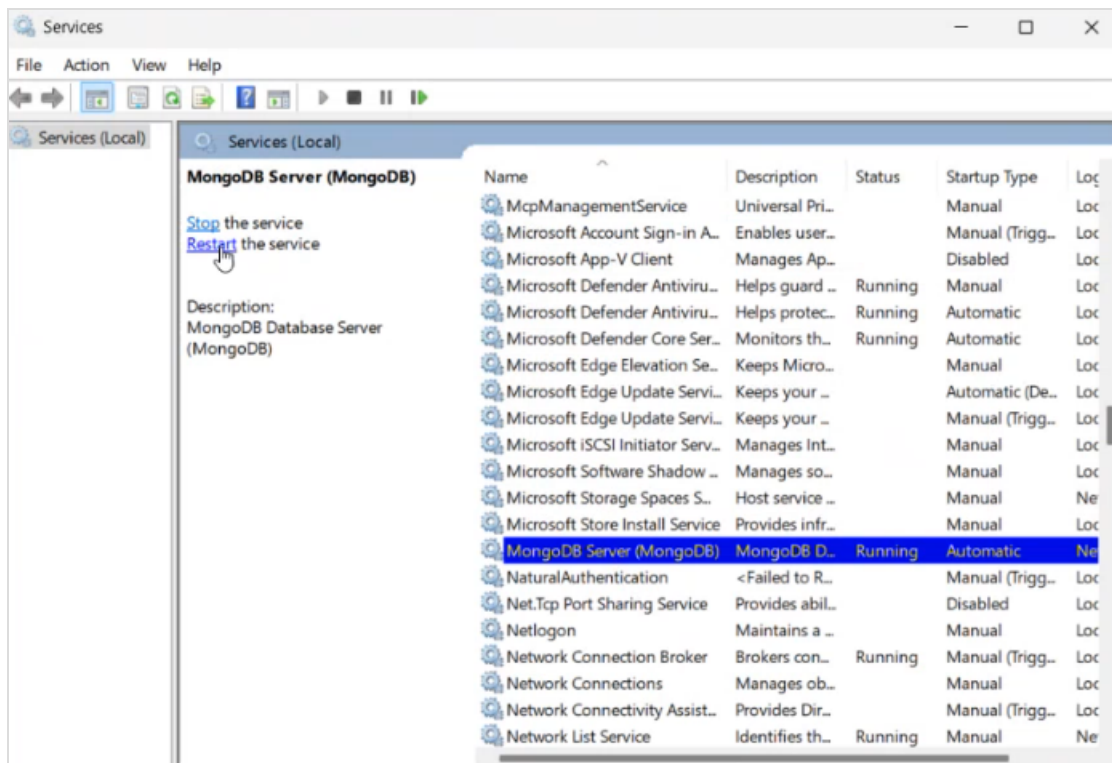


2. Open the configuration file and change the security authorization to disabled.

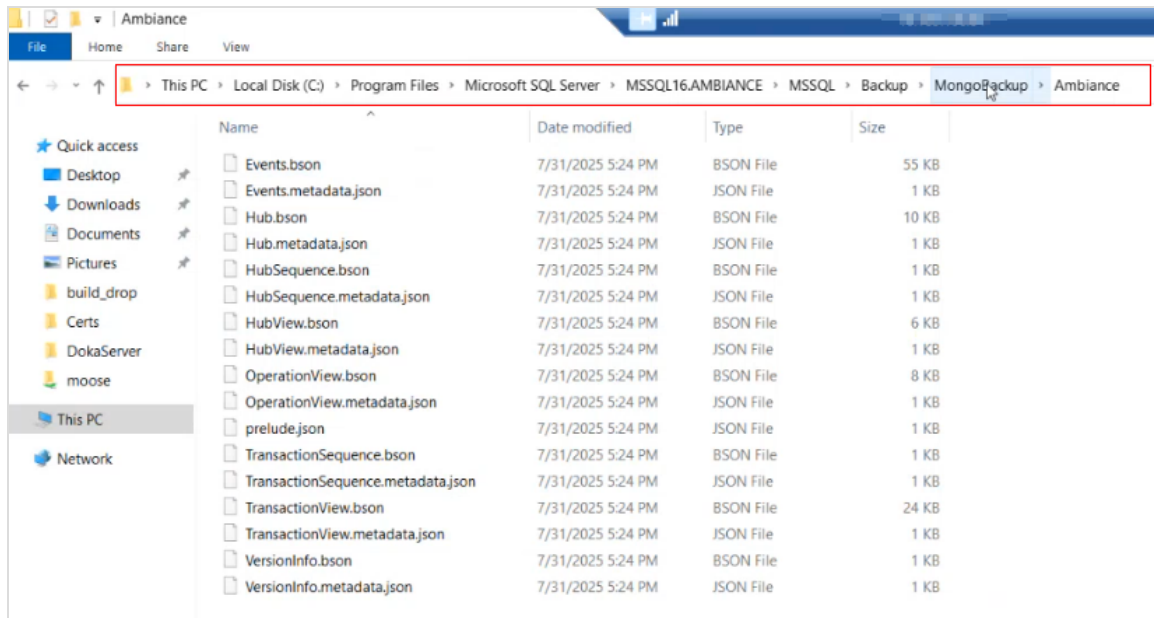
```
*mongod.cfg - Notepad
File Edit Format View Help
# mongod.conf
# for documentation of all options, see:
# http://docs.mongodb.org/manual/reference/configuration-options/
# Where and how to store data.
storage:
  dbPath: C:\Program Files\MongoDB\Server\8.0\data
# where to write logging data.
systemLog:
  destination: file
  logAppend: true
  path: C:\Program Files\MongoDB\Server\8.0\log\mongod.log
# network interfaces
net:
  port: 27017
  bindIp: 127.0.0.1

#processManagement:
security:
  authorization: "disabled"
#operationProfiling:
#replication:
#sharding:
## Enterprise-Only Options:
#auditLog:
```

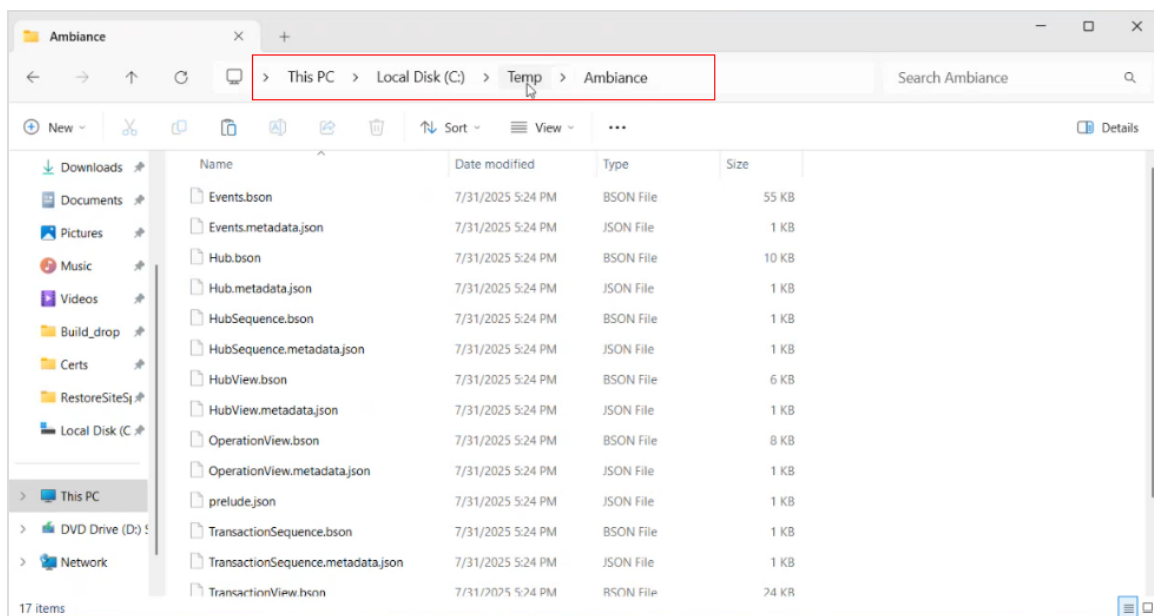
- Restart the MongoDB Server service.



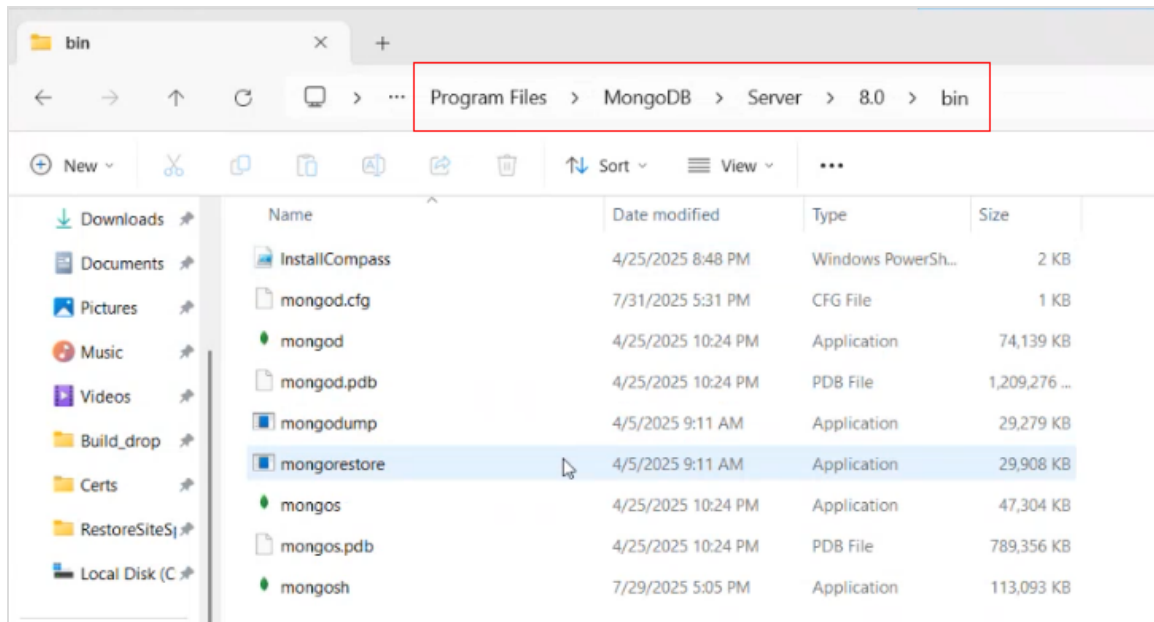
- Retrieve the Mongo backup files. Select the Ambiance|Community folder that contains all of .json files (events).



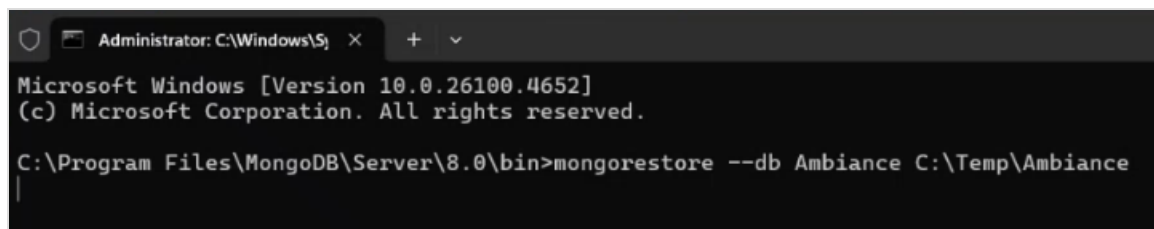
5. Copy files to the new server.



6. Go to the same directory where the configuration file is located.



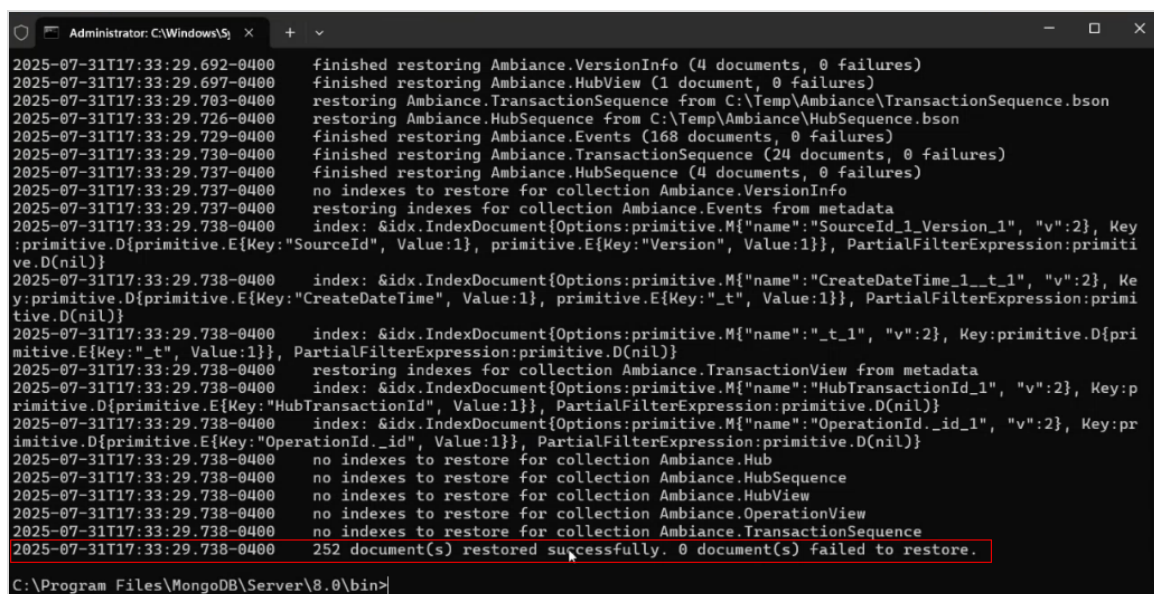
7. In Command Prompt, run the command mongorestore as shown in the following figure. ("C:\Temp\Ambiance" is where the MongoDB backup files were placed on the new server.)



It may be necessary to specify the username and password:

```
c:>Program Files\MongoDB\Server\8.0\bin>mongorestore --username value --password value --db Ambiance C:\Temp\Ambiance
```

8. When the command completes, the message indicates all files were restored successfully.



Verify that all online operations and events display in the Monitoring module.

C.4 Static IP address only. Update IP address

The following steps are required if Ambiance is configured using a static IP address.

1. In Ambiance, go to **System Settings > Online Communication**, update the Server IP address, then click **Save**.
2. Go to **Device Management > Registered Gateways and Paired Access Points**, select all gateways and issue the **Set Communication Settings** command. The new IP address is updated on all gateways.

C.5 Ambiance with polling feature only. Additional configurations

For sites that use the Polling service (LGS REST KF2 API), additional configuration may be required.

Ambiance offers a feature that polls third-party servers to detect requests for mobile keys. The feature requires an SSL certificate. When enabled, the Certificate Manager automatically renews the certificate. Consult the site IT Administration to configure the following polling service settings:

1. On the Ambiance server, go to:
`\dormakaba\AmbianceServer\Services\MobileKeyDeliveryService`.
2. Open the file `MobileKeyDeliveryService.exe.Config`.
3. Specify key values for the certificate:
 - `<add key="PollingServiceCertificateThumbprint" value="customValue" />`
 - `<add key="PollingServiceCertificateIssuerName" value="customValue" />`
4. Specify key values for the polling service URL:
 - `<add key="PollingServiceApiEndpoint" value="customValue" />`
 - `<add key="PollingServiceSiteName" value="customValue" />`
 - `<add key="PollingServiceRequestToken" value="/digitalKeyDetails_MPG" />`
 - `<add key="PollingServiceResponseToken" value="/digitalKeyDetails_MPG" />`
5. Specify the authentication settings for Ambiance to communicate with the polling service:
 - `<add key="PollingServiceMpgUserName" value="customValue" />`
 - `<add key="PollingServiceSecurityToken" value="customValue" />`
 - `<add key="PollingServiceIsSecurityEnabled" value="true" />`
6. Enable the polling service:
 - `<add key="PollingServiceEnabled" value="true" />`
7. Select whether to enable the automatic renewal of the SSL certificate:
 - `<add key="PollingCertificateManagerEnabled" value="true" />`
8. The following key values are read from the certificate thumbprint and auto-populated:
 - `<add key="CertIssuedTo" value="auto_populates" />`
 - `<add key="CertFriendlyName" value="auto_populates" />`
9. Save the file.

C.6 Update Ambiance workstations

On each workstation, use the Service Manager to change/update the current Ambiance server IP address. The Service Manager is located at:

`C:\Program Files\dormakaba\Ambiance\Community Server\Services\Service Manager\ServiceManager.exe`

Alternatively, uninstall and re-install the client on each workstation to ensure all references to the Ambiance server are updated.

C.7 Ambiance only. Update PMS server

The PMS vendor must update the PMS Server with the current Ambiance server IP address.



www.dormakaba.com

dormakaba Canada
105 Marcel-Laurin Blvd
Montreal, Quebec H4N 2M2
Canada
T: +1 877 468-3555

www.dormakaba.com