PHILIPS

dynalite

Multiroom System Manager

IT, Network & Integrations

Version 2.10, 2025-05-21

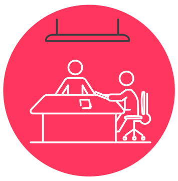
Table of Contents

This section provides an overview of the architecture, requirements, licensing, security, and general setup processes for the Multiroom System Manager deployment in a hotel project.

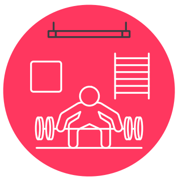
- System Architecture
- System Security
- Server Requirements
- IP Addresses and Ports
- Domain Dependencies
- Integrations
- License Options
- System Readiness

Guestrooms & Suites

Food & Beverage

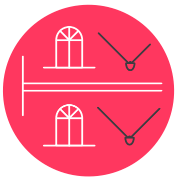


Meetings & Events



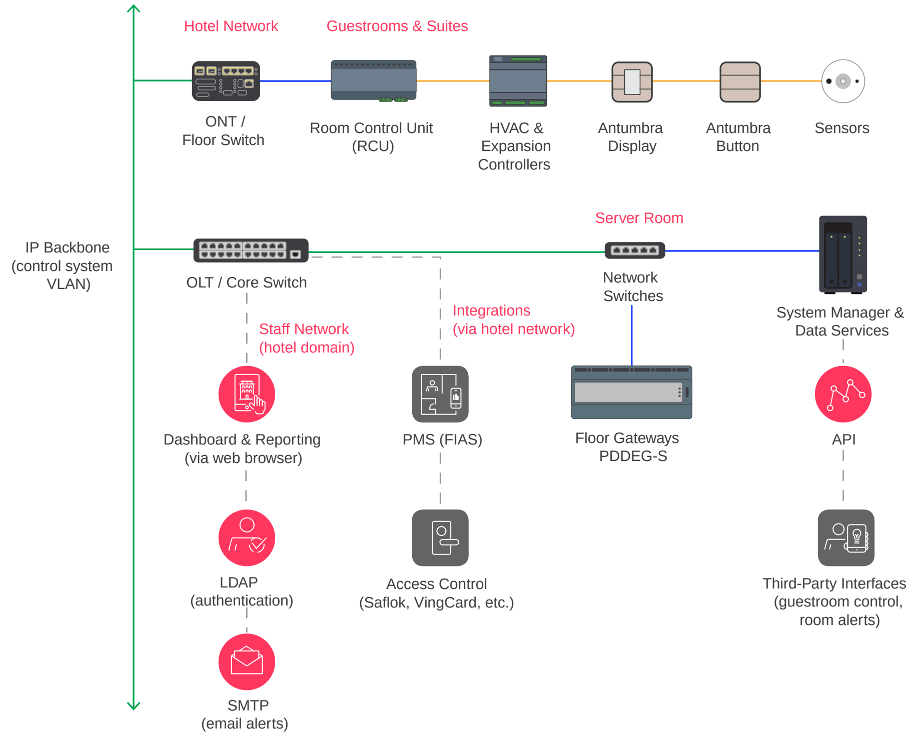
Facilities & Leisure

Common areas



Façade & Landscape

Chapter 1. System Architecture


Hotel Network
Guestrooms & Suites
ONT / Floor Switch
Room Control Unit (RCU)
HVAC & Expansion Controllers
Antumbra Display
Antumbra Button
Sensors
IP Backbone (control system VLAN)
Server Room
OLT / Core Switch
Network Switches
System Manager & Data Services
Staff Network (hotel domain)
Integrations (via hotel network)
Dashboard & Reporting (via web browser)
PMS (FIAS)
Floor Gateways PDDEG-S
API
LDAP (authentication)
Access Control (Saflok, VingCard, etc.)
Third-Party Interfaces (guestroom control, room alerts)
SMTP (email alerts)

Within the guestroom/suite, room control devices connect to a Room Control Unit (RCU) in an RS-485 sub-network.

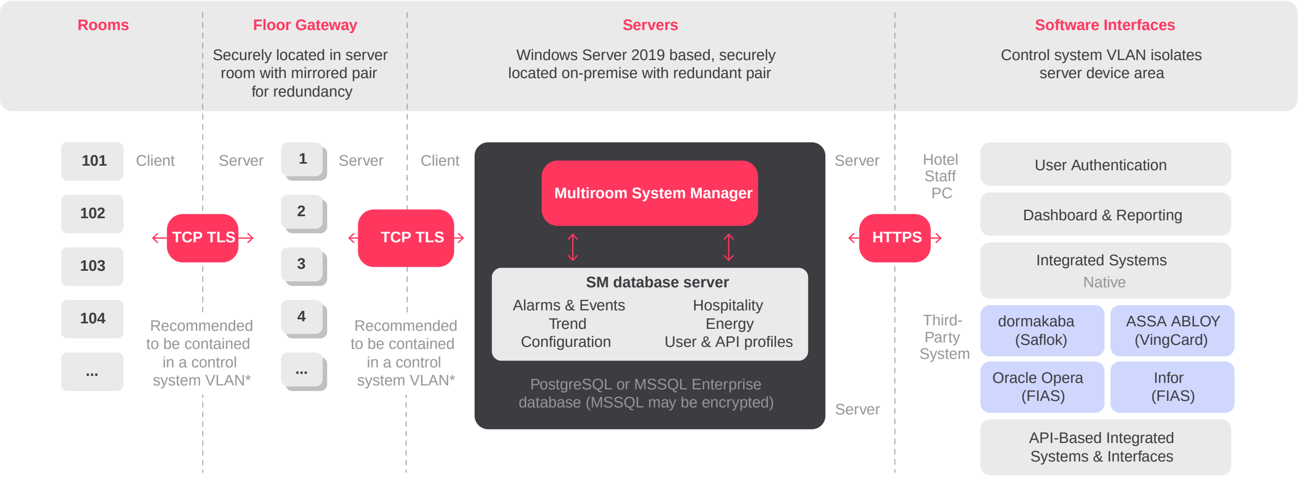
Groups of RCUs then connect via a secure IP connection to a floor Ethernet gateway.

Messages are routed by gateways to the Multiroom System Manager server which integrates with other hospitality systems.

Floor Gateways
One per tower floor - used for routing, filtering, real-time clock, schedules, and network encryption with full redundancy.

— Fibre / IP Backbone
— Ethernet
— DynNet
– – Network Routing

Chapter 2. System Security



Room control units authenticate with floor gateways and encrypt traffic using TLS 1.2. Each device holds the certificate.

System Manager authenticates with floor gateways using a TCP TLS connection.

You must use System Builder to import the Site CA certificate onto the SM server machine and any other machine that is needed to securely access the network. The certificate will be issued by Philips Dynalite with a 25-year period of validity (TLS_RSA_WITH_AES_128_GCM_SHA256, key size of 2KB).

* Network provision to be configured by the hotel IT.

2.1. End-to-End Encryption

- Network traffic is end-to-end encrypted from the room gateways to our on-premise server.
- Our hardware-accelerated guestroom controllers use TLS 1.2 with a 256-bit key to ensure data is protected.

2.2. Room Firewalls

- Our guestroom controllers prevent even the most informed intruder from connecting to other rooms, spaces, or our server.

2.3. Profile-Based Permissions

- Create profiles to easily allocate permissions, granting read-only access or full control per module.
- Restrict or grant users access only to certain parts of the hotel, such as specific floors.

2.4. Secure Interfaces

- Single sign-on enables your team to securely log in with their existing username and password.
- Simple tools help you manage users with ease.

Chapter 3. Server Requirements

For best performance, we recommend using physical servers running Windows Server 2016/2019/2022. If you prefer, our system can be installed onto a Windows Server VM such as Hyper V. The database server may be on the same or another machine.

For large sites we recommend using separate System Manager and database machines, with the MSSQL database option.

Standard **(1-500 rooms)**		**Large** **(500-1500 rooms)**	
Processor	2.7+ GHz, 8+ cores	**Processor**	2.7+ GHz, 16+ cores
Memory	32 GB	**Memory**	32 GB for SM + 32 GB for Database
Hard Disk	1 TB	**Hard Disk**	2 TB

For custom 1500+ room projects, please /GIT/multiroom/build/multiroom/latest/index.html/multiroom/2.10/support.html[contact us] to discuss system requirements.

3.1. Dependencies

When we install the applications, they will include:

- Microsoft SQL Express
- PostgreSQL
- Microsoft .NET Framework

3.2. Licenses

Where required, all licenses except the platform OS are included as part of your Multiroom System Manager license subscription.

3.3. Remote Support

To assist with setup and remote troubleshooting, we request secure remote access such as a VPN and Remote Desktop or TeamViewer.

Chapter 4. IP Addresses and Ports

4.1. IP Address Considerations

Multiroom System Manager is a suite of applications and services hosted by an on-premises server on a VLAN alongside our floor and room control devices. System Manager requires a range of static or dynamic IP addresses, allocated as follows:

Allocation Examples

- 250 rooms across 14 floors would require around 300 IP addresses.
- 1,200 rooms across two 35-floor towers would require around 1,350 addresses

4.1.1. Guestrooms and Suites

- 1 x IP address per unique room number or connected space
- **Recommended:** +5% contingency for future reconfiguration or expansion

Notes

- Only one IP address is required per room number, regardless of type
  (Standard room, presidential suite, villa, etc.)

4.1.2. Floor Network Gateways

- 1 x IP address per whichever is greater:
  - Each unique floor of the building
    OR
  - Each group of 25 rooms
- 1 x IP address for each alternate/redundancy gateway

Notes

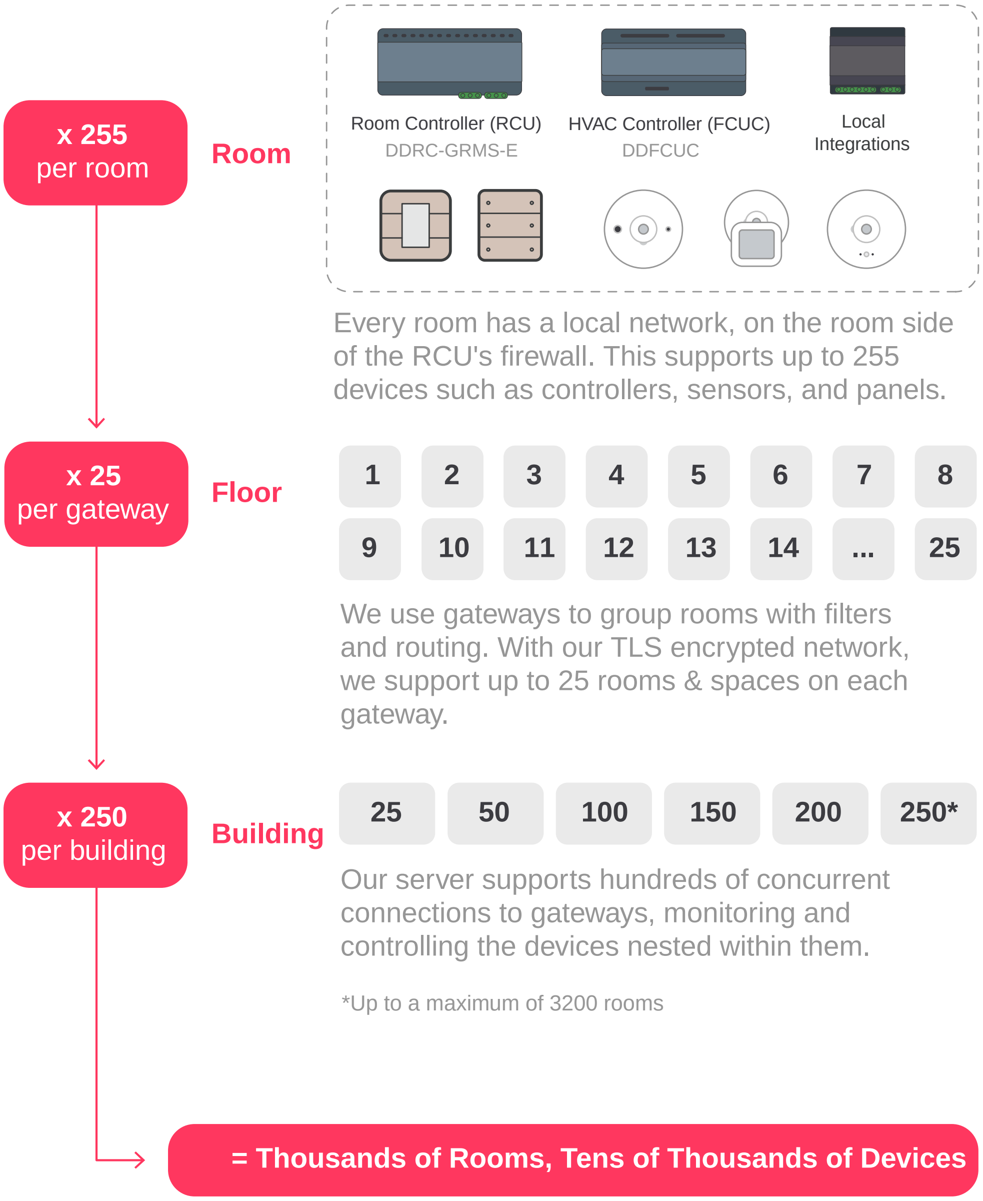
- A unique floor is any floor containing guestrooms.
- In projects with multiple wings or towers, each floor in each wing/tower is considered unique.
- Each floor gateway supports a maximum of 25 guestrooms or suites.
- Although called floor gateways, the devices are located centrally.

4.1.3. Central & Servers

- IP addresses are required for our application and data servers, as well as any backup and redundancy provisions.

Notes

- Depending on the size of the hotel and complexity of the system, we may run the system across multiple servers.
- The IT architecture example in System Architecture approximates a standard (1-500 room) property.
- We recommend that redundancy and backup services are included for each server.



x 255 per room

Room

Room Controller (RCU)
DDRC-GRMS-E

HVAC Controller (FCUC)
DDFCUC

Local Integrations

Every room has a local network, on the room side of the RCU's firewall. This supports up to 255 devices such as controllers, sensors, and panels.

x 25 per gateway

Floor

1 2 3 4 5 6 7 8
9 10 11 12 13 14 ... 25

We use gateways to group rooms with filters and routing. With our TLS encrypted network, we support up to 25 rooms & spaces on each gateway.

x 250 per building

Building

25 50 100 150 200 250*

Our server supports hundreds of concurrent connections to gateways, monitoring and controlling the devices nested within them.

*Up to a maximum of 3200 rooms

= Thousands of Rooms, Tens of Thousands of Devices

4.2. Network Segmentation

Our system comprises of two networks types, connected via each room’s RCU:

- RS-485 room/suite network, connecting up to 255 devices.
- IP trunk network joining all connected rooms, meeting spaces, and public areas to the server for monitoring, control, and integration.

This structure provides several key benefits:

- **Network resilience** - with every room independently operated by its local RCU, network outages do not affect guests.
- **In the event of power loss** - the RCU restores the room to its previous state thanks to local, continuous storage of room state in non-volatile memory.
- **Incredible scalability** - our nested design architecture supports thousands of rooms concurrently connected to our server, each with their own local room network of controller(s), panels, sensors, and inputs.

4.3. Firewall Rule Summary

4.3.1. Core System (Between RCU Devices)

Rooms & Suites <> RCU Gateways

Direction	Client > Host	Port	Connection	Encryption
Bidirectional	RCU > Gateway	50443	TCP/IP	TLS

RCU Gateways <> Interact Server (real-time)

Direction	Client > Host	Port	Connection	Encryption
Bidirectional	Interact Server > Gateway	51443	TCP/IP	TLS

ℹ Port 8734 is required for System Manager connection to the Data Access service and must not be used by any other service. Data Access usually resides on the same server, in which case a firewall rule is not required.

4.3.2. User Authentication and Notifications

Hotel Staff PCs <> Interact Server (Data Services)

Purpose	Direction	Client > Host	Port	Connection	Encryption
Staff accessing dashboards & reporting	Bidirectional	Hotel PC > Interact Server	443	TCP/IP	HTTPS

Interact Server (Data Services) <> Hotel LDAPS Service

Purpose	Direction	Client > Host	Port	Connection	Encryption
Dashboard user authentication	Outbound	Interact Server > LDAPS Server	636 [1]	LDAPS over TCP/IP	SSL

Interact Server (Data Services) <> Hotel SMTP Service

Purpose	Direction	Client > Host	Port	Connection	Encryption
Sending system notifications	Outbound	Interact Server > SMTP service	25, 465, 587[1]	SMTP over TCP/IP	StartTLS Implicit SSL

ℹ API clients with token-based access are restricted to approved data. The administrator can monitor and stop access as required.

4.3.3. System Integrations

Interact Server (real-time) <> Oracle Opera

Purpose	Direction	Client > Host	Port	Connection	Encryption
Synchronize Check-In/Out Events	Bidirectional	Interact Server > Oracle	By Oracle	FIAS over TCP/IP	HTTPS

Interact Server (real-time) <> Infor HMS

Purpose	Direction	Client > Host	Port	Connection	Encryption
Synchronize Check-In/Out Events	Bidirectional	Interact Server > Infor	By Infor	FIAS over TCP/IP	

Interact Server (real-time) <> dormakaba Saflok Messenger LENS

Purpose	Direction	Client > Host	Port	Connection	Encryption
Understand staff or guest occupancy	From Saflok	Saflok > Interact	3270	TCP/IP	

Interact Server (real-time) <> VingCard Visionline

Purpose	Direction	Client > Host	Port	Connection	Encryption
Understand staff or guest occupancy	To VingCard	Interact > VingCard	443 [2]	TCP/IP	HTTPS

[1] Unless otherwise specified by hotel.

[2] When installed on a separate server, you can use port 443. However, it will clash with the Dashboard when on the same machine as the Interact server, so please change to a different port number.

Chapter 5. Domain Dependencies

5.1. Dashboards & Management

5.1.1. Accessing Interact Applications

Why

- The Multiroom Dashboard’s browser-based interface enables hotel staff to serve guests, and monitor and manage the system.

How

- The dashboard and interact APIs are served locally on-premise as a web service, accessible via a domain gateway.
- A firewall rule needs to allow users on the admin network to access the Interact application server, which provides the webservices over HTTPS.
- Only the Multiroom System Manager domain gateway URL is required to be trusted on client PCs and should be added to the network’s DNS to allow staff access.

  `https://myhotel.example.com` is the only address that is externally accessible via the local network. After installation you can find the gateway URL in Windows IIS. This is the URL for all dashboard, API, and WebSocket connections. The gateway then routes requests to the individual APIs, as in the example table below:

Domain	IP:Port	Local/Remote
`https://myhotel.example.com`	`[SM server IP address]:443`	Remote
`https://api.example.com`	`127.0.0.1:443`	Local
`https://usermgmt.example.com`	`127.0.0.1:443`	Local
`https://dashboard-local.example.com`	`127.0.0.1:443`	Local
`https://energyapi.example.com`	`127.0.0.1:443`	Local
`https://dynalitecontrolapi.example.com`	`127.0.0.1:443`	Local
`https://publicapi.example.com`	`127.0.0.1:443`	Local

Requirements checklist

- **Firewall access opened**
  - □ Interact Server <> Staff PCs
  - □ Port 443
- **Authorisation**
  - □ For users to access the dashboard they will need:
    - □ An `@[hoteldomain.com]` user account with valid password (see LDAP (Active Directory)).
    - □ A user profile assigned within the dashboard by an authorised user.
- **Versions**
  - □ We maintain support for modern web browsers including Chrome, Edge, and Firefox.

5.2. LDAP (Active Directory)

5.2.1. User Authentication

Why

- Multiroom System Manager uses LDAP (Active Directory) to allow authorized users to log in with their existing `user@[hoteldomain.com]` username and password.
- This ensures consistent corporate password rule compliance and easy login for staff using the Multiroom Dashboard and reporting tools.
- Within System Manager, each user account is linked to one or more profiles to determine access rights (different modules, read/write permissions, etc.) once they are logged in. These rights and profiles are managed by authorized users.

How

- System Manager requires permission to connect to the hotel's LDAP server (a firewall rule allows connections from the application server).
- System Manager requires its own `user@[hoteldomain.com]` account, authorized to connect to, query, and authenticate users with the LDAP server.

Requirements checklist

- **Firewall access opened**
  - □ SM Server <> LDAP Server
  - □ Port 636 (LDAPS) or 389 (no encryption, StartTLS, or LDAP)
  - □ Interact acts as a client of the LDAP server
- **Authorised User Account**
  - □ `user@[hoteldomain.com]` account.
  - □ Authorisation to access and query the LDAP server to authorise users
  - □ Suggested that the account password does not expire

5.3. SMTP / Email Server

5.3.1. Email Notifications and Alerts

Why

- Multiroom System Manager sends emails to notify when:
  - □ New user accounts are granted access permission.
  - □ Alerts such as room exceptions are detected in rooms or in the system.

How

- System Manager requires permission to connect to the hotel's SMTP server (a firewall rule allows connections from the application server).
- System Manager requires a `user@[hoteldomain.com]` account authorized to connect to and send emails through the SMTP server.

Requirements checklist

- **Firewall access opened**
  - SM Server <> SMTP Server
  - Port 465 (or other if configured differently on the hotel network)
  - SM acts as a client of the SMTP server
- **Authorised User Account**
  - `user@[hoteldomain.com]` account.
  - Authorization to send emails through the SMTP server.
  - Suggested that the account password does not expire.
  - The email account is outbound only, so an out-of-office message can be created to explain that messages will not be read in case any users try to reply to a notification.

Chapter 6. Integrations

6.1. Property Management Systems

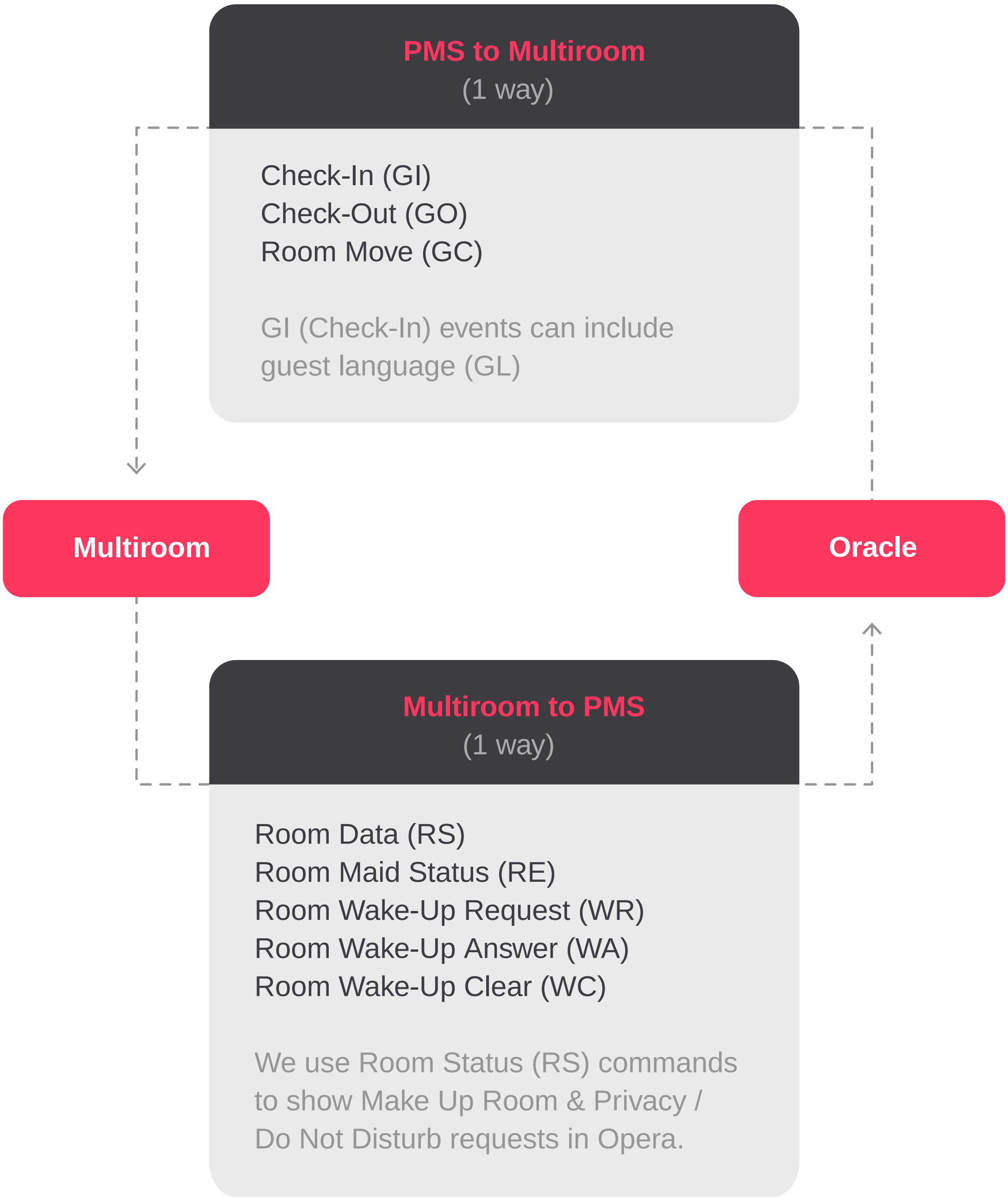
6.1.1. Oracle Opera

Why

- Integrating with Oracle Opera provides System Manager with critical information used in conditioning the room state, such as temperature setpoint, curtain position, power status etc.
- Check-in messages move the room state to condition ready for new guests to arrive.
- Check-out messages reset the room, removing customizations from previous guests such as DND or temperature setpoints, ready for cleaning and the next guest.
- We send Privacy/DND and Make Up Room guest status requests to Opera to make them easily visible to operators assisting guests.

How

- System Manager and Opera integrate over TCP/IP using the FIAS protocol encrypted with TLS 1.2; the firewall needs to allow this.
- From Oracle, you need to order our interface for them to support integration.
- From System Manager, the interface is included and can be simply configured when ready.



PMS to Multiroom
(1 way)

Check-In (GI)
Check-Out (GO)
Room Move (GC)

GI (Check-In) events can include guest language (GL)

Multiroom

Oracle

Multiroom to PMS
(1 way)

Room Data (RS)
Room Maid Status (RE)
Room Wake-Up Request (WR)
Room Wake-Up Answer (WA)
Room Wake-Up Clear (WC)

We use Room Status (RS) commands to show Make Up Room & Privacy / Do Not Disturb requests in Opera.

Data Flow

Requirements Checklist

- **Firewall access opened**
  - □ Real-time server <> Opera Server
  - □ Port to be assigned by Oracle
  - □ System Manager acts as a client of Opera
  - □ Certificate can be installed to provide a secure connection
- **Order the Interface**
  - □ FIAS connectivity is included as standard with Multiroom System Manager, but you need to purchase an interface on the Opera side.

  - Contact your Oracle representative to order our interface, quoting product ID (FKT): **IFC_PDH / FIAS_PDH**

- **Versions**
  - The integration is tested to be compatible with Oracle Opera v5 or later.

Certification

Architecture STR, powered by Philips Dynalite, is a 'Validated Integration' as certified by Oracle. You can verify our status on their website: https://www.oracle.com/us/partnerships/isv/ds-philips-dynalite-4414287.pdf

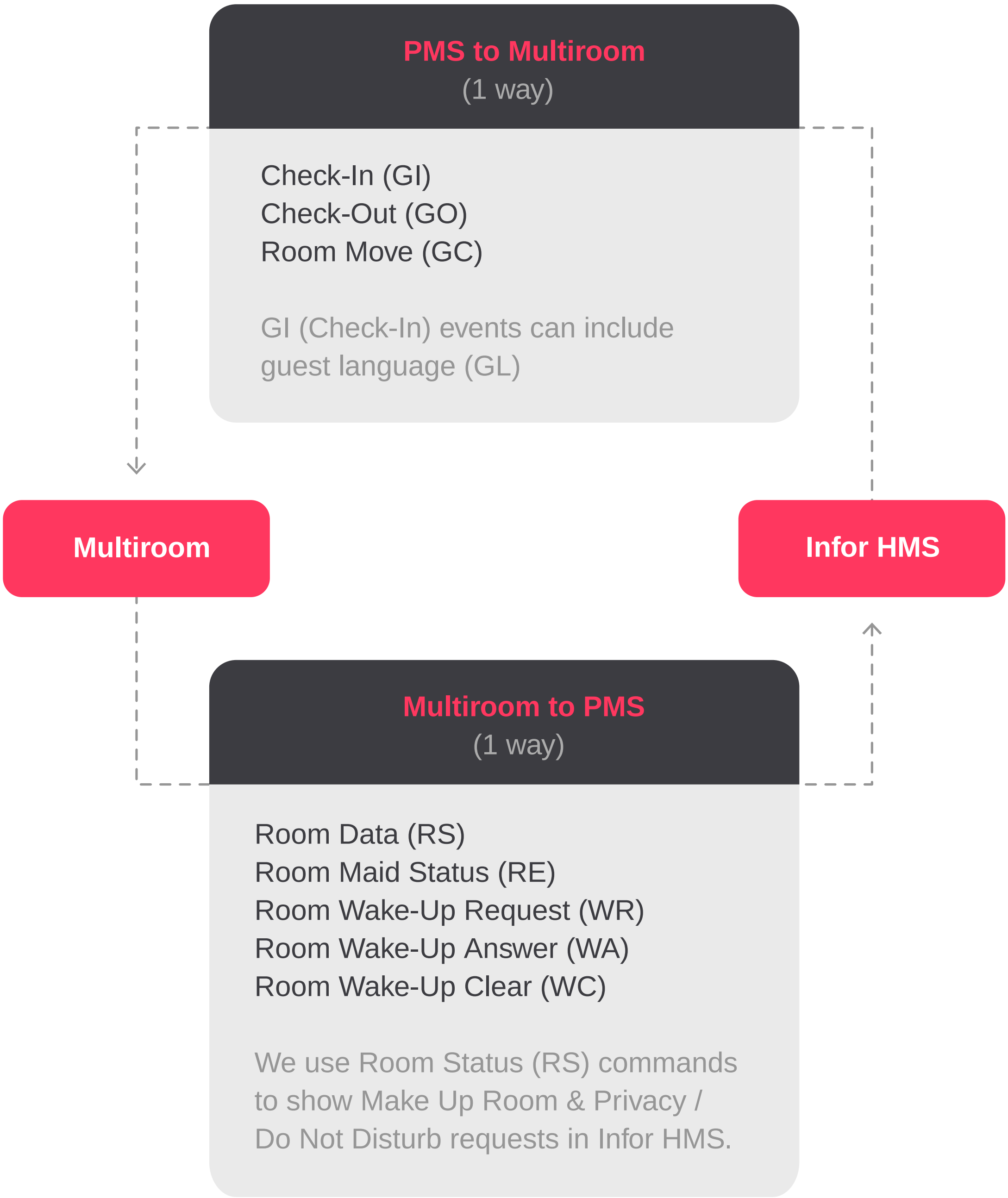
6.1.2. Infor HMS

Why

- Integrating with Infor HMS provides System Manager with critical information used in conditioning the room state, such as temperature setpoint, curtain position, power status, etc.
- Check-in messages move the room state to condition ready for new guests to arrive.
- Check-out messages reset the room, removing customizations from previous guests such as DND or a temperature setpoint, ready for cleaning and the next guest.
- We send Privacy/DND and Make Up Room guest status requests to Infor to make them easily visible to operators assisting guests.

How

- System Manager and Infor integrate over TCP/IP using the FIAS protocol; the firewall needs to allow this.
- You need to order our interface from Infor for them to support integration.
- From System Manager, the interface is included and can be simply configured when ready.



PMS to Multiroom
(1 way)

Check-In (GI)
Check-Out (GO)
Room Move (GC)

GI (Check-In) events can include guest language (GL)

Multiroom

Infor HMS

Multiroom to PMS
(1 way)

Room Data (RS)
Room Maid Status (RE)
Room Wake-Up Request (WR)
Room Wake-Up Answer (WA)
Room Wake-Up Clear (WC)

We use Room Status (RS) commands to show Make Up Room & Privacy / Do Not Disturb requests in Infor HMS.

Data Flow

Requirements Checklist

- **Firewall access opened**
  - □ System Manager Server <> Infor Server
  - □ Port to be assigned by Infor
  - □ System Manager acts as a client of Infor
- **Order the Interface**
  - □ FIAS connectivity is included as standard with System Manager, but you need to purchase an interface on the Infor side.
  - □ Contact your Infor representative to order our interface, quoting their SKU: **HMS-EAI-L066DT-**

EMS.

Certification

Architecture STR, powered by Philips Dynalite, is a 'Certified Integration' as certified by Infor.

6.2. Access Control

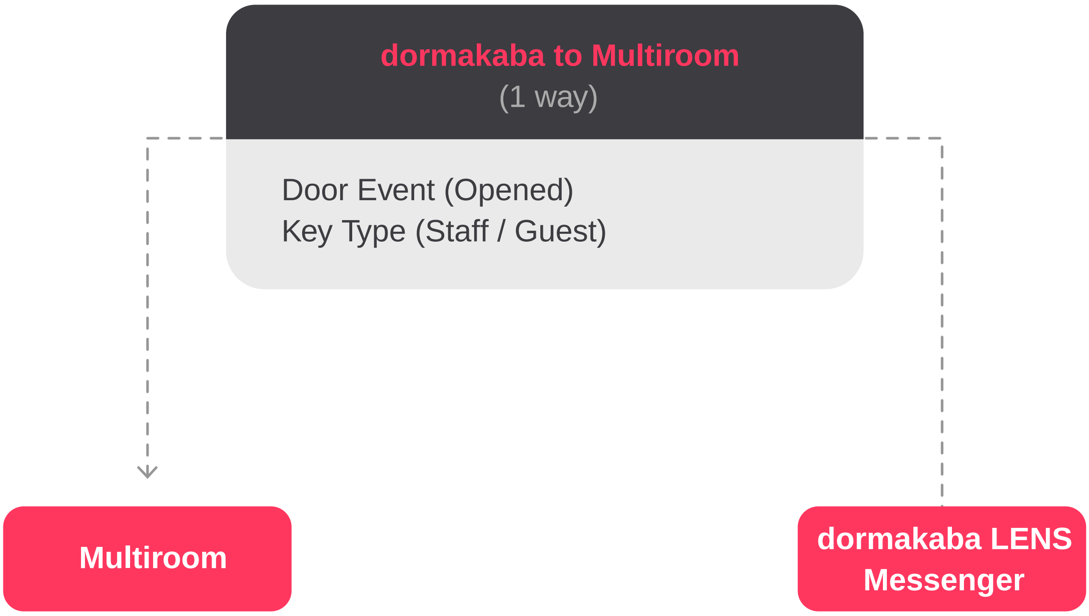
6.2.1. dormakaba – Saflok

Why

- By connecting to the Access Control server, the system can be made aware of occupancy type based on the key type used to enter the room.
- This means that, as well as real-time occupancy, we know if it’s a guest or staff member in the room.
- By knowing this we can condition the room differently for staff, such as brighter lighting to help inspection, as well as disregarding any changes they make from guest preferences such as temperature setpoint.
- We can also save energy by using a shorter timeout after staff occupancy compared to guest occupancy.

How

- System Manager subscribes to the APIs shared on dormakaba’s Saflok Messenger LENS server.
- Upon room entry, they send us an event that includes the guest/staff key type.



dormakaba to Multiroom
(1 way)

Door Event (Opened)
Key Type (Staff / Guest)

Multiroom

dormakaba LENS Messenger

Data Flow

Requirements Checklist

- **Firewall access opened**
  - □ System Manager Server <> dormakaba Messenger LENS Server
  - □ Port to be assigned by dormakaba

    - System Manager acts as a client of dormakaba
- **Credentials**
    - You will need to authorize dormakaba to issue credentials for us to authenticate when connecting to their server.

Certification

Architecture STR has been tested and certified by dormakaba as an approved integration. You can contact them to verify our status via: https://www.dormakaba.com

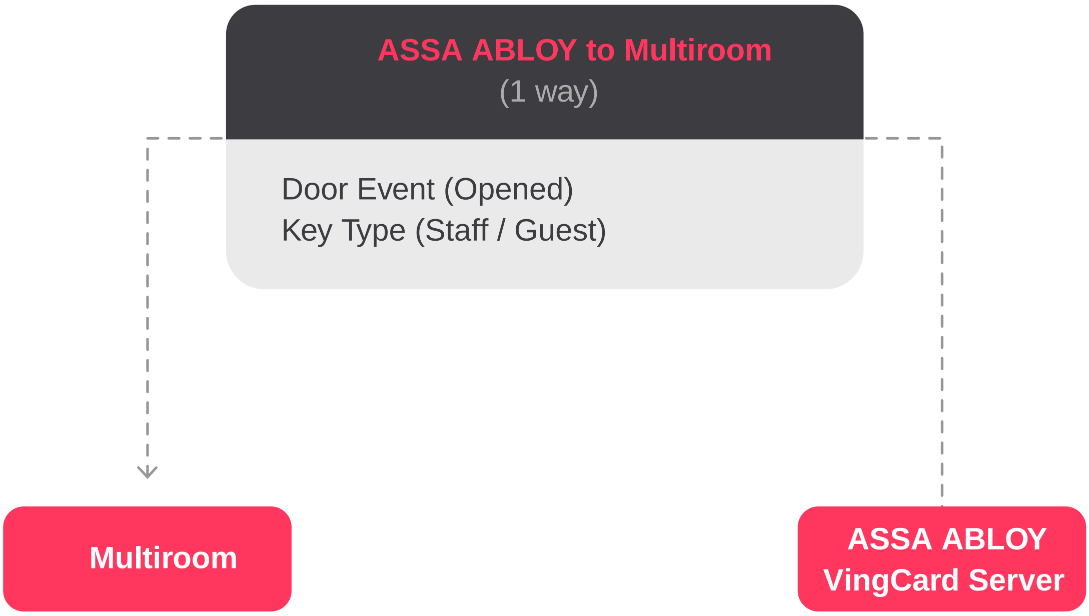
6.2.2. ASSA ABLOY (VingCard)

Why

- By connecting System Manager to the Access Control server, the Interact system can be aware of occupancy type based on the key type used to enter the room.
- This means that, as well as real-time occupancy, we know if it's a guest or a staff member in the room.
- By knowing this we can condition the room differently for staff, such as brighter lighting to help inspection, as well as disregarding any changes they make from guest preferences such as temperature setpoint.
- We can also save energy by using shorter timeouts after staff occupancy compared to guest occupancy.

How

- System Manager subscribes to the APIs shared on the ASSA ABLOY VingCard server.
- Upon room entry, VingCard sends us an event that includes the guest/staff key type.



Encrypted Data Flow

Requirements Checklist

- **Firewall access opened**
    - Real-time server <> VingCard Server

    - Port to be assigned by ASSA ABLOY (do not use 443)
    - System Manager acts as a client of ASSA ABLOY

- **Credentials**
    - You will need to authorize ASSA ABLOY to issue credentials for us to authenticate when connecting to their server.

Certification

Architecture STR has been tested and certified by ASSA ABLOY as an approved VingCard integration.

6.3. API Connections

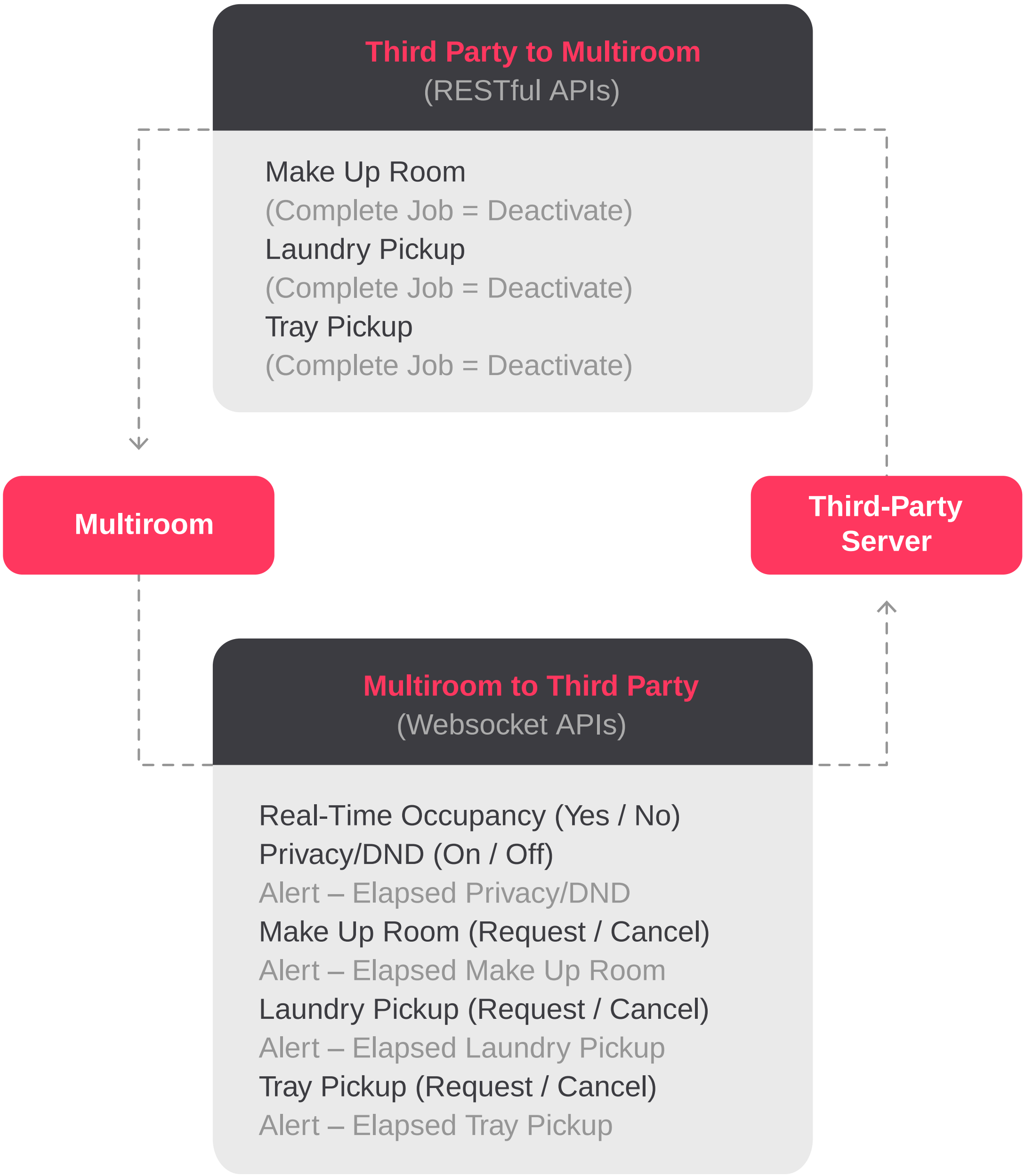
6.3.1. Housekeeping, Job Dispatch, and Guest Apps

Why

- Interact can share guest requests such as Laundry Pickup with third-party systems to aid them in delivering guest services. These can be automatically deployed in their system to a runner near to the room for fast response times, automatically clearing the room status when the job is marked as complete.
- Interact can share statuses such as real-time occupancy, Privacy/DND and Make Up Room requests. These are used in third-party systems to dynamically reprioritize housekeeper task allocations, optimizing efficiency by going first to rushed or vacant rooms.
- In addition, some third-party systems accept room alerts to help dispatch runners that can support verifying occurrences of extended Privacy/DND status (e.g. over 48 hours) to ensure guest safety.
- Third-party developers can create guest apps, enabling guests to control services in their room from a phone or tablet.

How

- Third-party systems often have custom interfaces and business logic based on the Hotel Integration API.
- These can be activated by the third-party system once firewall rules are enabled to allow communication.
- Refer to the Interact Developer Portal for more information.



Third Party to Multiroom
(RESTful APIs)

Make Up Room
(Complete Job = Deactivate)
Laundry Pickup
(Complete Job = Deactivate)
Tray Pickup
(Complete Job = Deactivate)

Multiroom

Third-Party Server

Multiroom to Third Party
(Websocket APIs)

Real-Time Occupancy (Yes / No)
Privacy/DND (On / Off)
Alert – Elapsed Privacy/DND
Make Up Room (Request / Cancel)
Alert – Elapsed Make Up Room
Laundry Pickup (Request / Cancel)
Alert – Elapsed Laundry Pickup
Tray Pickup (Request / Cancel)
Alert – Elapsed Tray Pickup

Encrypted Data Flow

Requirements Checklist

- **Firewall access opened**
  - □ Real-time server <> Third-party server
  - □ Port 3260
  - □ Third-party server acts as a client of System Manager
- **Credentials**
  - □ We will issue API credentials to third-party integrator for onsite integration.

Certification

Interact has tested and certified a number of API-based third-party integrators as 'Works with Architecture STR'.

Chapter 7. License Options

7.1. Three Feature Tiers

Freedom to upgrade anytime:

- Local control of lighting, HVAC, power, curtains & statuses
- Local button & display interfaces

Foundation
No Management System Software

- Network-ready - connect for integration in the future

Advanced adds central real-time visibility, management, and integration:

Real-time remote visibility and control of the whole hotel

Proactive monitoring and alerts of statuses, services, and environment

Native integrations for PMS & Access Control, APIs to connect an ecosystem of apps and systems

Self-management & update tools

Advanced
€15/room/year

- Annual onsite health check and software updates
- Access to online support and training

Enterprise brings rich historical data access:

Energy consumption data for lighting, power, and HVAC across all your connected spaces

Rich historical reporting to better understand guest behaviors, service, and performance

'Per Stay' report cards provide a summary of the services, energy, and conditions during a stay

Real-time diagnostic data to help with HVAC and other maintenance

Enterprise
€25/room/year

- Annual onsite health check and software updates
- Access to online support and training

7.2. Detailed Software Feature Matrix

		Advanced	Enterprise
Central Visibility & Control	Real-time visibility and control of all rooms, suites, and public areas	✓	✓
	Scheduling visibility and management for public areas	✓	✓
Proactive Room Alerts	Dashboard alerts for exceptions such as device offline, elapsed status, high temp, etc.	✓	✓
	Proactive email alerts for configurable room alerts	✓	✓
Reporting	Historical reporting		✓
	Energy reporting		✓
	Custom report builder		✓
	Data export – select and export room historical data	✓	✓
Maintenance	Self-management tools to update room defaults	✓	✓
	DALI light point monitoring and pairing tools	✓	✓

		Advanced	Enterprise
Integrations	**PMS (Property Management System) integration - Oracle Opera, Infor, Amadeus, Oasis**	✓	✓
	Access Control System (doorlock) integration - Saflok, VingCard	✓	✓
	API for operational integration - FCS, Messagebox, Knowcross	✓	✓
	API for guest app integration – Tapendium, Hudini, Digivalet, UIB, hotel apps	✓	✓
IT & Security	**End-to-end TLS network encryption**	✓	✓
	Single sign-on user authentication (LDAP/S)	✓	✓
	Profile-based user permissions and floor access	✓	✓

7.3. License notes

Multiroom System Manager licenses provide access to powerful software and integration features:

- Continuous software updates to bring new features and improvements.
- Unlimited users (staff members).
- Supports single sign-on via LDAP/S (Active Directory) and email notifications (SMTP required) for user management and room alerts.

> - License fees are based on number of rooms, license duration, and feature tier – our partner or your account manager may have included this upfront or as part of a lifecycle package.
> - The API (with features matching the license model) can be activated upon request at no extra cost.
> - Software update eligibility is throughout the licensed period; updates are self-installed unless otherwise included in a lifecycle package.
> - You can renew your license at any time to restore/extend access to updates and historical features.

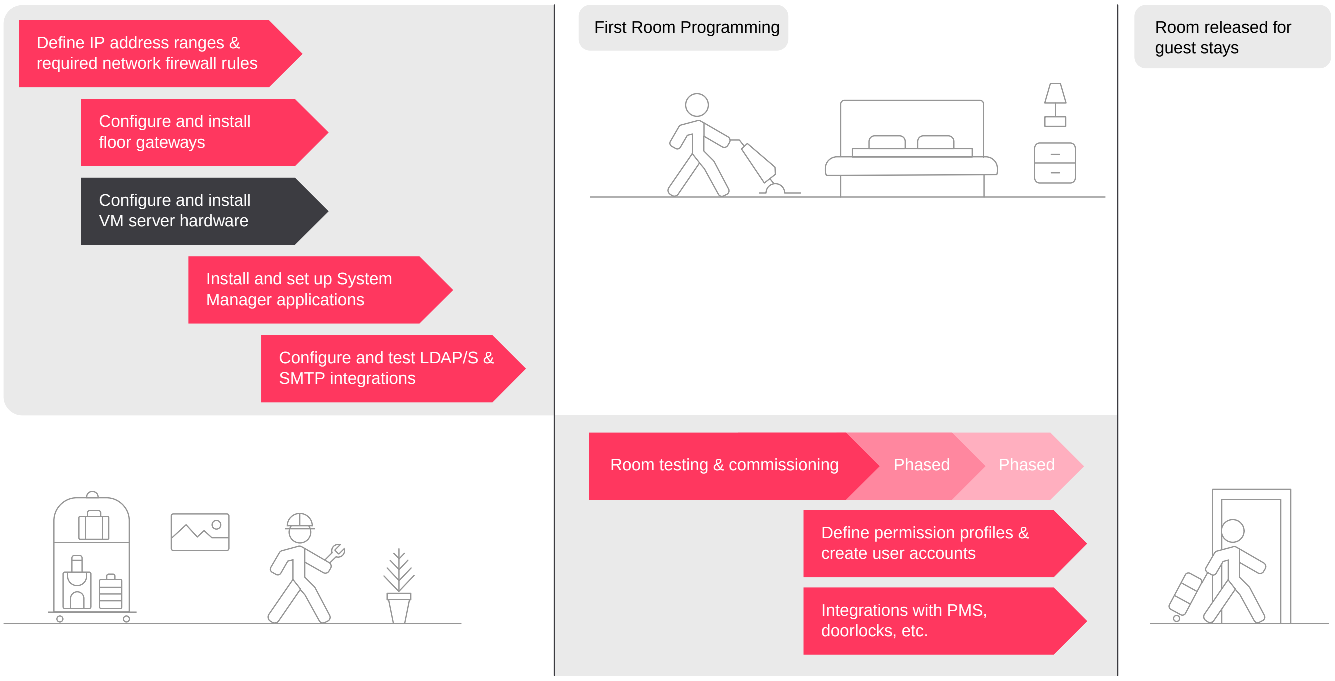
Upon installation, all features are available to trial for 30 days for up to 10 rooms.

If you do not renew your license:

- Real-time features including the dashboard and integrations will continue to work.
- You will lose access to updates and technical support.
- Users will see messaging periodically to notify them that the license has expired.
- If we provide your SSL Certificates, they will no longer be renewed upon expiry.

Chapter 8. System Readiness

8.1. IT Setup Flow



Define IP address ranges & required network firewall rules

Configure and install floor gateways

Configure and install VM server hardware

Install and set up System Manager applications

Configure and test LDAP/S & SMTP integrations

First Room Programming

Room testing & commissioning

Phased

Phased

Define permission profiles & create user accounts

Integrations with PMS, doorlocks, etc.

Room released for guest stays

8.2. IT Checklist

Hardware

- System Manager (SM) application Server and OS installed with local administrator access to the application server for installation
  - If required, redundancy and/or backup arrangements
- Network gateways and switches with sufficient ports and spare rack space to install our floor gateways alongside the server

Network Provisioning

- IP addresses in the quantity required
- Controls VLAN from rooms to the server and floor gateways

Functional Accounts & Interfaces

- Order PMS/HMS interface, set date for SM to connect
- LDAP/S (Query & Authenticate) authorized user
- SMTP (Send email) authorized user

Firewall Rules

- **SM Application Server <> Staff PCs:**
  - Port 443, SM acts as client
- **SM Application Server <> LDAP/S Server:**

  - Port 636 (LDAPS) or 389 (no encryption, StartTLS, LDAP), SM acts as client

- **SM Application Server <> PMS Server Interface:**
  - PMS vendor to advise port, SM acts as client
- **SM Application Server <> Doorlock Server Interface:**
  - Doorlock vendor to advise port. SM acts as server for Saflok and client for VingCard (do not use port 443)
- **SM Application Server <> API Integrations:**
  - Port 443, integration acts as client to SM