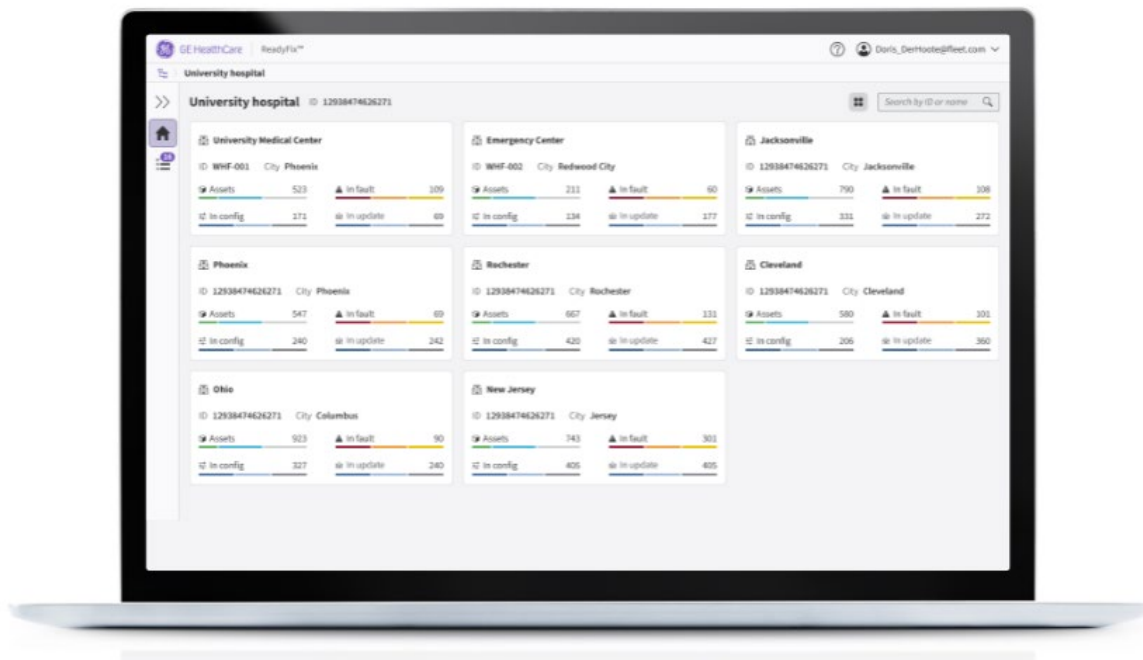


ReadyFix™

Implementation guide



Note: Images are illustrative examples only. Actual products and their features may vary based on configurations.

ReadyFix remote fleet management

ReadyFix is a cloud-based remote fleet management solution intended to simplify the operation and maintenance of compatible GE HealthCare devices. By remotely accessing real-time device data, you can proactively manage your asset, improve standardization, and help reduce interruptions to patient care.

This guide is intended to provide a detailed overview of the key process steps, resources, and critical items required for the delivery and installation of ReadyFix within your hospital network. It is designed to facilitate a seamless implementation by outlining the necessary preparations and coordination efforts.

Please use this guide in conjunction with the other GE HealthCare technical documents, which include the following:

- ReadyFix User Manual
- ReadyFix Gateway Service Manual

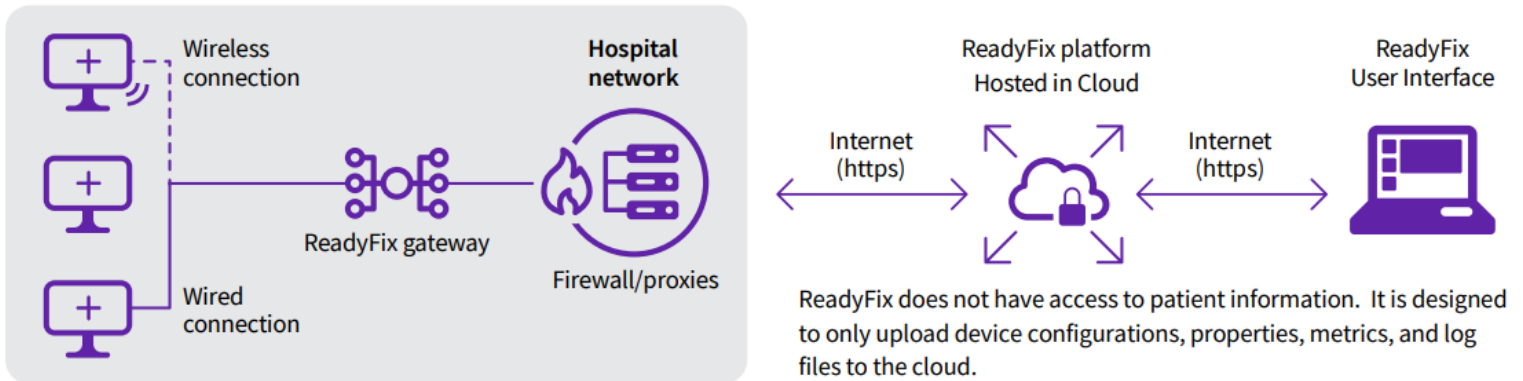
Your GE HealthCare project manager will provide these documents in advance of the project kick-off meeting or as requested.

Overview

ReadyFix is designed to:

- Gain visibility into real-time device data for proactive asset management
- Deploy standardized clinical or technical configurations, by care area or department
- Control firmware and software updates by care setting, pushing either immediately or on a schedule
- Retrieve logs and identify faults for advanced troubleshooting

ReadyFix Architecture – typical production deployment



ReadyFix leverages capabilities on smart devices to securely communicate to a central location in near-real time via a lightweight Internet of Things protocol. The device can share its properties and sensor data, including out-of-range data identified as 'faults', for users to proactively identify issues with the devices and minimize interruptions to clinical staff. Users of the ReadyFix application can share standardized configurations across multiple devices remotely or restore a previous configuration to a device. ReadyFix users can also see applicable firmware and software updates that are entitled to that device, and they can push or schedule a coordinated update to one or more devices.

Benefits of ReadyFix Gateway

The ReadyFix gateway is an optional component and offers enhanced data management, reducing overall traffic by localizing data processing. It facilitates secure communication and interoperability among devices and streamlines device connectivity and management. Standard configuration of ReadyFix includes the installation of a Gateway to provide full ReadyFix functionality. If a gateway is unable to be installed at a customer site, compatible devices may be directly connected to ReadyFix.

Privacy and Security

Key architecture & design influences for ReadyFix include NIST 800-53 and GE HealthCare Design Engineering Privacy & Security Procedure. Key features include

- Transport layer outbound TLS/HTTPS connections
- Mutual TLS (mTLS) between device and cloud
- Encryption standard FIPS 140-2 level 1
- ReadyFix uses X.509 certificates for device authentication, valid for one year. Certificate renewal is fully automated, ensuring continuous security with no manual effort required.
- User authentication and authorization with GE HealthCare IDAM. Federated authentication with your identity provider is configurable.

Technical requirements

Environments

ReadyFix is hosted by GE HealthCare in the cloud on Amazon Web Services (AWS) along with an on-premise ReadyFix Gateway installed in Customer Datacenter.

Network requirements

The device or gateway must be able to reach the GE HealthCare ReadyFix Application via the internet. ReadyFix is compatible with HTTP proxies with basic authentication. The ReadyFix solution, including both direct device connections, gateway connections initiates https connections to domains listed below. The customer is responsible for the allowing these domains and outbound network connectivity within the firewall.

Port	Protocol	Direction	Purpose	Source IP/Subnet	Destination IP/Subnet	Internet
443	HTTPS	Outbound	Communication between GE HealthCare Device and ReadyFix	GE HealthCare Device hostname/IP	See the below table for GE HealthCare Cloud URLs	✓
443	MQTT	Outbound	Communication between GE HealthCare Device and ReadyFix	GE HealthCare Device hostname/IP	See the below table for GE HealthCare Cloud URLs	✓

Direct Device Connection:

- [https:// ge-hc-prod.sac.keyscaler.io/](https://ge-hc-prod.sac.keyscaler.io/)
- [https:// pki-api.gehealthcare.com/](https://pki-api.gehealthcare.com/)
- [https:// readyfix-api.gehealthcare.com/](https://readyfix-api.gehealthcare.com/)
- <https://download.flexnetoperations.com/>
- *-us-east-1-api-iot-mtls.gehealthcare.com
- *-us-east-1-iot.gehealthcare.com
- *.iot.us-east-1.amazonaws.com
- *.data-ats.iot.us-east-1.amazonaws.com
- *-us-east-1.s3.us-east-1.amazonaws.com

Connection through ReadyFix Gateway:

In addition to the above domains, whitelisting of below 3 domains is required for Gateway connections:

- <https://gehpcps.ee-us.gehc-pcs.spectrocloud.com/>
- <https://idam.gehealthcloud.com/>
- *.dkr.ecr.us-east-1.amazonaws.com

Remote Access

Upon completing the device connection to ReadyFix, trained GE HealthCare users will have access to ReadyFix to view devices and pull log files. Remote initiation of any change, such as a configuration or software update, requires an open Service Record activity assigned to that GE HealthCare user. Tunneling is not allowed in ReadyFix, and GE HealthCare does not have access to view or update the ReadyFix Gateway remotely.

Disaster recovery

If the application becomes compromised and is not available in the primary region, the application will be hosted by the secondary region with RTO & RPO target < 24 hours. ReadyFix URLs would typically remain unchanged in the disaster recovery.

ReadyFix Gateway

ReadyFix Gateway is an optional component that is installed at the organization's data center. It utilizes the infrastructure provided by the customer site and the software is provided by GE HealthCare via Flexnet and Spectro Cloud.

Virtual Infrastructure requirements

ReadyFix Gateway requires vSphere™ Enterprise version 7.x or higher. Below are the minimum system requirements for the virtual machine configuration

- 8 Core CPU
- 64 GB RAM
- 512 GB Storage

Other pre-requisites to VM creation are:

- One static IP address

Patches/Upgrades

ReadyFix Gateway updates occur at a scheduled downtime and are triggered manually (remote). This activity is a collaboration between the Hospital IT and GE HealthCare service teams.

ReadyFix implementation project steps and teams

ReadyFix Implementation consists of four phases:

1. Whitelisting and network configuration
2. GE HealthCare IDAM onboarding
3. Installation of ReadyFix Gateway application on-site to streamline communication and help maximize security
4. Connecting compatible devices – follow device instructions to connect each compatible device to the ReadyFix application

The following table of customer and GE HealthCare team members outlines the roles and the corresponding responsibilities that are needed for a successful ReadyFix implementation. These resources will work together to plan, schedule, identify resources, and complete key steps to install and configure the product.

Hospital project team members	
Roles	Responsibilities
Project manager	Lead contact for GE HealthCare ReadyFix Project Manager; provide communication and coordination of hospital project team; responsible for project planning, timeline, and task management for all implementation activities; ensure all specifications meet the ReadyFix requirements, and coordinate resources for go-live support.
Network / infrastructure	Responsible for the design and configuring networking, firewall configuration to support ReadyFix; configuring vSphere and responsible for installation of ReadyFix Gateway
IT Security manager / Risk Approval Liaison	Responsible for overseeing the operations of the enterprise's security solutions through policy, architecture, and training processes of the organization, applying the security solutions to vendor applications. Ensure the documentation process meets the QA/Risk Management requirements for the hospital.
Bio-medical /clinical technology	Manages all biomedical devices; serves as liaison between IT and clinical to ensure proper setup of MAC VU360, and overall clinical project setup.
Super users	Assist with staff training; support staff during implementation and Go Live; serve as a resource to staff on unit for assistance and questions; provide basic troubleshooting; assist with testing prior to implementation.
Identity provider specialists	Responsible for onboarding ReadyFix into the hospital's Identity Management system, if hospital is using their own IAM for user authentication. A Client Admin role is assigned at onboarding to continue to manage users during lifecycle of the product.

GE HealthCare core project team members	
Term	Responsibilities
Sales specialist	Primary contact for demonstrating and representing the ReadyFix system and providing system design and quotation information.
Project manager	Primary point of contact; develops project plan with customer project manager; ensures milestones are achieved per plan; supervises and coordinates all phases of implementation; acts as liaison for ReadyFix team; responsible for timely communication of project status and issues; on-site visits based on the time and materials stated in quote.
Cloud onboarding operations	Responsible for configuring IDAM to the customer's Identity Provider, configure Cloud monitoring.

Acronyms, abbreviations, and definitions

Term	Definition
AWS	Amazon Web Services
GEHC	GE HealthCare
VM	Virtual Machine
CPU	Central Processing Unit
Mbps	Megabits per second
GB	Gigabyte
NIC	Network Interface Card
DHCP	Dynamic Host Configuration Protocol
IP	Internet Protocol
IDAM	Identity Access and Management

