INSTALLATION AND OPERATION MANUAL

Ascom Unite Connect for Clinical Systems

ascom

About this document

This document describes the installation and configuration of Connect for Clinical Systems. This manual also describes the configuration and administration of Workflows and activities related to specific alarm or event access rights for the users.

How to use this Document

The document is mainly intended for Ascom installation personnel and a local administrator for normal system maintenance.

CH | REP   Ascom (Solution) AG, Gewerbepark Hintermättlistrasse, 5506 MÄGENWIL, Switzerland

CE
2460

Manufacturer

Ascom (Sweden) AB

Grimbodalen 2

SE-417 49 Göteborg

Sweden

Phone +46 31 55 94 00

www.ascom.com

Abbreviations and Glossary

Alarm	State of the alarm system when it has determined that a potential or actual hazardous situation exists for which operator awareness or response is required; sent from source devices and received by Connect for Clinical Systems for processing and distributing as notifications/alerts.
Alert	Alert message from equipment such as patient monitors and nurse call systems.
C4CS	Connect for Clinical Systems A software application installed on a Windows server environment capable of acquiring alarms, events, parameters, and waveforms from clinical systems, and forwarding that information as alerts to designated display devices.
Event Manager	A component of Connect for Clinical Systems that triggers events, manages indication and redirection for those events.
ICU	Intensive Care Unit
Interactive Message	A message sent from Connect for Clinical Systems to a handset, requesting a response from the use.
Handset	Any type of Ascom handset or pager.
RabbitMQ	RabbitMQ is the most widely deployed open source message broker.
UPS	An Uninterruptible Power Supply can be used for maintaining a continuous supply of electrical power in case the normal power supply fails.
Unite	Name of Ascom IP-based protocol for handling events and messages, messages, and alarms.
Unite Admin	An interface enabling configuration and administration of the software.
Unite Assign	An interface enabling users to dynamically assign alerts to recipients.
Unite CM	Unite Connectivity Manager in an Elise3 Module or a virtual environment.
Unite PS	Unite Platform Server A server that handles communication interfaces, message routing, activity logging, administration of systems, and other essential messaging services. It is a software-only product installed on a Windows server.
UNS	Unite Name Server Contains the number plan that translates the numbers used by the users and applications to destination addresses.

Contents

1 Introduction

This manual provides information required to install and configure Connect for Clinical Systems. For additional information and technical assistance, please contact your Ascom service representative. This current version applies to software version 8.10 of Connect for Clinical Systems.

> **Caution**
>
> A general understanding of the features and functions of Connect for Clinical Systems and its components is a prerequisite for the proper use of this equipment. Do not operate this equipment before reading these instructions thoroughly, including all appropriate warnings and cautions.

Connect for Clinical Systems is a software application installed in a Windows server environment capable of acquiring alarms, events, parameters and waveforms from clinical systems and forwarding that information as notifications to designated display devices.

Connect for Clinical Systems operates within the Ascom Unite Messaging Suite for Healthcare suite of software applications.

Connect for Clinical Systems utilizes Unite Assign as an interface enabling users to dynamically assign alerts to recipients.

Connect for Clinical Systems relies on the Unite Admin client as an interface enabling configuration and administration of the software.

> **Caution**
>
> US Federal and Canadian law restricts this device to sale by or on the order of a licensed medical practitioner.

Connect for Clinical Systems is installed on specified hardware in healthcare facilities in critical care units, sub-intensive units, general wards and other departments and relies on the proper use and operation of connected medical devices, systems, display devices and the medical IT network. It is used by nursing staff with relevant education, background and training who can interpret the data from clinical systems and apply it towards effective patient care.

1.1 Vigilance and reporting incidents

End users, or resellers / distributors must inform Ascom in writing, within five (5) business days from knowledge of an event, of all incidents relating to the Products. A complaint in this instance may be an oral or written statement or insinuation that the Product fails to meet requirements with respect to identity, quality, durability, reliability, safety, effectiveness, or performance of a device.

> Any serious incident, that is any incident that directly or indirectly led, might have led or might lead to the death of a patient, user or other person, the temporary or permanent serious deterioration of a patient's, user's or other person's state of health or a serious public health threat, that has occurred in relation to the Product should be reported to the manufacturer, via email to vigilance@ascom.com, and the competent authority of the Member State in which the user and/or patient is established.

For any serious incident, or if there is a perceived Product malfunction that could contribute to death or injury, or if a customer expresses concern about patient safety, then end users or resellers / distributors will notify Ascom as soon as possible using best efforts to provide such notice orally (Ascom Technical Assistance Center) within twenty-four (24) hours of gaining knowledge, or from the receipt of such

complaint, or becoming aware of such Product issue. Oral notification shall be followed with written (email) confirmation within 24 hours to vigilance@ascom.com.

End users or resellers / distributors will provide sufficient information to allow Ascom to fulfil its regulatory reporting obligations for incidents and events that must be reported and registered according to national regulations within the Territory. If an event is considered to be an incident which must be reported to National Competent Authorities, then Ascom shall prepare and submit a report.

If any regulatory body or competent authority provides written notice to an end user, or reseller / distributor with respect to inquiries about, or investigations of any Product, or to conduct an inspection or audit of facilities used for the storage of Products, or request any information related to the any Product, then end user, or reseller / distributor shall promptly notify Ascom.

1.2 Warnings, Cautions and Notes

Please read and adhere to all Warnings, Cautions and Notes listed throughout this manual.

Depending on the characteristics of the connected medical devices, Connect for Clinical Systems can be used for primary (DAS/CDAS) or secondary (DIS) notification of alarms. The presence of a single DIS device makes the full system secondary. In this case the user shall handle the entire system as secondary and he/she will not rely upon that system.

1.2.1 Definitions

Warning

Outlines items that if not followed, may result in death or serious injury to the patient or damage to the equipment.

Caution

Alerts the user that special care should be taken for the safe and effective use of the device.

Provides additional general information.

1.2.2 Summary of Warnings and Cautions

Warning

Acceptance testing must be performed for each location supported by this product. Failure to complete acceptance testing may result in failed or delayed notification, resulting in potential patient harm. Functional verification of the products should occur before the product is used in a clinical environment with a live patient. Additionally, this testing should be repeated after any changes to the configuration or system upgrades.

Warning

This product provides methods to temporarily suppress alerting and redirection for the duration of a silenced alarm and (optionally) for the duration of all active alarms after they are silenced on the patient monitor. Failure to take into account operation of the silence feature of the monitor by unqualified or un-trained personal may lead to improper delays and/or suppression of notifications leading to potential patient harm.

Caution

The product does not provide operator configuration for conditions or settings. All configurations and settings must be done during implementation of the product and should be documented and agreed upon with clinical staff within the organization before the product is put into use.

Caution

It can take up to two seconds between the alarm generation and the alarm sending on the Digistat Suite. The Digistat Suite then waits for an acknowledgement from the Product. If such acknowledgement is not received within two seconds a timeout occurs. Therefore, the maximum delay after which an alarm notification is provided is 4 seconds. If there is a timeout:

   A connection alarm is triggered. The alarm can be canceled by the user. It is also canceled if a new connection with Confirmed Delivery is established.

   Digistat Suite data sending and Confirmed Delivery is stopped until a new connection is established. If Digistat Suite is not in Reliable state, it immediately attempts to restore connection without Confirmed Delivery.

Caution

The Product must be installed and configured by specifically trained and authorized personnel. This includes Ascom staff and any other person specifically trained and authorized by Ascom. Similarly, maintenance interventions and repairs on the Product must be performed according to Ascom guidelines only by Ascom personnel or another person specifically trained and authorized by Ascom.

Caution

The healthcare organization shall implement internal procedures in order to always ensure the presence of at least one clinical staff member near redundant systems that can be implemented through Desktop workstations or alarm light towers.

Caution

In case Connect for Clinical Systems is used for the primary notification of alarms, redundant systems shall be implemented through Desktop workstations or alarm light towers.

Caution

It is the responsibility of the healthcare organization using Connect for Clinical Systems to define an emergency procedure to put into effect in case of system unavailability. This is necessary to:

Make it possible for the departments to keep on working.

Restore as soon as possible the system to full availability (back-up policy is part of this management).

Caution

The Product has been verified and validated during installation or upgrade phase and its acceptance testing has been performed on the hardware (PC, server, mobile devices) and software (e.g. operating system) together with other software components (e.g. browser, antivirus, etc.) already present. Any other hardware or software installed may compromise the safety, effectiveness and design controls of the Product.
It is mandatory to consult an authorized Ascom before using together with the Product any other software than those validated in the installation or upgrade phase.
If any other software (utilities or applications programs) on the hardware on which the Product runs needs to be installed, healthcare organization shall inform Ascom for further validation. It is suggested to apply a permission policy that prevents users from performing procedures such as the installation of new software.

Caution

If the local network is at least partially based on WiFi connections, given the possible intermittency of the WiFi connection, network disconnections are possible, that cause the activation of the "Recovery or Disconnected Mode" which in case the product is used for primary notification of alarms, can cause system unreliability. The Healthcare Organization shall ensure an optimal network coverage and stability, and train the users, in the management of these temporary disconnections.

Caution

It is recommended for the healthcare organization using the Product to stipulate a maintenance contract with Ascom or an authorized Distributor.

Caution

To ensure compatibility with the product software, use only approved components and third-party software that conforms to Ascom specifications, to install, operate, use, service and/or repair any part of the product. Use of incompatible software, medical systems and display devices, accessories, components, or cables may render the product unsuitable for its intended use.

Caution

Incorrect settings or silencing of display devices can jeopardize the performance of the system.

Caution

Operators should check that the current notification events and assignments are appropriate prior to use of this product with patients.

Caution

Incorrectly setting the volume of a display device, used in conjuncture with this product, below that of the ambient environment may lead to missed notifications and jeopardize the performance of the system.

Caution

For proper operation, ensure appropriate function of each device's display before each use.

Caution

Mobile display devices are wireless devices and may be subject to intermittent signal dropout. A crowded wireless environment or interference from other wireless devices, either intentional or unintentional, may result in a significantly increased amount of signal dropout experienced by any one or multiple wireless device(s).

Caution

Only compatible display devices, capable of supporting the outlined minimum characteristics and communication protocols included in this manual, may be used with the product.

Caution

Only compatible medical systems, capable of supporting the outlined communication protocols included in this manual, may be used with the product.

Caution

Changes or modifications not expressly approved by Ascom (Sweden) AB could void the user's authority to operate the equipment.

Caution

Other systems distributing information on the same messaging system can impact the overall messaging capacity of Connect for Clinical Systems.

Caution

Ascom may make available updates of the product software. Failure to apply updates when so advised may result in impaired performance or safety of the product, or exposure to security vulnerabilities.

Caution

A general understanding of the features and functions of Connect for Clinical Systems and its components is a prerequisite for the proper use of this equipment. Do not operate this equipment before reading these instructions thoroughly, including all appropriate warnings and cautions.

Caution

US Federal and Canadian law restricts this device to sale by or on the order of a licensed medical practitioner.

Caution

This product is designed to be connected, and to communicate information and data via a medical IT network. It is the sole responsibility of the user organization to design, install, operate, supervise, monitor, maintain and service the medical IT network in such ways that are adequate to preserve the safety, effectiveness and security of the medical IT network and its connected devices and systems.

Caution

If duplicate conditions are entered (i.e., ICU|BED3 and ICU|BED3 for separate Unite locations) only one of those locations is recognized and used to identify where the triggered events occurred.

Caution

Operation of the product without adequate consideration of filtering can negatively impact performance and adoption of the product.

Caution

Operation of the product without adequate consideration for the impact of frequent alarm updates, which may occur as a result of an improperly configured medical device, can negatively affect performance and adoption of the product.

Caution

Special consideration must be paid to the configuration of Filters and triggers that involve more than one care unit. Failure to take into account the configuration for all care areas may result in improper delays and/or suppression of notifications leading to potential patient harm.

Caution

Proper installation of the product includes configuration of the Unite supervision node and Unite fault handler to inform responsible individuals of failures in the notification systems that may be preventing alerts from being received by the intended recipient.

1.3   Intended Use/Purpose

The intended use/purpose of the Ascom Unite Connect for Clinical Systems is to provide an interface with clinical systems to forward information associated to the particular event to the designated display device(s).

For medical, near real time alarms, Connect for Clinical Systems is intended to serve as a parallel, redundant, forwarding mechanism to inform healthcare professionals of particular medical related events.

Connect for Clinical Systems does not alter the behavior of the primary medical devices and associated alarm annunciations. The display device provides a visual, and/or audio and/or vibrating mechanism upon receipt of the alert.

Connect for Clinical Systems is intended for use as a secondary alarm. It does not replace the primary alarm function on the monitor.

Intended Purpose (EU/EFTA/UK/AUS)

The intended purpose of the Ascom Unite Connect for Clinical Systems is to provide an interface with clinical systems to forward information, including vital physiological parameters, associated with particular events to designated display device(s) in order to support monitoring of patients. The display device(s) provide(s) a visual, and/or audio and/or vibrating mechanism upon receipt of alert(s).

Connect for Clinical Systems applies configurable processing and filtering to event notifications, reducing their frequency and number, in order to present clinically actionable information to healthcare professionals.

For medical, near real time alarms, Connect for Clinical Systems is intended for use as a secondary alarm, i. e. a parallel, redundant, forwarding mechanism to inform healthcare professionals of particular medical related events.

For selected source devices and systems, Connect for Clinical Systems acts as integrator and communicator of a Distributed Alarm System (DAS/CDAS) to reliably forward and deliver physiological and technical alarms to healthcare professionals on designated display devices and to specified systems.

Connect for Clinical Systems is indicated for use with specified medical devices by healthcare professionals whenever there is a need for monitoring the physiological parameters of patients. The patient population and patient conditions are established by the connected medical devices.

Connect for Clinical Systems is installed on specified IT-systems and relies on the proper use and operation of connected medical devices, systems, display devices and the medical IT network.

Connect for Clinical Systems is used in healthcare facilities, in critical care units, sub-intensive units, general wards and other departments and, depending on the specific configuration, when outside the healthcare facility.

1.3.1 Clinical Benefits to be Expected

- Reduces the risk of missing critical patient alerts.
- Helps reduce alarm fatigue by decreasing the number of patient alert messages received by caregivers.
- Helps improve response time to critical patient events.
- Contributes to workflow effectiveness by avoiding unnecessary work interruptions.
- Provides near-real time indication of system status to users.[1]

1.4 Software Device Identification

Information on all mandatory and optional items contained in the software label are described in Medical Device Software Label. The software label can be found under the Infrastructure tab by clicking into the system name. Below is a default layout. Symbols and their meanings are described below in 1.4.1 Symbols and Descriptions, page 8.

---

1. This claim may ONLY be made for the Class IIb system (Unite Connect for Clinical Systems, Unite View, Unite Axess for Smart Devices).

1.4.1 Symbols and Descriptions

In the SW "About" File	Title of Symbol	Description
CE 2460	CE mark	Indicates that the conformity of the device with the provisions of Council Directive 93/42/EEC of 14 June 1993 and Regulation 2017/745 of the European Parliament and of the Council concerning medical devices to enable it to move freely within the Community and to be put into service in accordance with its intended purpose.
MD	Medical Device	Indicates that the item is a medical device
▲▲▲	Manufacturer	Indicates the medical device manufacturer, including address and telephone number.
∿	Date of manufacture	Indicates the date when the medical device was manufactured
REF	Catalogue number	Indicates the manufacturer's catalogue number so that the medical device can be identified.
📖i	Consult instructions for use	Indicates the need for the user to consult the instructions for use.

In the SW "About" File	Title of Symbol	Description
⚠	Caution	Indicates the need for the user to consult the instructions for use for important cautionary information such as warnings and precautions that cannot, for a variety of reasons, be presented on the medical device itself.
Rx only	Prescription device	Caution: Federal law restricts this device to sale by or on the order of a licensed medical practitioner.
UDI	Unique Device Identifier	Indicates a Unique Device Identifier that adequately identifies a device through its distribution and use.

1.5   Hardware Requirements

These requirements refer to the physical operating environment required for adequate operation of the application. In order to support the simultaneous operation of multiple installations, these requirements (RAM, Disc space, etc.) will need to be increased for each additional installation instance.

RAM	32 GB (16 GB Minimum).
Processor	64-bit processor: 3 GHz, 4 cores.
Disk Space	100GB (50 GB Min) (recommended free disk space for the installation).
Connections	TCP/IP base Local Area Network Connection.

1.6   Software Requirements

Operating System	Windows® Server 2016. Windows® Server 2019. Windows® Server 2022. Windows Server Essentials 2019 (Small Footprint Unite deployments only).
Web Server	IIS 7.5.

Database	SQL Server 2016 Enterprise or Standard.
	SQL Server 2017 Enterprise or Standard.
	SQL Server 2019 Enterprise or Standard.
	SQL Server 2022 Enterprise or Standard.
	SQL Server 2019 Express (Small Footprint Unite).
Messaging Platform	Unite Platform Server 4.19 and higher.
	All installation instances of C4CS must be co-located on the same server where Unite PS is already installed.
Framework	.NET Framework 4.8
	ASP.NET Core 6.0 Runtime Windows Hosting Bundle
Message broker	RabbitMQ v3.10
	RabbitMQ v3.11
	RabbitMQ v3.12
	Use Erlang/OTP as recommended by RabbitMQ.

Use of the Dräger Infinity WinAcces requires Microsoft Visual C++ redistributable 2010 x86 (bundled with installer) and use of the teleCARE IP driver requires Microsoft Visual C++ redistributable 2015-2019 x86 (bundled with installer).

1.7 Time Settings

It is recommended that the system is connected to an Internet time server for synchronization on this and all endpoints.

1.8 Technical Support

For technical assistance, please contact your Ascom service representative.

1.9 Supported Clinical System Device Inputs

Connect for Clinical Systems is designed to accept inputs from a variety of clinical systems utilizing standardized and proprietary protocols including the following:

Compatible Sources for Distributed Information Systems (DIS)	
Spacelabs XprezzNet Gateway	
Versions	XprezzNet Gateway v1.3.5.
Monitors	qube, XPREZZON, and Ultraview SL 2400, 2600, 2800 bedside monitors.

Dräger Infinity Gateway	
Versions	Dräger Infinity Gateway VF7.2 and VF9.0.1
Monitors	M540, M300, Infinity Delta and Delta XL
GE CARESCAPE Unity	
Versions	Unity version 0 and 1.
Monitors	Dash 3/4/5000, Solar 9500, Solar 8000M/I, ApexPro, CDT-LAN, GE DINAMAP PRO 1000, Eagle 3000, Eagle 4000, Solar 7_8000, Tramscope, Unity Network ID, Dash 2000, Octoacomm, CARESCAPE Monitor Bx50, Dash 2500, B20 V1 Monitor, B40 V1 Monitor, B40 V2 Monitor.
Ascom Digistat Connect	
Versions	7.0.0 or later
Ascom teleCARE IP Nurse Call	
Versions	NISM 7.0.3 and up, NIGW 2.0.0 and up. vNISM 3.1.0.
Ascom Telligence Nurse Call	
Versions	6.2 and higher
Compatible Sources for Distributed Alarm Systems (DAS) & Distributed Alarm Systems with Confirmation (CDAS)	
Ascom Digistat Suite	
Versions	7.0.0 or later and corresponding DAS certified drivers. Please see Digistat DAS Driver Compatiblity information provided with Digistat Care product. For specific information related to the functionality and requirements related to Digistat please review the Digistat Care User Manual.

1.10 Supported Display Devices

Compatible Communicators for Distributed Information Systems (DIS)	
Unite Axess For Smart Devices (Android)	
Version	v5.1.0 or later
Unite Axess For Smart Devices (iOS)	
Version	v6.0.0 or later
Unite View	

Versions	v4.6.0 or later
Ascom Smart Device Alert Handling Software for Myco	
Versions	14.3.0 or later
Ascom DECT/WiFi devices	
Versions	All currently supported and maintained Ascom devices, according to product life cycle plan, until end of repair.
Compatible Communicators for Distributed Alarm Systems (DAS) & Distributed Alarm Systems with Confirmation (CDAS)	
Unite Axess For Smart Devices (Android)	
Versions	v6.2.0 or later.
Unite Axess For Smart Devices (iOS)	
Versions	v6.2.0 or later
Supported Display Devices for Non-Medical System	
Any device capable of receiving messages from Ascom Unite PS	

For additional details on specific system compatibility and functionality refer to the Connect for Clinical Systems, Data Sheet, TD 93252EN and Appendix A Clinical System Protocols, page 121.

1.11 Download the Connect for Clinical Systems Software

Download the Connect for Clinical Systems software from the Ascom Software & License Portal.

1.11.1 Validate Downloaded Software File

The Release Notes for the software includes an MD5 checksum that can be used to validate that the downloaded file has not been changed.

1. Calculate an MD5 checksum of the downloaded file. See Calculating an MD5 checksum in Windows, page 12.

2. Compare the calculated MD5 checksum with the checksum shown in the Release Notes. If something is wrong with the file, the MD5 checksum will not be equal to the one in the Release Notes.

Calculating an MD5 checksum in Windows

1. Open the **Command Prompt**. Click the Search charm, enter `cmd` into the text box and press **Enter**.

2. Enter `certutil –hashfile <filename> MD5 >> MD5.txt`

3. Press **Enter**. The MD5 checksum is written to the file "MD5.txt".

2   Deployment Considerations

> **Caution**
>
> This product is designed to be connected, and to communicate information and data via a medical IT network. It is the sole responsibility of the user organization to design, install, operate, supervise, monitor, maintain and service the medical IT network in such ways that are adequate to preserve the safety, effectiveness and security of the medical IT network and its connected devices and systems.

After the completion of validation and data ports are established, the user organization must establish and maintain appropriate security measures including, but not limited to:

- Network firewalls.
- Authentication and access control systems.
- Encryption of data.
- Installation of antivirus (malware) protection.
- Data backup.
- Security logging and event monitoring

This will ensure consistency of operation and will protect the medical IT network configuration and its connected devices and systems against security breaches, unauthorized access, interference, intrusion, leakage, theft and/or loss of data or information.

2.1   Assumed Knowledge

You should have a fundamental understanding of the required Microsoft Windows Server Operating Systems, Microsoft Windows Internet Information Services (IIS), Microsoft Windows SQL Server concepts, along with fundamental firewall, security, and networking knowledge. The configuration also requires knowledge about Ascom professional messaging.

2.2   Alternative Working Procedure

- The healthcare organization shall define alternative working procedures in case the system becomes unreliable or stops functioning.
- The healthcare organization shall implement adequate procedures to bring Connect for Clinical Systems back to its functionality in the shortest time possible.

> **Caution**
>
> It is responsibility of the healthcare organization using Connect for Clinical Systems to define an emergency procedure to put into effect in case of system unavailability. This is necessary to:
>
> Restore as soon as possible the system to full availability (back-up policy is part of this management).
>
> Make it possible for the departments to keep on working.

2.3   Deployment Requirements

Connect for Clinical systems is software application intended to be installed and operated within a Windows Server environment. The supported validation version of the Windows operating systems compatible with

Connect for Clinical Systems are listed specifically in the previous Software Requirements section and within the Connect for Clinical Systems, Data Sheet, TD 93252EN.

In addition to providing the requisite environment for the software to operate, Connect for Clinical Systems relies on a number of other dependencies to facilitate the delivery of alerts to display devices. These dependencies include connectivity, with read and write permissions, to a database (hosted locally or remotely), and access to a number of auxiliary services distributed, installed, and maintained by the Ascom Unite Platform Server (Unite PS).

Due to certain constraints related to the configuration of the Connect for Clinical System (C4CS), C4CS must be installed and operated on the same server as a Unite Platform Server. Since certain auxiliary services of the Unite Platform Server are required during installation, the Unite Platform Server MUST be installed on the server before Connect for Clinical systems can be installed.

Any changes made to the alarm source should be evaluated to determine if the changes will affect the alert flow.

After completion of validation, the following should remain consistent.

- Data ports

- Firewall configuration

> For any system upgrade (for example, SQL server), components must be verified as compatible.

> Various patches are currently supported. However, some patches (i.e., Rabbit MQ and SQL server) require reverification, and upgrading must not be performed prior to consulting with the manufacturer.

2.4   Maintenance

Connect for Clinical Systems is not a self-monitored system. Prior to installing, the following must be verified as adequate for the operating environment:

- Available disk space.

- RAM and CPU capacity.

The system must be regularly administrated and monitored. Maintenance of the main software server (i.e., to ensure adequate hardware space) must include the dependent servers (e.g., the runtime server and the SQL server) in order to meet optimal performance.

2.5   High Availability Deployment Architecture

Connect for Clinical System offers a number of deployment models in order to meet the specific reliability and operational requirements of the customer's desired environment. These models involve different system architecture options which can significantly impact the deployment requirements.

The principal goal of this section is to describe the various models that may be employed during the design and implementation stages of Connect for Clinical Systems.

Each one of the models proposed in this section are described as a method to minimize and/or mitigate the impact of unscheduled and/or unplanned downtime. The various models described in this section are done with the intention of providing solutions to a wide range of requirements that may be placed on the performance of the product in an individual environment.

2.5.1 High Availability (Cluster Deployment)

The High Availability Clustered Deployment model involves the separate installation of multiple instances of Connect for Clinical Systems on separate nodes (physical servers) operating simultaneously as a "cluster", where all nodes participate in the processing of alarms, events, and alerts so that if any one of the nodes is intentionally or unintentionally removed (due to hardware failure or maintenance) from the cluster, that there is minimal interruption in operation of the complete solution.

In order to fully realize this concept, it is recommended that there are no less than three nodes operating in the Connect for Clinical System/Unite Platform Systems cluster and that a common database is installed and operating remotely in a separate cluster dedicated exclusively for the database.

Additional requirements related to the deployment of this High Availability model are incorporated and maintained within the Pre-configuration of Windows for Unite Applications, Configuration Notes, TD 92993EN.
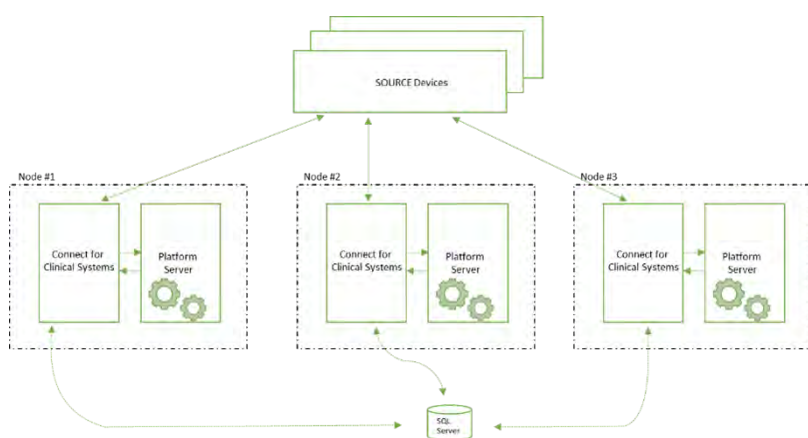
2.6 Small Footprint Unite (SFU) Deployment

For smaller facilities, Connect for Clinical Systems can be installed, configured and operated in an SFU deployment with a single teleCARE or Telligence integration using Windows Server Essentials 2019 and SQL Server 2019 Express. In an SFU deployment, certain hardware specifications and capacity limits are reduced to ensure that SFU deployments have the same performance as other Unite deployments.

For more details see 1.6 Software Requirements, page 9, 7.6 Nurse Call, page 115, teleCARE IP Nurse Call, page 123 and Telligence Nurse Call, page 123.

2.7 Data Management

As noted in the previous section. Connect for Clinical Systems relies on the availability and access to a database for the purpose of operational as well as configuration functions. The availability of the database can be supported in a number of ways, including installing the database locally on the same server as Connect for Clinical System and the Unite Platform Server, or remotely on a separate server.

Although the local method can sometimes provide a simpler deployment architecture and requires less infrastructure, a remote deployment is always recommended.

This recommendation is due to the benefits of data being physically separated from the application environment. This physical separation promotes the use of best practices related to data storage (e.g. RAID, routine schedule backups, data redundancy, UPS, etc.) and represents the first step in offering a reliable and scalable solution.

Connect for Clinical Systems does not manage or contain Protected Health Information (PHI).

2.7.1   Backup and Restoration

In the case of deployment of the Connect for Clinical Systems utilizing a local database, regular backups (manual or automated) of C4CS databases are recommended as a simple means to preserve the configuration and minimize the downtime of the Connect for Clinical Solutions as a result of any hardware failure that may occur. This database itself can be backed up and restored using standard SQL Server Management tools.

In the event of an application environment host failure, another standby virtual/physical machine can be provisioned and with the addition of the restoration of a recent backup of the database, the solution can be restored to a fully functional state.

Backup & Restore is the more lightweight technique recommended for Connect for Clinical System to minimize and mitigate downtime. This lightweight approach to availability lends itself well to smaller IT installations, where an acceptable minimum downtime of 15 minutes or more, involving manual restorations and re-deployment techniques, are acceptable.

In deployments utilizing a remote database, regular backups of data may not be necessary, if this was already considered in the overall IT infrastructure maintenance plan. However, by separating areas of concerns it should only be necessary to consider the restoration or redeployment of either the application OR the data environment, but not both.

2.7.2   High Availability (VMWare HA)

The VMWare High Availability (HA) solution refers to the pooling of VMs and hosts into "clusters" and providing the means to monitor those VMs and in the event of a failure, automatically restarting the failed VM on different host. VMware HA is a reactive approach to failures and protects against scenarios such as host failures, host isolation and application crashes.

Connect for Clinical Systems deployed within a VMWare HA cluster is not without downtime and should be deployed as alternative to the manual restoration model described in the previous section where some down time is acceptable but manual intervention is not desired.

The downtime associated with VMWare HA should be only the result of the period of time that it takes for the Primary Active Host to detect the failure and the period of time that it takes to restart the VM on another host.

Connect for Clinical Systems can be easily incorporated into a VMWare HA cluster by Hospital IT staff, provided that the software has been properly deployed to one of the primary hosts. In addition, the interfaces to the external system (e.g. Patient Monitors, Nurse Calls, etc.) provided by Connect for Clinical System support recovery of all active alarms through immediate acquisition on restart.

Consideration for this Deployment Model

- Down time = (Failure Time + Reboot).

- Remote data centralization on separate host (required).
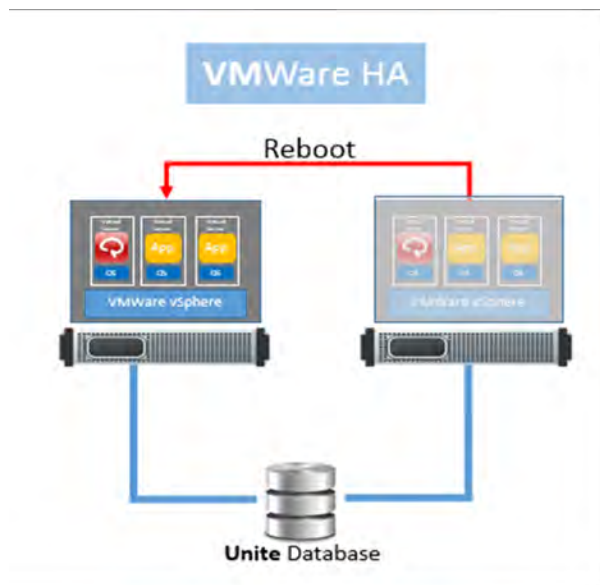
Additional Information: `https://pubs.vmware.com/vsphere-4-esx-vcenter/index.jsp#com.vmware.vsphere.availability.doc_41/c_createha.html`.

2.7.3   Fault Tolerance (VMWare Fault Tolerance)

VMware Fault Tolerance offers mission critical virtual machines continuous availability by deploying and maintaining a Secondary VM synchronized and continuously available, identical to the Primary VM in the event of a failover situation.

The Secondary VM in a Fault Tolerance configuration, is created and runs in virtual "lockstep" with the Primary VM. VMware vLockstep replicates the entire Primary VM environment, memory, services and processes to the Secondary VM, which is typically running on another server host. Utilizing the synchronization provided by vLockstep, the Secondary VM represents an exact copy of the primary and can take over for execution without interruption.

Within VMware Fault Tolerance, the Primary and Secondary VMs exchange heartbeats to monitor the status of one another to ensure that Fault Tolerance is continually maintained. A transparent failover occurs if the host running the Primary VM fails, in which case the Secondary VM is immediately activated to replace the Primary VM. A new Secondary VM is started and Fault Tolerance redundancy is reestablished within a few seconds. If the host running the Secondary VM fails, it is also immediately replaced. In either case, users experience no interruption in service and no loss of data.
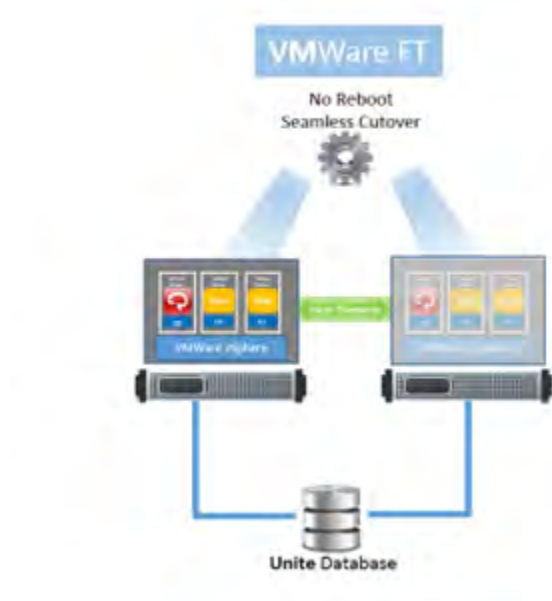
Consideration for this Deployment Model

• No appreciable downtime.

• Remote data centralization on separate host (required).

• Additional Information: `https://pubs.vmware.com/vsphere-4-esx vcenter/index.jsp#com.vmware.vsphere.availability.doc_41/c_ft.html`.

2.8 IP Ports

IP ports for C4CS should not be load balanced.

Inbound Ports

Port	Protocol	Description	Source	Destination
443 (default)	TCP	Web traffic	Client	Unite PS
3217	UDP	Unite traffic	Unite modules	Unite PS
8181	TCP/ HTTP	Unite Node Supervisor Web interface	Web client	Unite Node Supervisor
8190[2]	TCP/ HTTP	Connect Supervisor Web interface	Web client	Connect Supervisor

---

2. Subsequent installation ports will be sequentially numbered as 8x90, where x increments for each installation.

Outbound Ports

Port	Protocol	Description	Source	Destination
5672	TCP	RabbitMQ traffic	Unite PS	RabbitMQ
3217	UDP	Unite traffic	Unite PS	Unite modules

Internal Ports

Port	Protocol	Description	Source	Destination
8000[3]	TCP	Waveform Snapshots Requests	Alarm Service Engine	Driver Host
8185[4]	TCP/ HTTP	Alarm Service Engine Status	Web Client, Node Supervisor	Alarm Service Engine
8186[5]	TCP/ HTTP	Driver Host Status	Web Client, Node Supervisor	Driver Host
8187[6]	TCP/ HTTP	Connect proxy status	Web Client, Node Supervisor	Connect proxy

Driver-specific Ports

Port	Protocol	Description	Source	Destination
8001	TCP	Digistat Connect Traffic (Default)	Digistat Connect	Digistat Connect Driver
7000	UDP	Rwhat Traffic	GE Router	Carescape Unity Driver
7001	UDP	Unity Traffic	GE Router	Carescape Unity Driver
2000	UDP	Time Synchronization Traffic	GE Router	Carescape Unity Driver

---

3. Subsequent installation ports will be sequentially numbered as 8x00, where x increments for each installation.
4. Subsequent installation ports will be sequentially numbered as 8x85, where x increments for each installation.
5. Subsequent installation ports will be sequentially numbered as 8x86, where x increments for each installation.
6. Subsequent installation ports will be sequentially numbered as 8x87, where x increments for each installation.

Port	Protocol	Description	Source	Destination
2007	TCP	Carescape waveform control channel	Carescape Unity Driver	GE Carescape Gateway
4446	UDP	Carescape waveform binary data stream	GE Carescape Gateway	Carescape Unity Driver

2.9 Access Controls

Connect for Clinical Systems does not contain operator configurable alarm limits or parameters. Access to the configuration of Connect for Clinical Systems is made only through Unite Admin. Only those individuals with proper knowledge, training and authority should have access to the configuration of this system.

The Unite Admin configuration utility may be installed either on the server itself or optionally on a separate client PC. Please see the Unite Platform Server, Data Sheet, TD 93266EN for specific information related to the client runtime requirements for the Unite Admin configuration utility.

If the Unite Admin utility is made available in an environment where it may be exposed to individuals without proper knowledge, training and authority, steps MUST be made to prevent unauthorized access to configuration.

- After any configuration change made using the Unite Admin, the application should be manually logged out, using the already provided functionality.
- Unique usernames and passwords should be utilized and configured with appropriate authority level applicable to responsibility of each individual, as already provided by the application.
- All workstations with access to the Unite Admin utility should be configured to automatically logout after a preset time of no activity to be no greater that 5 minutes, to prevent possible access violations in cases where the Unite Admin utility is left open and unattended.

For configuration of security measures including encryption settings, default login credentials and user access rights see the Unite Platform Server, Configuration Manual, TD 93280EN.

Risks may need to be analyzed and evaluated when interfacing with a network that includes other equipment. Refer to the Pre-configuration of Windows for Unite Applications, Configuration Notes, TD 92993EN.

2.9.1 Interoperability

Ascom provides verification towards the supported Microsoft Operating System version defined in the Data Sheet. Verification testing of the software includes all current recommended security updates at the time of testing. Once installed, security updates of the Operating System are recommended to be applied under supervision to verify continued interoperability.

2.9.2 Malware Detection Compatibility

Connect for Clinical Systems is verified to be compatible with F-Secure Virus and Malware Detection Software. Connect for Clinical System is not able to guarantee compatibility with all other Malware and Virus detection software. Ascom recommends that other vendor Virus and Malware detection software be installed and verified on site before the software is put in use to assist in patient care. Additionally, any virus malware definition updates should only be applied under supervision.

The compatibility and use of malware detection software must be considered before and after system verification activities have been performed. Additionally, post-malware updating verification will be identified as required.

3   Solution Overview

Connect for Clinical Systems provides a centralized platform for the acquisition of events/alarms and waveform data from external clinical systems. Multiple installations of the product can be utilized through multiple, simultaneous integrations and drivers. Three medical (including Nurse Call) and a non-medical installation can run in parallel as separate installations. This isolates a malfunction or fault to a specific installation, and prevents malfunctions on one installation from impacting the operations of the other installation.

In addition to acquisition, the platform is able to provide intelligent filtering and redirection rules to provide dispatching of the information related to these events/alarms to clinical operators. Dispatched alerts are provided with presentation attributes that enable display devices to present those alerts with priority consistent with that of the originating system, including color & tones.

Connect for Clinical Systems operates within the Ascom Unite Messaging Suite for Healthcare utilizing the functions of the various applications making up the complete notification platform.

Unite Admin

The Windows based Ascom Unite Platform Manager (Unite PS) makes it possible to configure and administer the various components of the platform including Connect for Clinical Systems.

Unite Assign

The graphical user interface for the scheduling & assignment of staff members to events and alerts generated by external clinical systems.

The Assign application makes it possible to assign staff to locations (beds, rooms, units), to specific alert types, or to different roles, so that the right person receives the right information to his or her phone.

Unite View

The software application enabling central display or "dashboard" of specific alarms and alerts across an entire hospital ward or unit. This dashboard list of current alarm conditions allows managers and nursing to keep in touch with active patient alarms and alerts in a central location.

Unite Platform Server (Unite PS)

The notification gateway responsible for managing devices and facilitating the delivery of alerts to mobile and fixed display devices.

Unite CM/CS

The legacy notification gateway responsible for managing devices and facilitating the delivery of alerts to mobile and fixed display devices.
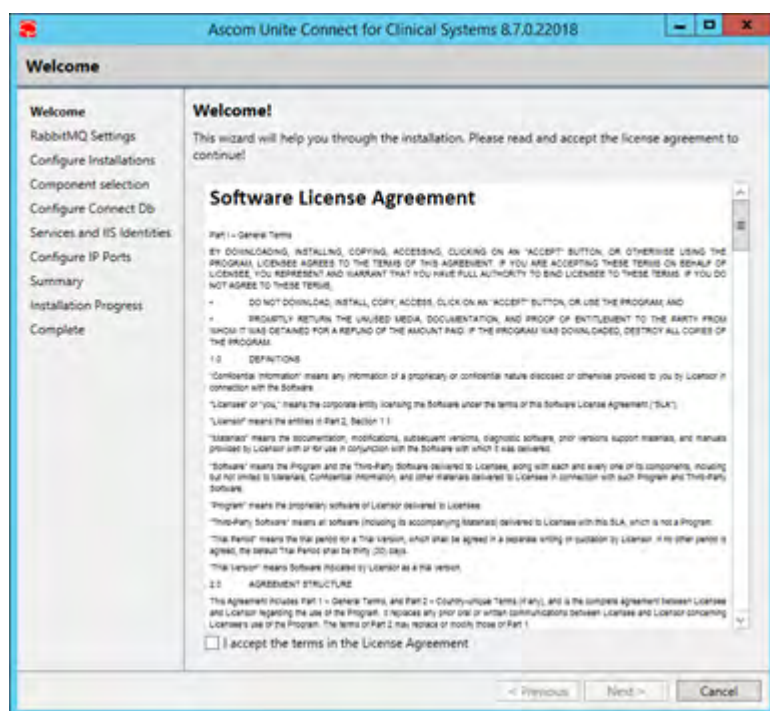
4 Installation

The Connect for Clinical Systems installer installs the Core Components of the C4CS application along with optional applications.

Connect for Clinical Systems can support multiple installations on the same server with runtime components that operate independently. Each installation is a standalone instance of C4CS with its own components (e. g., Driver Host and ASE), installed and operating independently on the same hardware.

Installations can be defined as medical and non-medical when installed, and each installation has its own database.

Since each installation has its own components and database, a malfunction in any of those components within one installation will not impact the operation of the other integration. For example, a non-medical driver plugin cannot cause any failures to occur in the medical Driver Host and therefore cannot interrupt the operation of the medical installation.
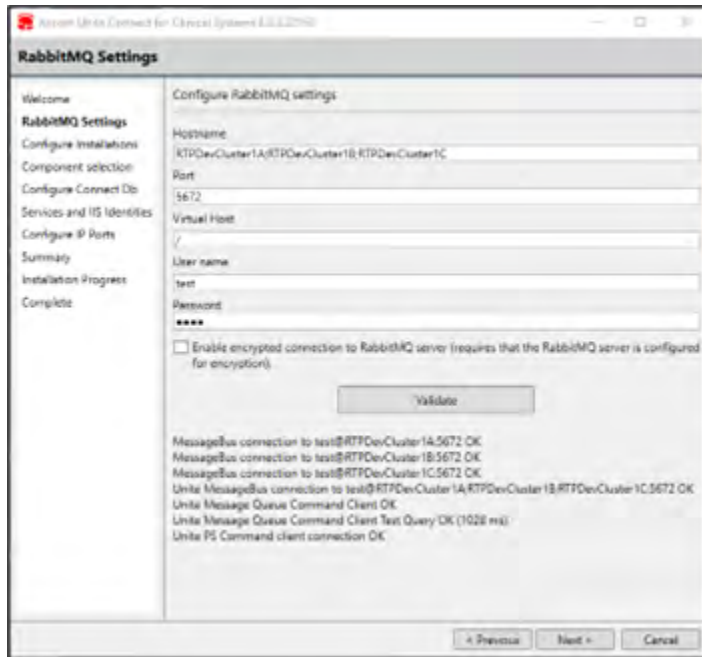
4.1 Welcome

Select **I accept the terms in the License Agreement** to continue. Click **Next** to configure RabbitMQ settings.

4.2 RabbitMQ Settings

A connection to RabbitMQ is required for both single node and clustered installations of C4CS. The RabbitMQ connection settings are configured on this screen. These settings must be the same settings used for Unite PS.

If communication to RabbitMQ is to be encrypted, and if encryption is configured within the RabbitMQ broker, select the box labeled **Enable encrypted connection to RabbitMQ server**. Multiple parallel RabbitMQ connections are supported when installed on a cluster with Active-Active non-clustered RabbitMQ. In this case, multiple RabbitMQ hostnames are configured by entering the hostnames delimited with a semicolon. Once the settings have been entered, click **Validate** to validate the connection to RabbitMQ and the connection to Unite PS. At least one connection must pass validation, and the connection to Unite PS must be valid, before pressing **Next** is allowed.

> After initial installation, changing the RabbitMQ settings on this page will only apply during upgrade of Common Components, and not when installation is limited to installing drivers.

For more information about RabbitMQ settings, including clustering options for RabbitMQ, reference the Pre-configuration of Windows for Unite Applications, Configuration Notes, TD 92993EN.

4.3 Configure Installations

Each time the installer is run, the user interface will allow the choice between installing or upgrading a medical or a non-medical device installation. A unique name must be assigned to each installation, and that name is limited to 15 characters and cannot include spaces or special characters.

4.3.1 New Installation

The next screen to appear is shown for a new installation with no previously installed instances.

By default the **Medical** option is selected for the first installation. To install an instance of the product for non-medical purposes, clear the check mark from the **Medical Device** option.

Provide the installation name for the required installation instance type. This name will be used to identify the components and logs for the installation. The selected name cannot be changed once installation is complete.

The first Medical installation will, by default, not include the Installation Name in the Windows service names for it's services. To Include the Installation Name in the Windows service names, select the **Use Installation**

Name in Service Names. This option is only available on the first Medical installation as other installation instances will always include the Installation Name in Windows service names

Up to 3 medical installation instances, and up to 1 non-medical installation instance is permitted, for a total of 4 possible installations of the product on the same machine.
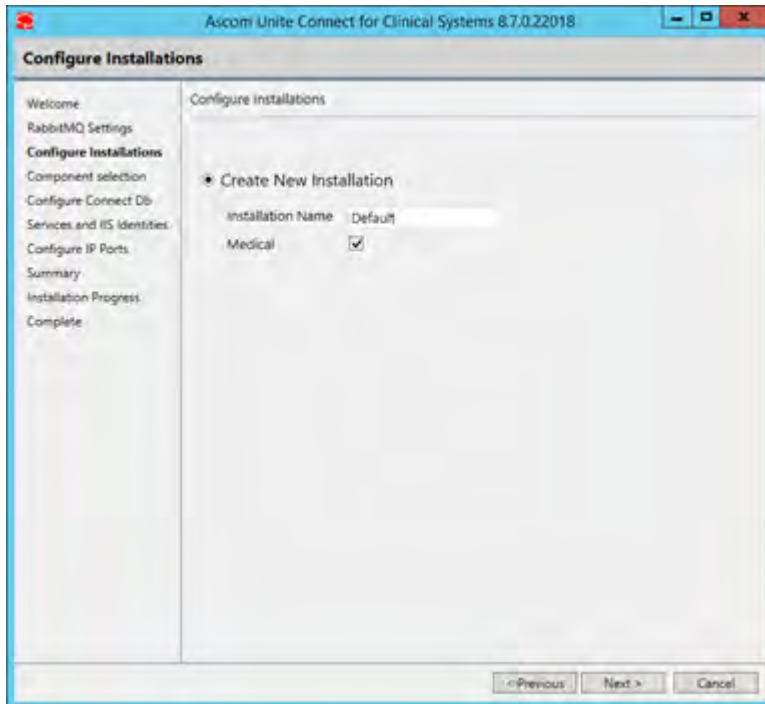
4.3.2   New Installation or Upgrade with a Previously Installed Instance

An alternative to the previously described screen may be presented if the installer is run on a machine where the product is already installed.

The screen below shows that the medical device installation is already installed. To upgrade this instance to a new version or to install an additional driver, select the **Update Existing Installation** radio button, and select the named installation from the table located below.

To install an additional installation instance (e.g., a non-medical device installation) select the **Create New Installation** radio button, deselect the **Medical** option and provide the installation name for a non-medical instance.
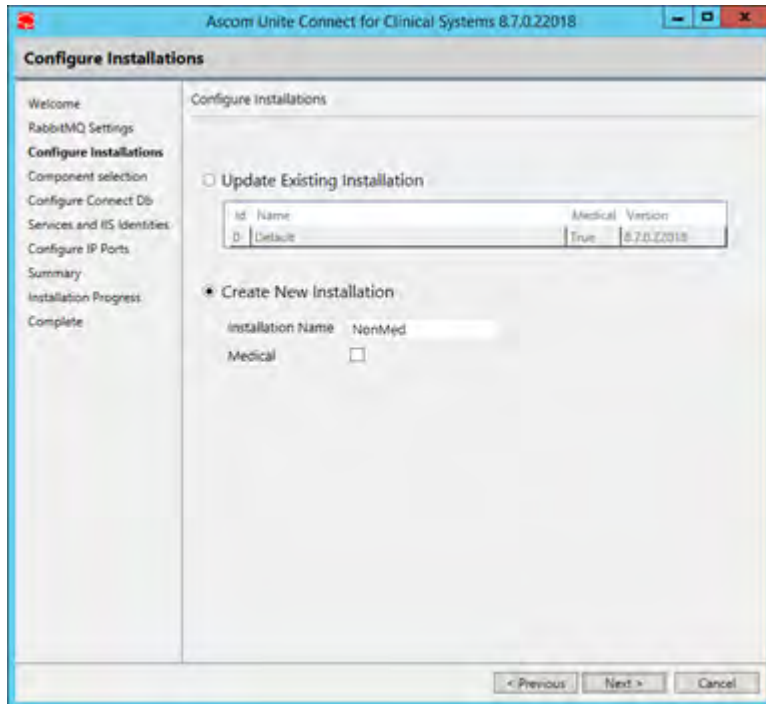
Click **Next** to proceed with the install or to update components.

4.4   Component Selection

For the medical device installation, shown below, only applicable medical device drivers are available.
There are no non-medical device drives bundled with the C4CS installer when installing or upgrading a non-medical device installation.
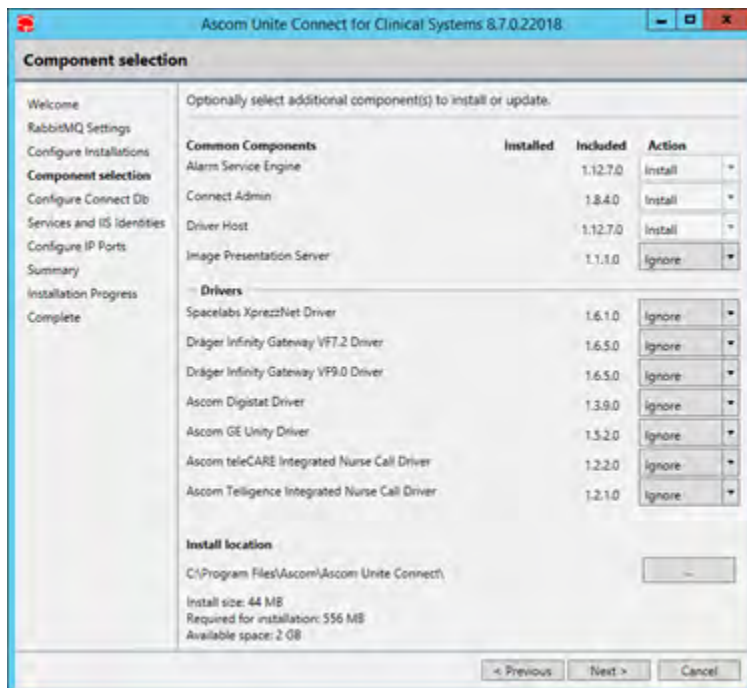
Before proceeding with an installation, drivers with an available upgrade have an upgrade warning icon indicating that the user must select to either **Upgrade** or **Keep Version** for those drivers.
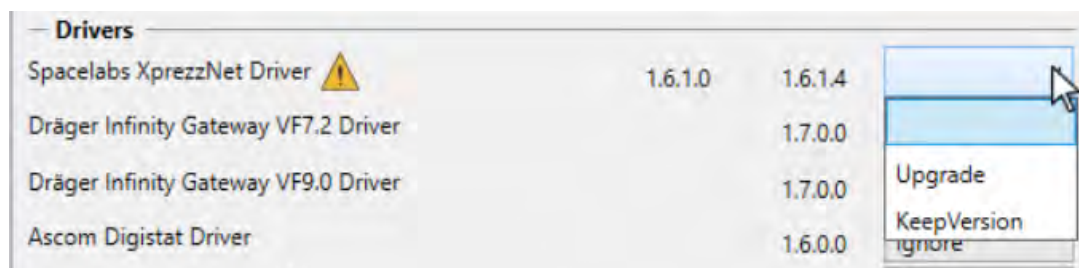
4.4.1 Component Selection — Non-Medical

For a non-medical installation, shown below, only the Common Components are available for installation.

The installation of non-medical device drivers requires the manual copying of the driver distribution package to the `C:\ProgramData\Ascom\Ascom Unite Connect\C4CS-1-******` location on the local machine where the installation has occurred.

The `******` portion of the file path will correspond to the unique name provided to the installation chosen within the **Configure Installations** screen described in 4.3.2 New Installation or Upgrade with a Previously Installed Instance, page 25.
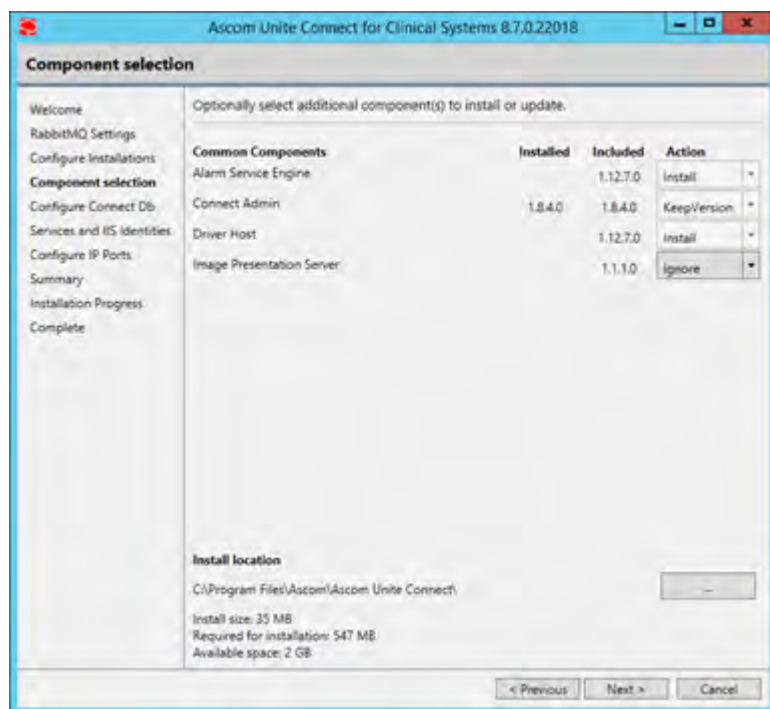
The core components of Connect for Clinical Systems will be installed by default.

4.4.2 Image Presentation Server

Optionally, you can install the IPS along with the core components or install it separately at a later time. To install an Image Presentation Server (IPS), select "Install" from the items Action list. When selecting to install the IPS, additional configuration settings are required, and an additional step is added to the installation wizard. See 4.6 Image Presentation Settings, page 29 for these configuration settings.

The Image Presentation Server is only required when utilizing waveform snapshots with GE CARESCAPE Unity, Dräger Infinity Gateway, or Spacelabs XprezzNet drivers.

The Image Presentation Server is NOT required or utilized when receiving waveform snapshots from Digistat.
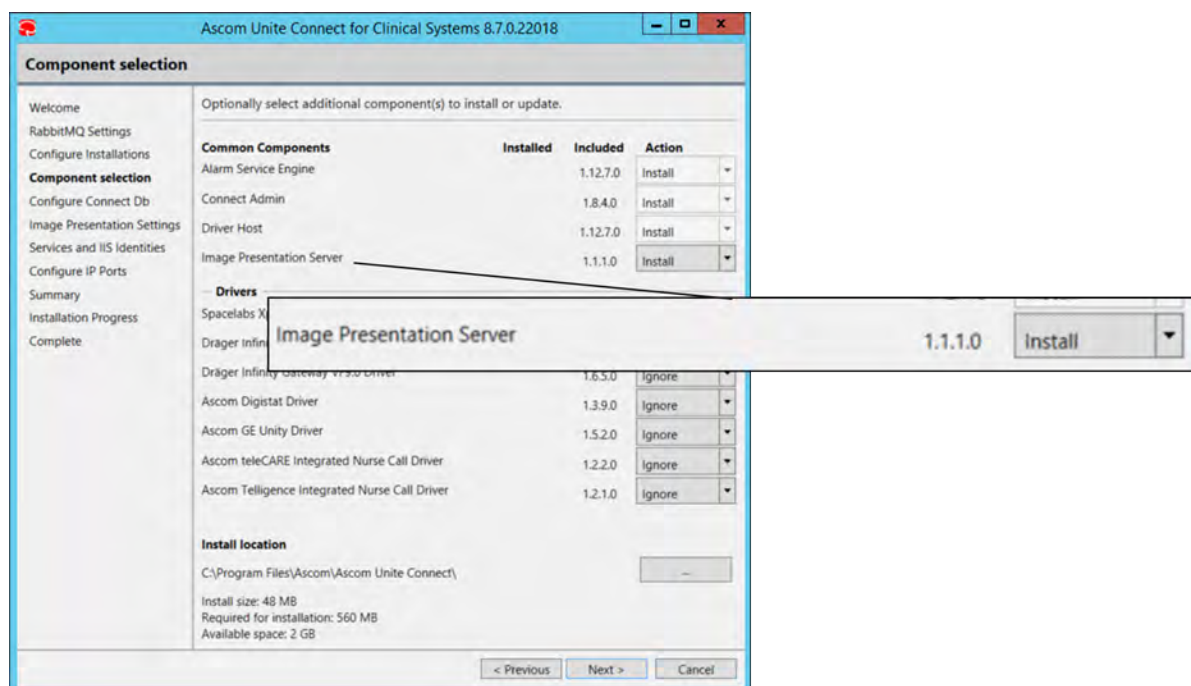
4.4.3   Keep Previous Driver Version during Upgrade

While upgrading other system components, an existing version of an installed driver can be retained and can continue operating with the upgraded software. This is done by selecting the **Keep Version** option of a specified driver.

4.5   Configure Connect DB

Specify a unique, database for each installation instance. In the situation where both a medical and non-medical installation are present on the same machine, the database used for each installation must be separate. The following example shows a database being selected for the medical installation instance.
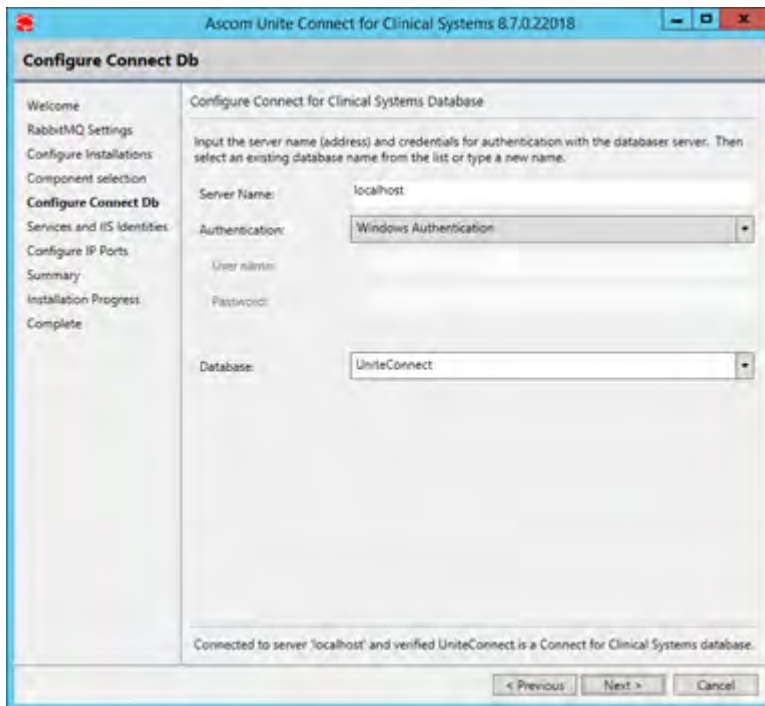
- **Server Name:** The name of server hosting SQL Server to which Connect for Clinical Services will be connecting.

- **Authentication:** The type of credentials Connect for Clinical Systems will use to access Unite PS SQL Server database. If you select **Windows Authentication,** then the application accesses the database using a Windows User account. If you select **SQL Server Authentication,** then the application will access the database using a preconfigured SQL Server login. Username and password are required for this type of authentication.

- **Database:** The name of the database to use for Connect for Clinical Systems (the database will be created if it does not already exist.

> If appropriate permissions are not available to create a database instance during installation, installation can proceed using a pre-existing empty database instance (i.e. with no defined data) created outside of the installer.

4.6   Image Presentation Settings

1.   In the **Site** drop-down list, select the IIS web site that shall be utilized to host the Ascom Image Server application. The selected website must listen on port 80.

2.   If a virtual directory within the IIS web site is desired, enter the name of the Virtual Directory in the Virtual Directory field. This field is optional.

3.   In the **Application Pool** drop-down list, select the application pool associated with the web site.

4.   Click **Next**.
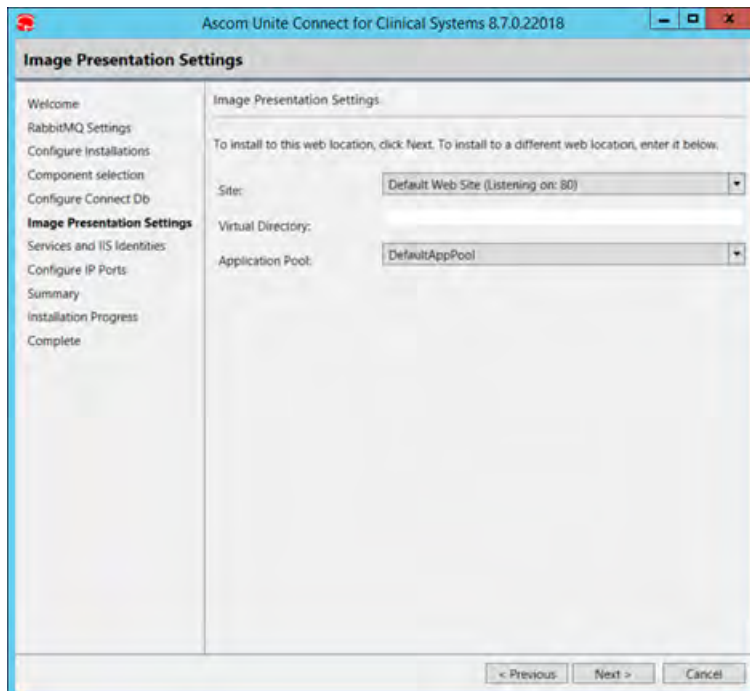
4.7 Services and IIS Identities

The Service and IIS Identities are used when the SQL database is placed on another server or if the environment does not allow default accounts.
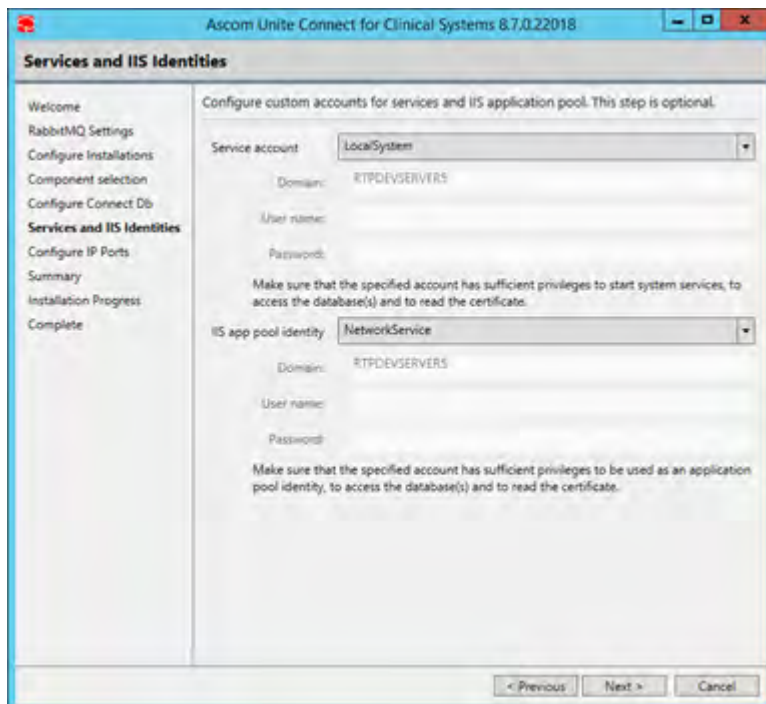
1. In the Service account drop-down list, select **Custom Account**.

2. Enter the Windows domain for custom accounts.

3. Enter the username and password for custom accounts.

4. In the IIS app pool identity drop down list, select **Custom Account**.

5.   Enter the Windows domain for custom accounts.

6.   Enter the username and password for custom accounts.

7.   Click **Next**.

When using custom accounts, you will not be allowed to proceed until the parameters set for the custom accounts are verified to allow for a successful connection.

4.8   Setting IP Ports

Shown below, the ports identified are for the purpose of hosting supervision interfaces for each of the components listed, in addition to the ports used to enable internal communication for use with waveform generation. The default ports specified should be validated to determine if they are available for use. Select **Validate** to proceed.
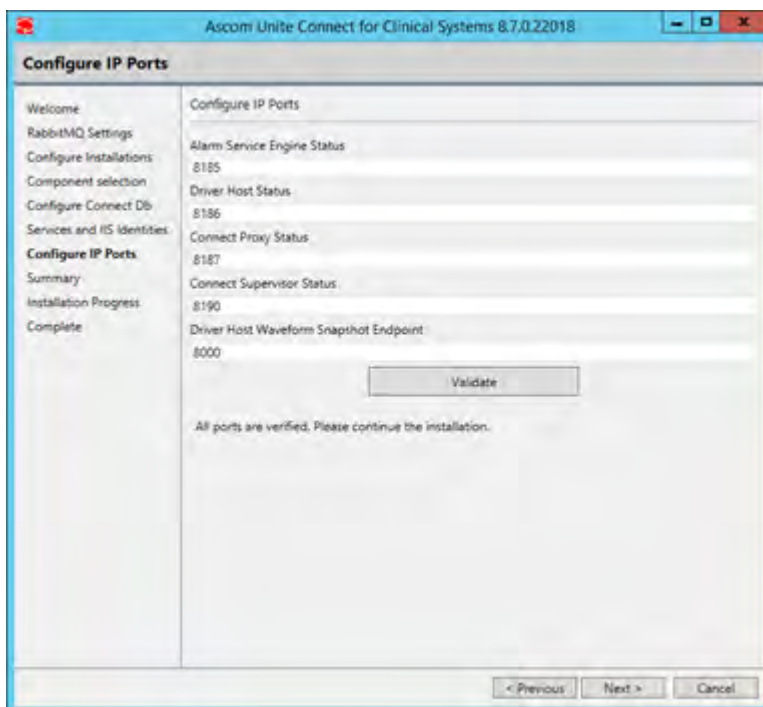
The ports for any subsequent installations including a non-medical installation are unique and should represent unused ports from those assigned to any other service or for the previously installed medical device.

4.9   Summary
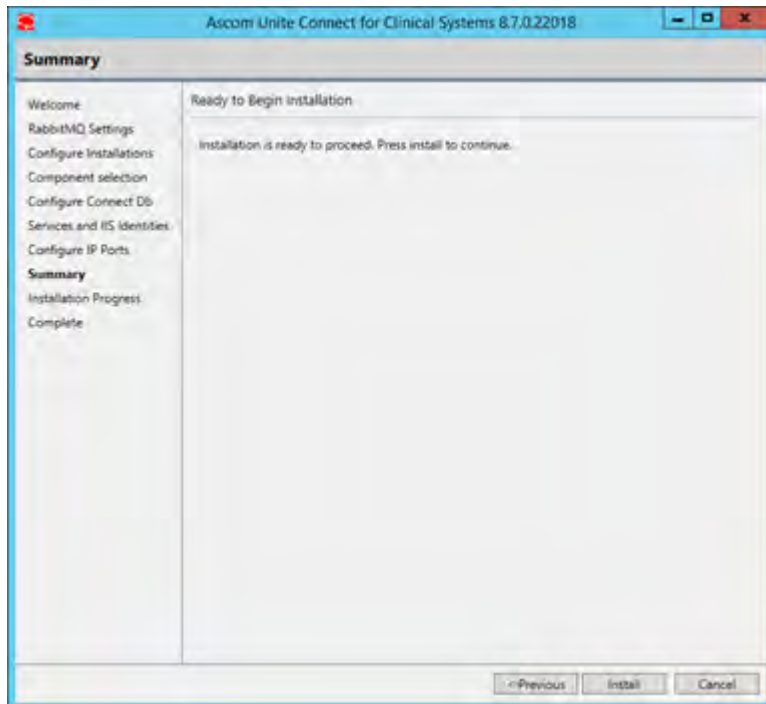
In the Summary window, click **Install**.

4.10   Complete
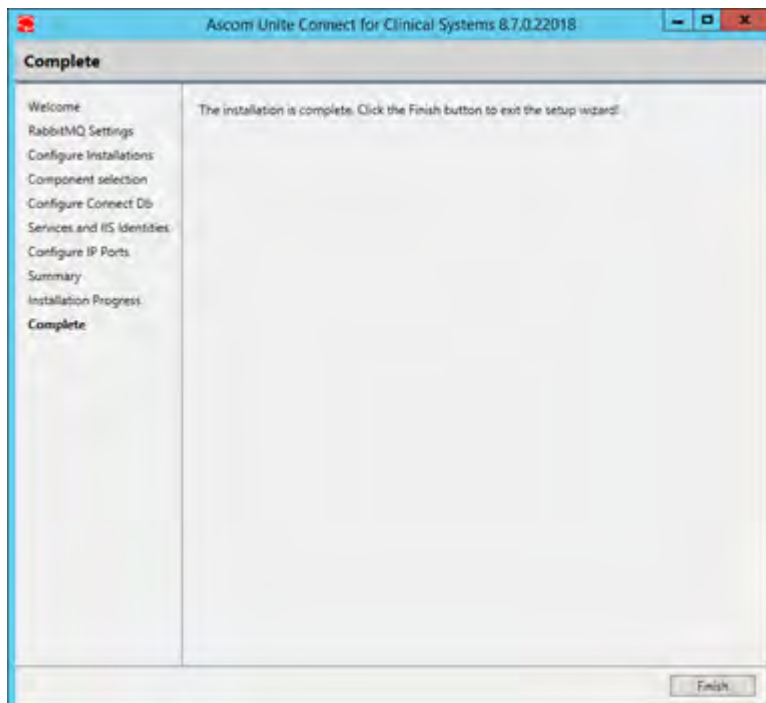
Click **Finish** to complete the setup wizard or **Exit** to cancel the setup.

After a successful installation of Connect for Clinical Systems, the label for the installation is shown within the Unite Admin Infrastructure list. If multiple instances are installed, a label for each installation is shown.

For example, in the image below, two installations (one medical and one non-medical) of Connect for Clinical Systems are shown in the infrastructure list on the left, along with the version number of each installation.
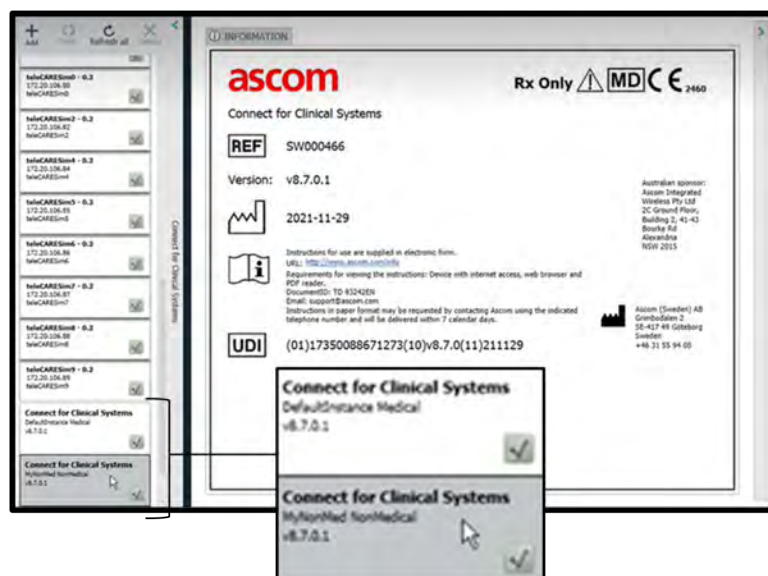
4.11 Upgrade an Installation Instance

When multiple parallel installations instances are installed on the same server, each installation can be upgraded separately without interrupting the operation of the other. Upon restarting the installer with one or more instances previously installed, a screen appears as shown in 4.3.2 New Installation or Upgrade with a Previously Installed Instance, page 25.

To upgrade an instance to a new version, select the Update Existing Installation radio button, and select the named installation from the table located below.

> ⚠️ **Important**
>
> Only sequential upgrades of Connect for Clinical Systems major software versions are supported (e.g., upgrading from 8.6.0 to 8.7.0 is supported, but upgrading from 8.5.0 to 8.7.0 is not supported).

Ensure that the upgrade is being performed on a passive node. See Unite Platform Server, Installation Guide, TD 93273EN.

4.12 Uninstall Connect for Clinical Systems

- Remove all Workflows and driver instances in Unite Admin.
- Delete all instances of all integrations based on Connect for Clinical System before completely uninstalling it from the system.

If these steps are not taken, running the uninstaller will not allow the installation to be uninstalled.

4.12.1 Uninstall an Instance

Instances can be uninstalled separately without affecting the operation of other installed instances. After running the uninstaller, a screen will appear showing the installed instances along with a prompt to **Select Instance**. Select the instance to be uninstalled as follows and click **Uninstall**.
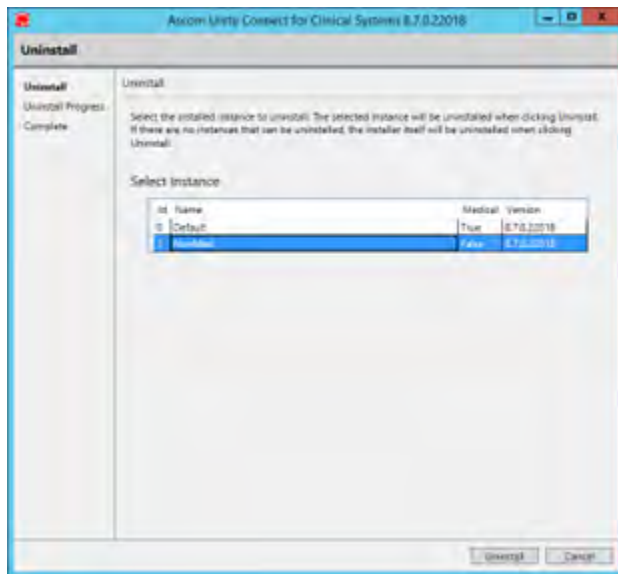
5 Integration Setup

5.1 Integration Overview

Ascom integrations such as those supported by Connect for Clinical Systems are managed by first adding them through Unite PS and Unite Admin. Integrations include a device specific driver (installed using the installation utility described in the previous section) and at least one configuration template which contains a default set of capabilities for utilizing Connect for Clinical Systems Event Management for receiving, filtering and distributing information from the various clinical systems supported by the product. These predefined configuration templates can be applied to the system according the available licenses and drivers installed.

Adding, configuration, and maintenance of an integration, are all done through the Integrations configuration section of the Unite Admin. The Integrations configuration area of the Unite Admin is depicted using the following icon:
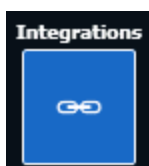
Before adding the first integration to the system, users, devices, organizations and locations should already be configured, please see the Unite Admin System Configuration help files for details related these topics.

After installation of an integration is completed, assignment clients such as Unite Assign can be configured for the destination of alerts, based on location and available devices/users.

> If any locations are changed within an integration, you need to reapply any assignments within Unite Assign.

5.2 Adding an Integration and Selecting an Installation

Integrations are associated with a specific installation instance, described in .

1. To add an integration, click **Add**.

2. From the Select system drop-down, select from the available Clinical Systems based on available licenses and installed drivers.

Clinical System	
System Name	**System Description**
Spacelabs – XprezzNet	Integration Template & Driver for Spacelabs monitors connected to the Spacelabs XprezzNet Patient Monitoring Gateway.
Dräger Infinity Gateway	Integration Template & Driver for Dräger monitors connected to the Dräger Infinity Patient Monitoring Gateway.
Digistat Connect	Integration Template & Driver for the Digistat Connect software used to extend the available medical device connectivity of Connect for Clinical Systems.
GE Carescape Unity	Integration Template & Driver for GE CARESCAPE monitors connected to the GE CARESCAPE Unity network.

Ascom teleCARE IP	Integration Template & Driver for acquiring and distributing Events received from the Ascom teleCARE IP Nurse Call System.
Ascom Telligence	Integration Template & Driver for acquiring and distributing Events received from the Ascom Telligence Nurse Call System.
Ascom – Custom Connect	Integration Type associated with non-medical integrations. Templates available for this type of integration are provided by the installation of a non-medical type driver. See 4.3.2 New Installation or Upgrade with a Previously Installed Instance, page 25 for details on installing non-medical drivers.

3.   From the **Apply Template** drop-down, select a template.

4.   Change the name of the integration if necessary.

5.   Any integration that is added must be associated with an installation. Select an installation from the drop-down menu. The installation names configured during installation, shown in 4.3 Configure Installations, page 24 , will be visible.

6.   Press **Add** to complete the Adding an Integration step.

When adding a medical integration, it can only be associated with medical installation instances. In this example, since the chosen driver represents a medical device, only the medical device installation (named Default in this screen shot) is available. Additionally, the installation instances available for selection will only include those where the required driver is installed.
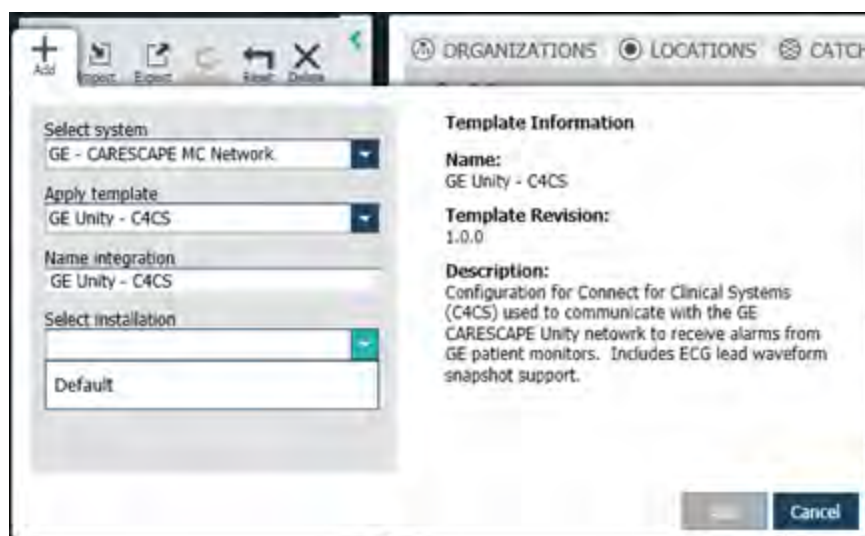
Non-medical device integrations are available if installed (see 4.3.2 New Installation or Upgrade with a Previously Installed Instance, page 25 for details) under the **Ascom – Custom Connect** system type.
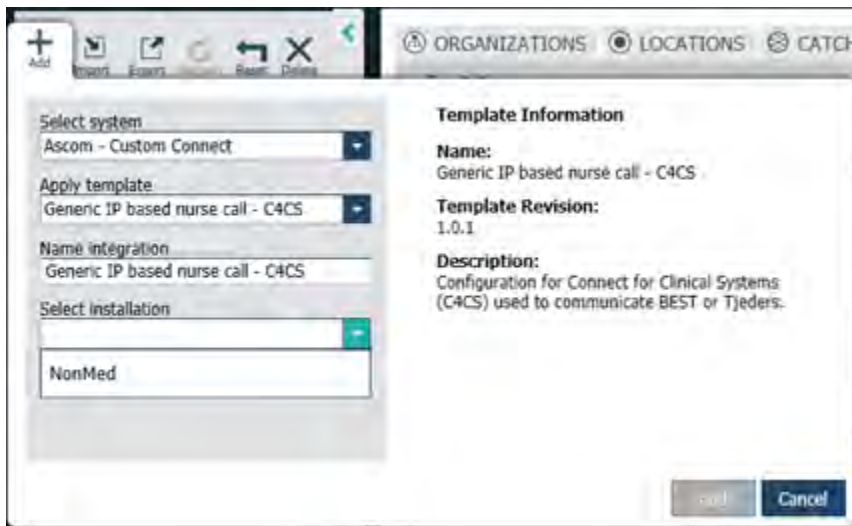
5.2.1 Templates

Clinical System			
System	**Device Type**	**Template Name**	**Template Description**
Spacelabs	Patient Monitor	XprezzNet-C4CS	• 3 Levels of Redirection. • Waveform Support. • Unite Catchnet with Unhandled Fault generation. • Accept/Busy User Acknowledgment. • Visible in Unite View. • Notification of Cleared Alarm from Patient Monitor.
Dräger	Patient Monitor	Infinity Gateway-C4CS	• 3 Levels of Redirection. • Waveform Support. • Unite Catchnet with Unhandled Fault generation. • Accept/Busy User Acknowledgment. • Visible in Unite View. • Notification of Cleared Alarm from PM.

Digistat Connect	Alarm Aggregator	Digistat Connect-C4CS	• 3 Levels of Redirection. • Waveform Support (provided by Digistat). • Unite Catchnet with Unhandled Fault generation. • Accept/Busy User Acknowledgment. • Unite View Operator Mode with Dispatch. • Notification of Cleared Alarm.
GE Carescape Unity	Patient Monitor	GE Unity-C4CS	• 3 Levels of Redirection. • Unite Catchnet with Unhandled Fault generation. • Accept/Busy User Acknowledgment. • Unite View Operator Mode with Dispatch and Persistence. • Notification of Cleared Alarm from PM.
Ascom teleCARE IP	Nurse Call	Integrated Nurse Call-C4CS	• 3 Levels of Redirection. • Unite Catchnet with Unhandled Fault generation. • Accept/Busy User Acknowledgement. Unite View Operator Mode with Dispatch. • Notification of Cleared Events. • Ability to request cancellation from handset. • Ability to initiate speech callback from handset.

Ascom Telligence — C4CS (Simplified)	Nurse Call	Integrated Nurse Call-C4CS	This template contains a simplified set of workflows that support mapping multiple Telligence event priorities to each workflow. • 3 Levels of Redirection. • Unite Catchnet with Unhandled Fault generation. • Accept/Busy User Acknowledgement. • Unite View Operator Mode with Dispatch. • Notification of Cleared Events. • Ability to request cancellation from handset. • Ability to initiate speech callback from handset.
Ascom Telligence — C4CS	Nurse Call	Integrated Nurse Call-C4CS	The workflows and assignment templates in this integration template are equivalent to the events in the C4NC Telligence integration template. • 3 Levels of Redirection. • Unite Catchnet with Unhandled Fault generation. • Accept/Busy User Acknowledgement. • Unite View Operator Mode with Dispatch. • Notification of Cleared Events. • Ability to request cancellation from handset. • Ability to initiate speech callback from handset.
Non-Medical Templates	Custom	Custom	• Templates available for this type of integration are provided by the installation of a non-medical type driver. See 4.3.2 New Installation or Upgrade with a Previously Installed Instance, page 25 for details on installing non-medical drivers.

5.3   Refreshing an Integration

If the location structure has been changed for an organization associated with an integration, a refresh is needed to update the integration with the latest data.

1.   Select the integration you want to refresh.

2.   Click **Refresh**.
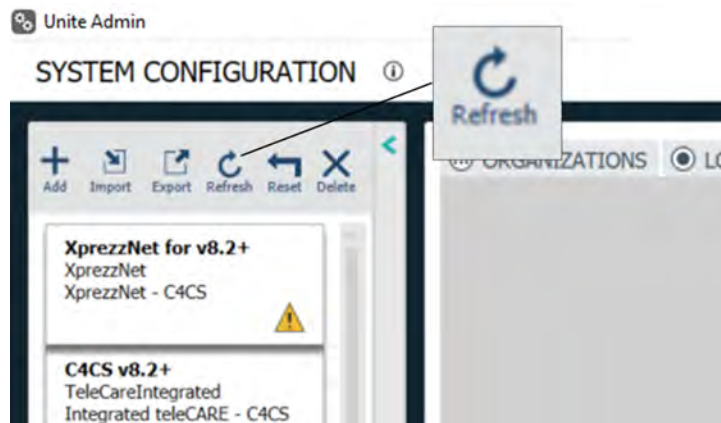
5.4   Resetting an Integration

An individual Integration can at any point in time be re-initialized back to the factory default configuration, and all changes made for this integration will revert back to a point when the integration was first added to the system. When reset, and all settings are reset to the default values except for the organization settings, location conditions, and Assignment Templates settings (which keep their values).

To reset an integration, from the Integrations tab:
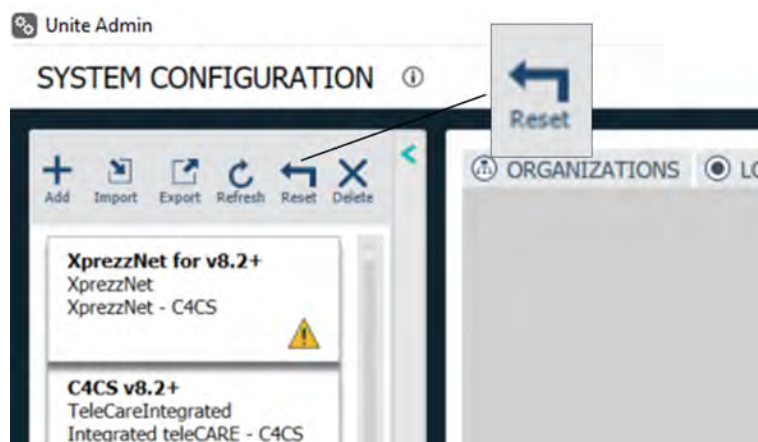
1.   Select the specific Integration from the available integrations on the left-hand side of the screen.

2.   Click **Reset**.

3.   A warning displays asking if you want to keep the integration as it is with modifications or reset the integration.
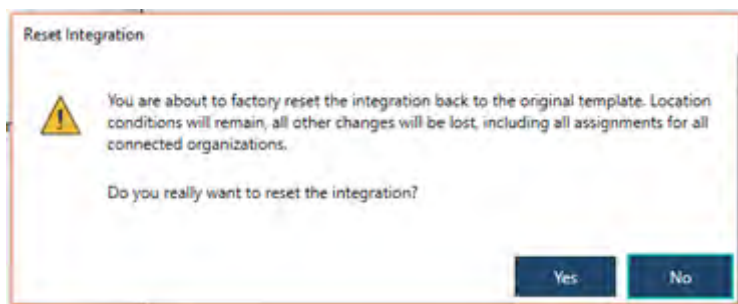
4.   Click **Yes** to confirm the reset, and **No** to cancel the reset and keep your modified settings.

5.5   Deleting an Integration

An integration can be deleted. This deletes all Notification Events, their assignments and any Location Conditions, and returns the system back to the point before the integration was added. Other settings in other areas such as ORGANIZATION and LOCATIONS will be preserved.
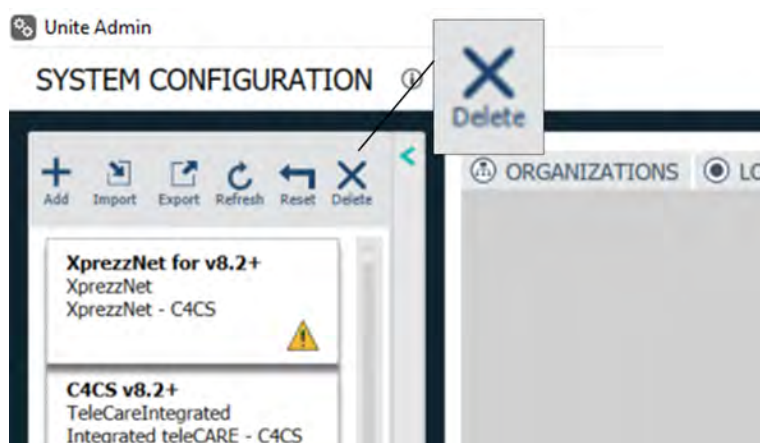
To delete an integration, from the Integrations tab:

1.   Select the specific Integration from the available integration on the left-hand side of the screen.

2.   Remove all Workflows, and Driver Instances associated with the Integration.

3.   Remove all associations between the Integration and Organization and Locations.

4.   Click **Delete**. A warning displays, prompting you to keep or delete the integration:

5.   Click **Yes** to confirm the delete, and **No** to cancel the delete and to keep the integration.

5.6   Organization and Location Configuration

Organization and Location Condition configuration provides the mechanism by which location information received from an external clinical system, can be associated to the units, rooms, & beds defined in the Ascom Unite system. This activity provides the appropriate information necessary to utilize applications

such as Unite Assign, Unite View and Connect for Clinical Systems own event management capabilities to accurately direct alerts to caregivers based on the location of an active event and/or alarm.

5.6.1   Organization Identification

The first step in configuration is to identify the appropriate organization that will be utilizing the integration (organizations should have already been established during the installation of Unite PS and Unite Admin application; see Unite Admin System Configuration help files for more information).

This step is accomplished by selecting the ORGANIZATIONS tab for the specific integration, selecting Edit and choosing the Organization(s) and/or Unit(s) within which the integration is to be used. Multiple Organizations can be selected at once and when complete, click **Done**.

5.6.2   Location Conditions

The next step in configuration is to define the relationship between the descriptions of the location where the external clinical system indicates there is an event/alarm and the corresponding location defined in the Unite system.

> Unite Locations should have already been established during the initial installation of the Unite Admin application; see Unite Admin System Configuration help files for more information).

The method for completing the location conditions setup first involves gathering the format by which the external clinical system provides the description of its locations.

> Special attention should be placed upon the type of external system and how the received event/alarm location can best represent a location in Unite by which the appropriate care-providers should be assigned.

For instance, a patient monitoring integration used exclusively with telemetry may consist of different ways of reporting the patient's location, versus a system consisting of only fixed (bed based) patient monitors. For

those integrations that contain multiple ways in which the external event/alarm location can be described, please see 5.6.2.1 Location Conditions – Driver-Specific, page 43 for driver-specific format details.

The remaining step to completing this portion of the configuration is to enter the content according to the format by which the external clinical system provided the location description. This information should be entered for each location defined in the organization Units selected for the facility.

> Location conditions are case sensitive. For instance, the location conditions ICU|BED1 and ICU| Bed1, are recognized as separate locations that operate independently.

Caution

> If duplicate conditions are entered (i.e., ICU|BED3 and ICU|BED3 for separate Unite locations) only one of those locations is recognized and used to identify where the triggered events occurred.

In addition, the Assignment Template Types available for the integration are available next to each location, by selecting these Assignment Template Types, that location will now be published to all Unite application indicating that this location supports these notification Assignment Template Types. See 5.9 Assignment Templates, page 47.
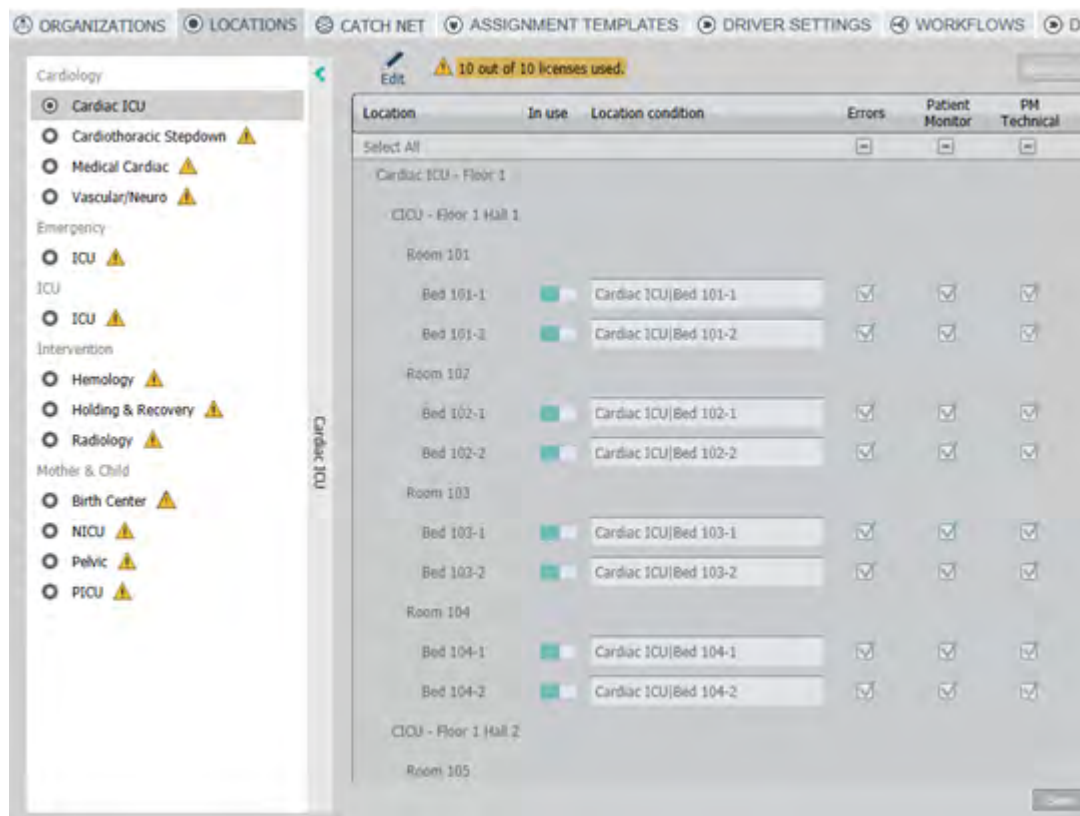
Additionally, the switch on left hand side of each location permits that location to be disabled, which prevents it from being visible in a number of locations throughout the Unite system. Locations should only need to be disabled when they are part of the location topology but are not used or do not contain clinical systems intended for integration.

5.6.2.1   Location Conditions – Driver-Specific

Dräger

When entering location conditions in Unite Admin for the Infinity Gateway Driver, the location conditions shall be entered in the format CareUnit|BedName where the Care Unit is the Dräger Care Unit and the Bed Name is the Dräger Bed Name.

When wireless beds are present in a configured unit, all of the wireless beds are polled for alarms (not just the configured wireless beds). Location conditions for wireless beds can be configured to be extracted in multiple ways, as shown in the infinity gateway driver settings.

When using the Patient Name, the Wireless Bed Label Delimiter is used to split the patient name and either the first (prefix) or last (postfix) value can be used as the external ID in combination with the Care Unit. For example, in Unit CU20, if the patient name is "1011 John Doe", when the settings Wireless Bed Label delimiter is a space, and settings Wireless Bed Label Source = PatientNamePrefix, then the bed identifier of "1011" is extracted. Therefore, to match this particular Wireless bed configuration, the Location Condition for this bed must be configured as CU20|1011.

When there are unknown wireless beds in a hospital unit, the unknown wireless beds will be replaced by <CareUnit>|* as a catch all location. To receive alarms for unknown wireless beds, a location condition will need to be created using the text "<CareUnit>|*", where <CareUnit> is the name of the care unit containing wireless monitors. For example, if the Care Unit is CU20, then CU20|* should be used in a location condition mapping to a catch all location where users can be assigned to receive alerts from the unknown wireless beds.

XprezzNet

The Location Condition configured in Unite Admin needs to match the Location Condition Type setting. The DeviceName, Bed, and DeviceLocation fields are received from XprezzNet and can be entered directly in the Unite Admin Location Condition. The DeviceNameOrBed Location Condition Type indicates that the driver will first attempt to use the DeviceName and if that is not found it will use the Bed field received from XprezzNet to identify the location.

The PatientID2 Location Condition Type can be used, typically with telemetry monitors, when Spacelabs XprezzNet puts the patient's admitted room into the PatientID2 field. In this case the same room identifiers shall be configured in the Unite Admin Location Conditions.

Digistat

Setting Digistat location conditions depends on which template version is being used:

Digistat Connect Version 6.0

When entering location conditions in Unite Admin for the Digistat Connect Driver, the location condition entered shall be the location name as defined in Digistat Connect. Typically, this does not include a reference to a Room, only a bed. (e.g., "ICU^^BED1").

Digistat Suite 7.1

In order to simplify the configuration required when installing a combined Digistat/Unite system, Digistat Version 7.1 uses the Unite location identifiers so that Digistat and Unite can share a known location. This eliminates having to configure Unite location conditions for Digistat. The following also applies:

- Even though the Unite PS integration location conditions do not need to be configured, the Events that apply to each location (Ventilator, Monitor, Pumps, etc.) still need to be selected.

- An alarm for a location can still be received when the Unite Location ID is provided.

- Loss of connectivity for a location can still be detected when the Unit Location ID is provided

GE CARESCAPE

When entering location conditions in Unite Admin for the GE CARESCAPE Unity driver, the location condition shall be entered in the format GECareUnit|GEBedName, for example: ICU|BED1

5.7   Nurse Call Location Mapping

Similar to Location Conditions, Location Mapping provides a method for establishing a relationship between the location description provided within every received Nurse Call Event and the corresponding location defined in Unite.

Location Mapping is an activity initiated when a Nurse Call location topology is first Synchronized (required). Synchronization is a method only available to specific integrations which support the Synchronization feature. These integrations are specifically denoted as "Integrated" integrations, such as teleCARE IP and Telligence Integrated.

Synchronization is a method whereby the location topology (structure associating Units, Rooms, Beds, and bathrooms together) which has already been established in the Nurse Call system, is read and understood directly from the Nurse Call system by the Unite Platform Server. Upon completion of synchronization, which occurs automatically upon adding a system component (NISM, IMT, etc.) of the Nurse Call System to the Unite Platform Server infrastructure, the entire location structure defined in the Nurse Call, is then available for mapping.

5.7.1   Organization Mapping

Before mapping locations, the organization(s) must first be mapped. Mapping of organizations can be performed manually within the Integration by associating the Nurse Call Organization to the Unite Organization on the Organization Mapping tab. When a Nurse Call organization is mapped to a Unite organization, the locations within those organizations can be mapped on the **Location Mapping** tab. Multiple Nurse Call organizations can be mapped to a single Unite organization. When this occurs, locations from all mapped Nurse Call organizations will be available to map to locations within the Unite Organization on the **Location Mapping** tab.
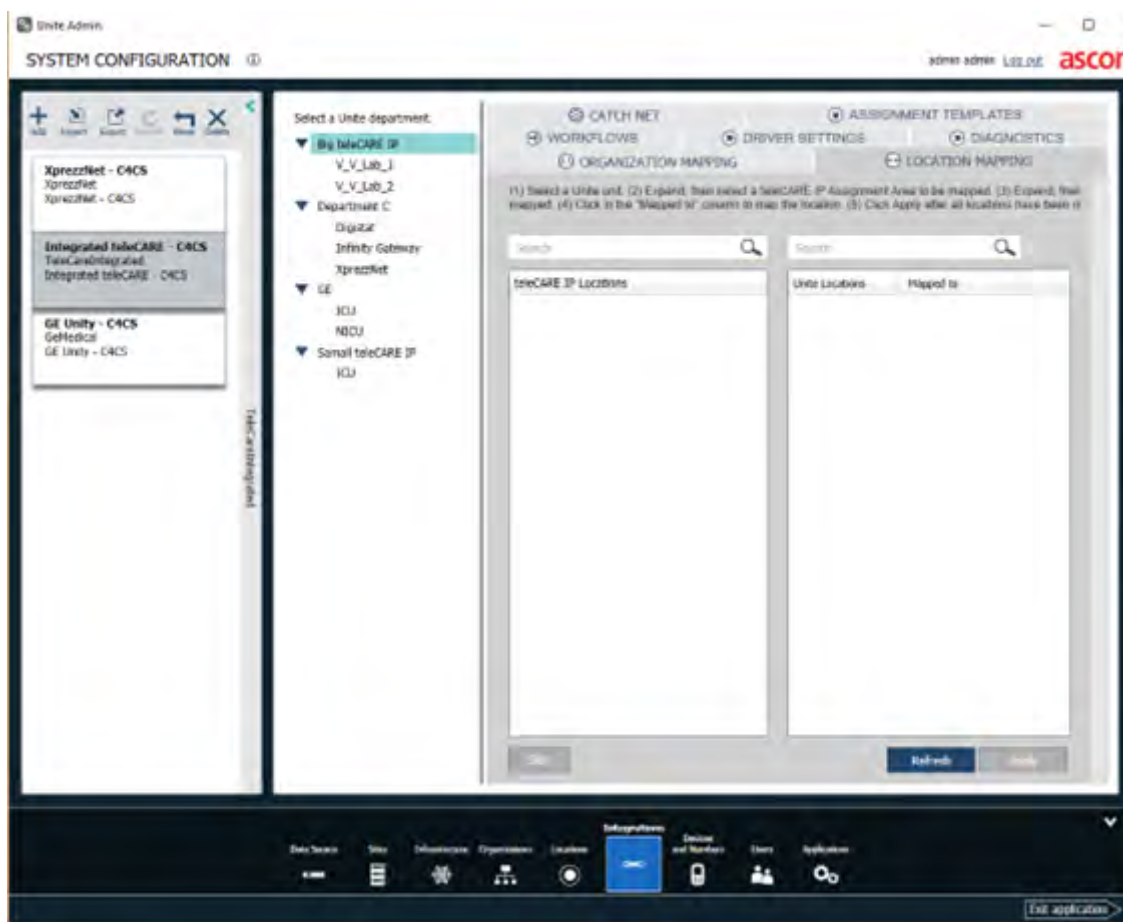
5.7.2   Location Mapping

Mapping of locations can be performed manually within the Integration by associating the Nurse Call Location to the Unite location using the provided UI. The process of manually mapping involves selecting a Nurse Call location followed by selecting the corresponding Unite location. Once all locations have been mapped, or updated through manually mapping, the changes can be applied (saved) by pressing **Apply**.

5.8   Location Importing

As an alternative to the manual Locating Mapping process described in the previous section, Location Importing can generate Location Maps automatically based on the information acquired during synchronization. Location Importing allows for automatic creation of a corresponding location structure in Unite that matches that of the Nurse Call and requires only the definition of {Empty} Department (no Unit).

Once the appropriate {Empty} Department is defined, the Nurse Call location topology can be "copied" into Unite, automatically creating corresponding Unite Locations for every Nurse Call location imported. Importing is performed on an entire Care Area/Unit at once but can only occur once for an Organization.

Nurse call locations are imported through Infrastructure in the Unite Admin. The nurse call server (i.e., NISM for teleCARE) must be selected, then the data can be imported through the Synchronized Data tab. The method for importing locations will differ depending on the host configuration being used.

The process not only creates a corresponding Unite Location (i.e. Room, Bed, Bath, etc.) with corresponding description (i.e. "Room 101") it will also establish a "Map" between the Nurse Call location and the Unite location. This can be observed after mapping the appropriate Nurse Call Care Area/Unit to Unite

Organization manually after creating an Integration (more info is available about creating an Integrations in future sections of this document).

> Organizations still need to be manually mapped, even if locations are imported

Locations can be imported from the nurse call system server (NISM/vNISM or IMT) in the **Infrastructure** tab as follows:

1. In the Infrastructure tab, select the server, then select the **SYNCHRONIZED DATA** tab.

2. Select one or more organizations from the list.

3. From the drop-down menu under **Location Import**, select the corresponding organization.

4. Select **Import Locations**.
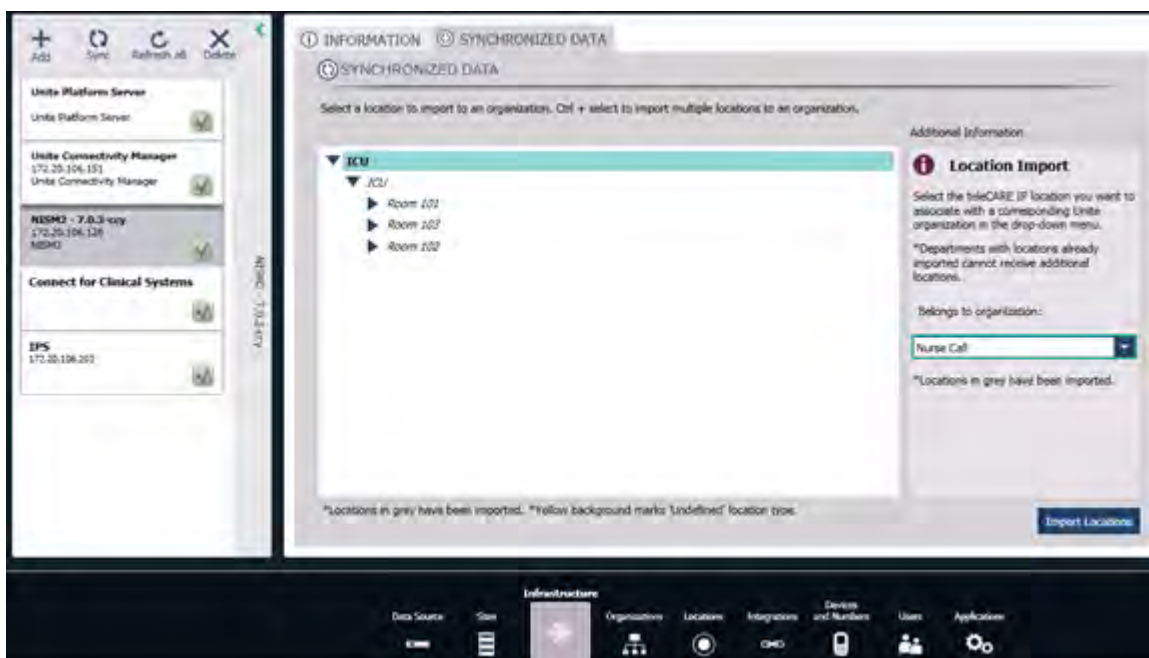
5. Repeat Steps 1 – 4 for all organizations in the Synchronized Data list.

6. Go to the Integrations tab and select the teleCARE IP integration.

7. Select a Unite Department; the department will appear in the Unite Department window.

8. Select from the teleCARE IP Assignment Area where it is to be mapped; it will appear next to the Unite Department entry under "Mapped to."

9. Repeat Steps 7 and 8 for all Unite departments.

5.9   Assignment Templates

Assignment Templates are a way to categorize alarms and alarm types processed by Connect for Clinical System so staff assignments can be properly made. Additionally, Assignment Templates provide a method to define the graphical icon which best represents the type of alarm that the Event is intended to be associated with and displayed in Unite Assign when using "Event-Based Assignments." This icon also accompanies the Alert when delivered on an Ascom display device.

Assignment Templates are configured with a Template Name, Template Description and an Assignment Type (Category), as shown below. The Assignment Type determines the icon that is shown on display devices.
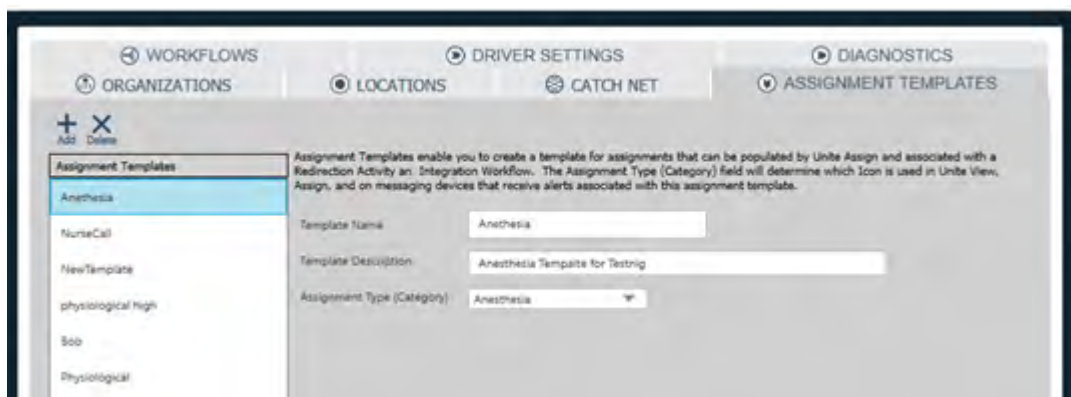
Setting	Description
Name	The name given to the Assignment Template. This name is displayed in the Assignment Template setting in the Redirection activity within Workflows, as well as in the Redirection tab as an assignable alarm in the configuration UI for Role-based Assign.
Description	Describe the type of alarm the Assignment Template represents.
Type	The Unite alarm category with which this Assignment Template is associated. The Unite alarm category provides categories of alarms to which staff assignments can be made in Alert-Based Assign and associates an icon with these categories in Alert-based Assign, Unite Axess and Myco.

The following table displays all assignable alarm "Types" identified by icons that can be associated with Assignment Templates and Drivers:

Icon	Assignment Type (Category)	Applicable Driver
	Anesthesia Delivery Unit	Digistat
	Blood Filtration	Digistat
	Blood-gas analyzer	Digistat
CODE A	Code A	Nurse Call
CODE B	Code B	Nurse Call

Icon	Assignment Type (Category)	Applicable Driver
☆	Custom Connect Category A	Custom Connect
⬚	Custom Connect Category B	Custom Connect
⊛	Custom Connect Category C	Custom Connect
△	Custom Connect Category D	Custom Connect
🛡	Custom Connect Category E	Custom Connect
🔔	Emergency Call Blue	Nurse Call
🫁	Heart-lung machine	Digistat
👶	Incubator	Digistat
💉	Infusion pump	Digistat
⚗	Lab Information System	Digistat
📟	Medical Alarm Blue	Nurse Call
👥	Nurse Assistance Blue	Nurse Call
🛏	Nurse call	NurseCall
⎍	Patient Monitor Blue	Patient Monitor
⚙	Technical Call Blue	Patient Monitor

Icon	Assignment Type (Category)	Applicable Driver
1👆 2👆	Pushbutton (specified as 1 or 2)	Nurse Call
👫	Toilet Call Blue	Nurse Call
⬯	Ventilator	Digistat
1 2 3 4 5	Workflow (Specified as 1 through 5)	Nurse Call

For some integrations, such as Nurse Call, there may be a 1-to-1 relationship provided by default within the default template between Assignment Templates and Workflows.

Example – Nurse Call

In the Workflows (shown below) the "Patient Call" Workflows makes use of the Assignment Template also named "Patient Call" within the Redirection Activity.

This signifies that role assignments associated with this Workflow should be configured under the "Patient Call" event for the Role Based Redirection Chains.

For Alert Type based Assignments the assignments for this Workflow would be configured for the Patient Call Alert type.

The icon associated with Type "Patient Call" will appear in the alert sent to Myco, Axess and Unite View.
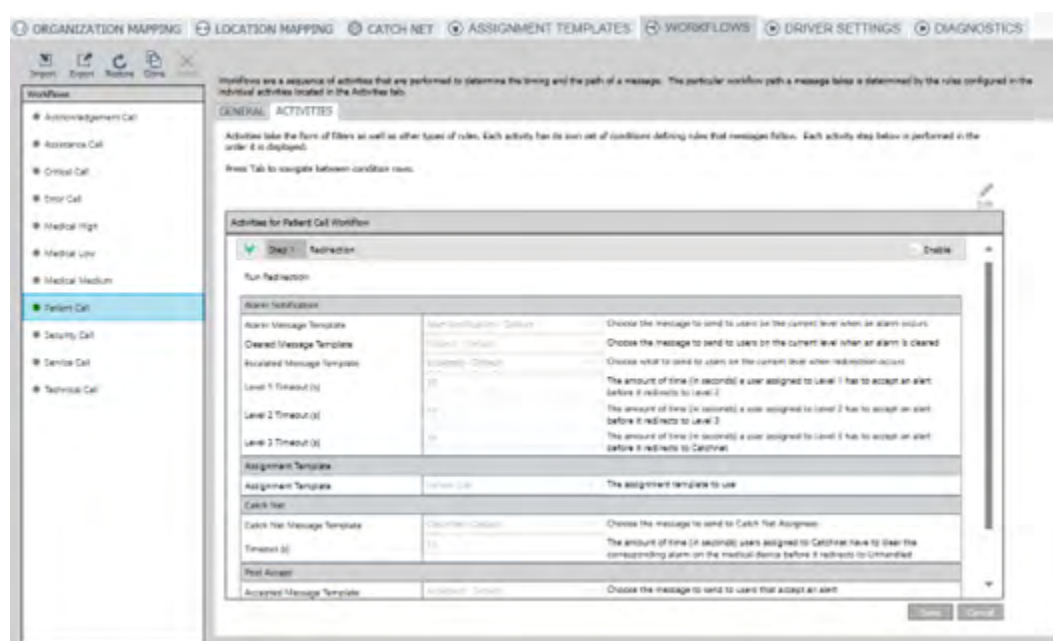
The default templates provided with other integrations may assume a many-to-1 relationship between Workflows and Assignment Templates. For instance, Patient Monitoring integrations can typically all utilize any one of two Assignment templates to differentiate between Technical and Physiological alarms

Example – Patient Monitoring

- Asystole, Tachy, Brady, and Vtach would typically belong to the Type "Patient Monitor."

- Leads Off and Low Battery typically would belong to the Type "PM Technical."

- The creation of one Assignment Template called "Physiological High" which can be associated with the Type "Patient Monitor," as shown below:
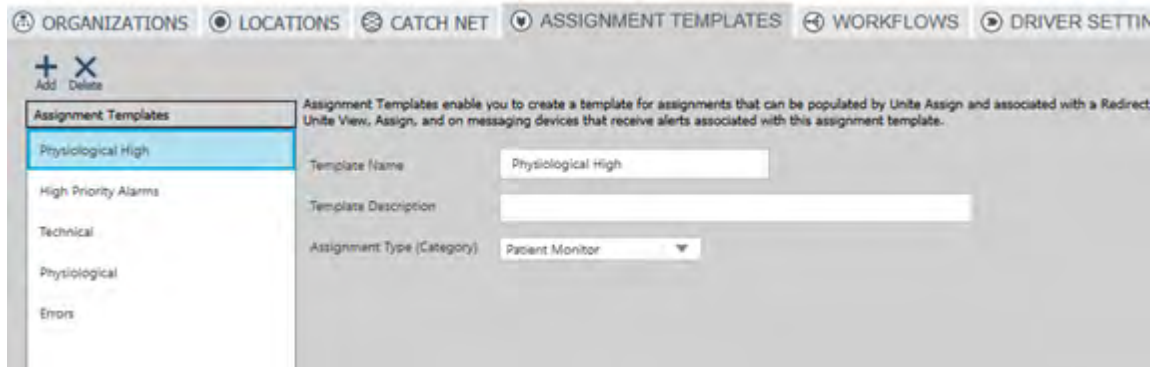
- A Workflow called "Physiological High Alarms." can be set with conditions based on the Priority Equal to High as a General Condition.

- Within the Activities of this Workflow a Pass Filter can be established to allow the selected high-priority alarms to "pass" through this Workflow (i.e., Asystole, Vtach, Vfib, HR High) as shown below:
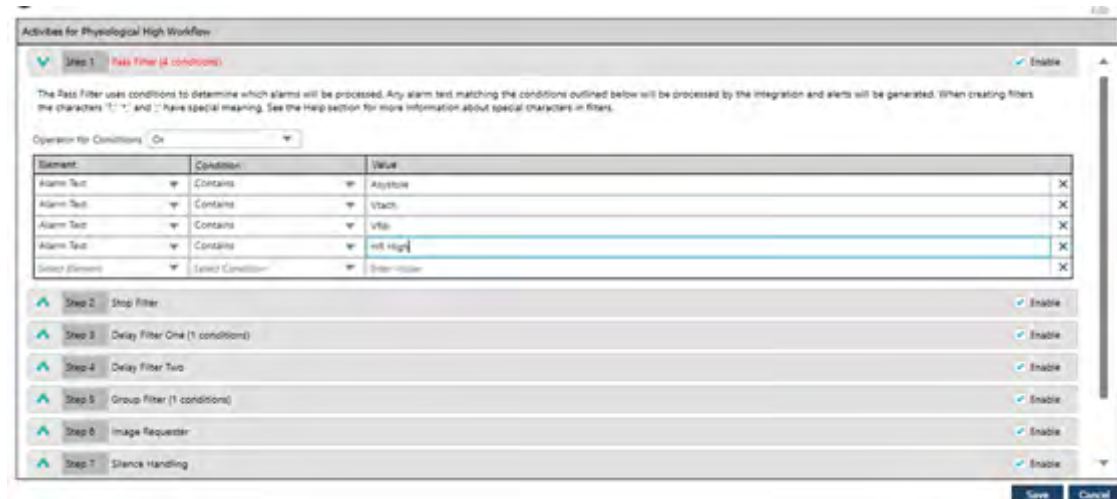
- In the Redirection Activity of this Workflow, the chosen Assignment Template, Physiological High, will define Assignments associated with the execution of this Workflows redirection behavior.

- In Role-Based Assign, role assignments can be defined based on the "Physiological High" Event for Redirection Chains configuration in Unite Assign.

- For Alert-Based Assignments, staff assignments can be made under the alarm Type "Patient Monitor."

- The icon associated with Type "Physiological" will appear in the alerts sent to Myco, Axess and Unite View.

5.9.1   Adding an Assignment Template

To add an Assignment Template:

1. Click the **Add** icon above the Assignment Templates column.

2. Type the name of the new template.

3.   Add a description of what alarms the template represents.

4.   Select a **Type** from the Assignment Type (Category) drop-down.

5.   Click **Save**

5.9.2   Modifying an Assignment Template

To modify an existing Assignment Template:

1.   Click the Assignment Template you wish to modify.

2.   Make changes to the Name, Description, and/or Assignment Type.

3.   Click **Save**.

5.9.3   Deleting an Assignment Template

To delete an Assignment Template:

1.   Click the Assignment Template you wish to delete.

2.   Click the **Delete** icon above the Assignment Templates column.

3.   A popup will appear asking you to confirm the deletion of the template.

4.   Click **Yes**.
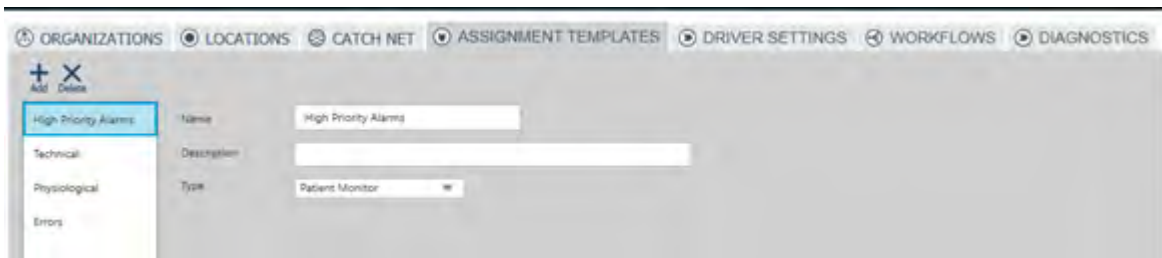
5.10   Import and Export a Configuration

After configuring an integration with applicable assignment templates, message templates and workflows, the configuration may need to be replicated at another site (i.e., a hospital chain of 6 hospitals can be configured at one site, and the configuration can then be duplicated at the other 5 sites). This is achieved by exporting the integration template, message templates and workflows and importing them to the other sites, eliminating the need to reconfigure the integration manually.

This process is intended to enable support for sharing an initial configuration from one site to multiple other sites during installation and provisioning.

The following content can be imported and/or exported:

1.   Integration template - contains the defined set of capabilities that receive, filter and distribute information from supported clinical systems using Connect for Clinical Systems Event Management.

2.   Message template - used to define alert structure and content.

3.   Workflows - defined behavior related to the distribution of alerts to display devices.

5.10.1   Single File Import/Export

The customized workflows, filters, assignment templates and message templates from an integration can be exported in a single file. This single file can then be imported as a new integration template at another site for reuse. The single file export contains:

- All integration Assignment Templates.

- All integration Workflows (including global filters).

- All Message Templates in use by the Integration.

Importing the configuration on another customer site results in a new integration template that is available for selection when creating integrations. Once an integration is created using this new template, it is not possible to update that integration by importing an updated template. If an updated template is imported, the integration must be re-created to take advantage of the updated integration template.

5.10.1.1   Single File Export

Use **Export** to export the Integration as a template from a selected integration.

1.   Select the integration in which you wish to export it as a template. In this example, we are exporting the GE Unity - C4CS integration.
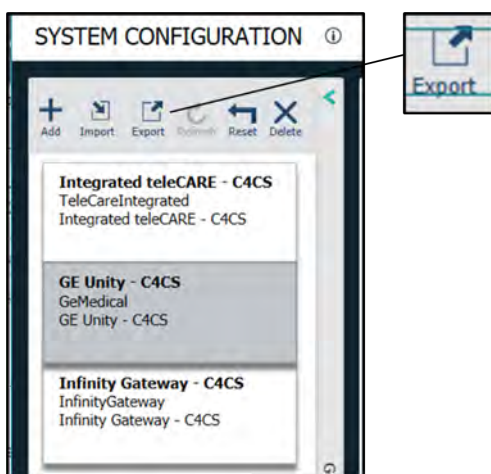
2.   Click **Export** in the left pane.

3.   Select **Export As New...**.
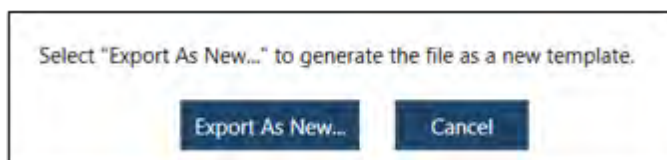
4.   Specify the name of the new template and the location where it will be saved. For this example, it is called "GE Unity Integration C4CS," Then click **Save and Continue**. The following message appears: "Your template has been generated and is ready for export."
.Specify where you want the integration to reside. In this example it is saved to the Desktop folder.

5.   Click **OK** to acknowledge the template has been generated.

Confirm the file name of the new template, then click **Save**.

5.10.1.2   Single File Import

The Single File Import is accomplished by importing an integration template.

Use **Import** to update an existing Integration template or to add a new template to your system.

1.   Click **Import** in the left pane.

2.   Browse for the location of the template to be imported. In this example it is in the Desktop folder.

3.   Select the template ("GE Unity Integration C4CS" in the Desktop folder) and Click **Open**.

4.   The message appears "The import is complete." Click **OK**.

5.   Add the imported integration. See 5.2 Adding an Integration and Selecting an Installation, page 35. In this example the system that should be selected is "GE – Carescape MC Network." The template is located under the selected system.

6.   Under "GE – Carescape MC Network" select "GE Unity Integration C4CS."
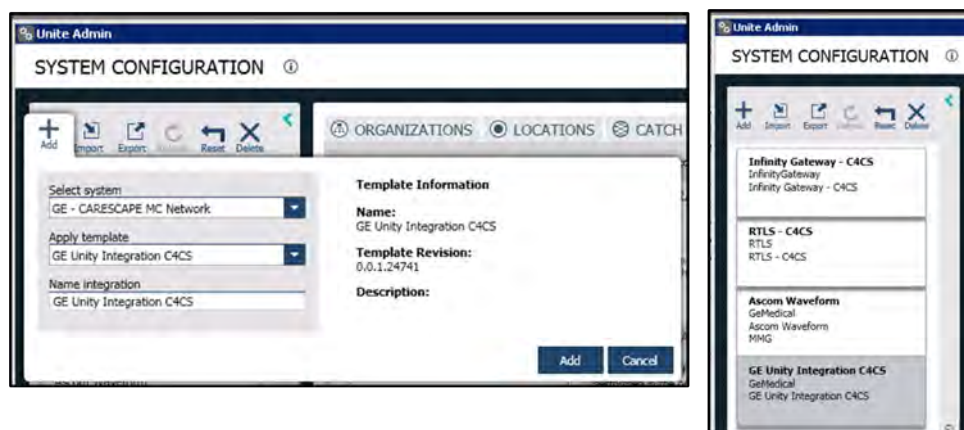
5.10.2   Export

Export an Integration as a Template

To export the integration template, which includes the Assignment Templates, follow the steps in 5.10.1.1 Single File Export, page 53.

Export Message Templates

All Message Templates currently referenced by a Workflow MUST be exported in order for importing of Workflows to work properly.

Export message templates as follows:

1.   Locate the file "ExportImportTemplates.exe" utility and launch it by double-clicking it. The default file path to the utility is "C:\Program Files\Ascom\Ascom Unite Aware\Unite System Core \MessageCompo-sitionService\ExportImportTemplates\."

2.   Double click the file to run the utility and follow the instructions in the command prompt window.

3. Type "1" to export a template by GUID. Where the GUID is a unique identifier assigned to the specific message template, as it is known by the software.

    The GUIDs assigned to each message template, known by the software, are identified within a specific table within the Unite database (i.e. the database holding all of the configuration information defined for the Unite PS). The individual GUIDs can be read from the database utilizing SQL Server Management Studio and by executing the following query on the Unite PS database.

    SELECT * FROM [Unite].[MessageComposition].[EventHandler_pda_def]

    The syntax of the query above assumes the database in question is named Unite, the name of the database should be modified to reflect the database naming convention chosen for your customer.
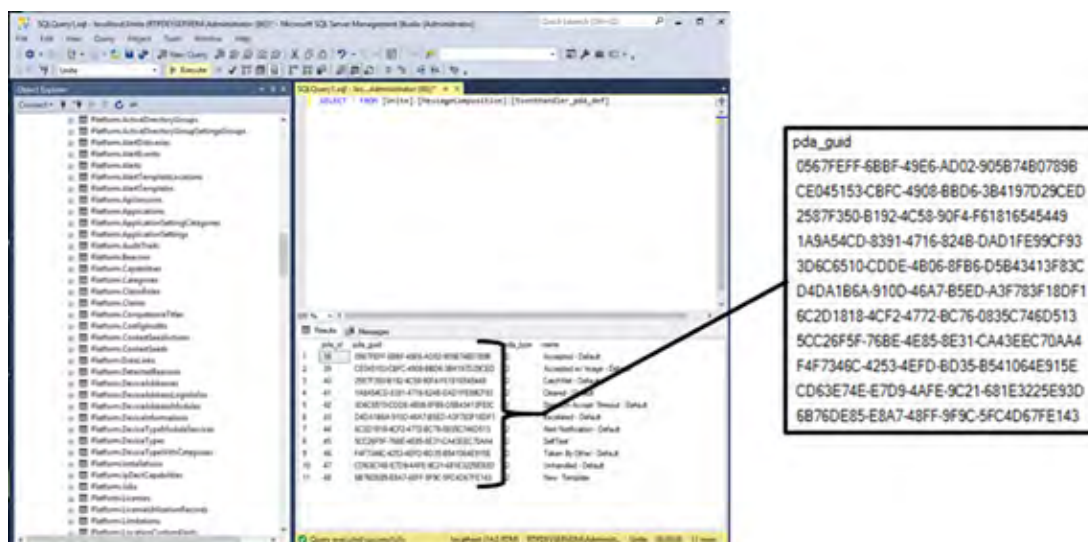
The Message Template Export utility can export templates individually or as a group by specifying a number of GUIDs in single expression.

To generate a single expression with a number of GUIDs identified, the results of the above query can be copied and pasted into an editor like excel or notepad in order to combine them into a single string separated by commas.

4. After entering these GUIDs to export, they will appear in the Export folder.

> The default location for the templates for export is: `C:\Program Files\Ascom\Ascom Unite Aware\Unite System Core\MessageCompositionService\ExportImport-Templates\Exports\`.

> When exporting templates, files in the "Exports" folder with the same file name are overwritten.
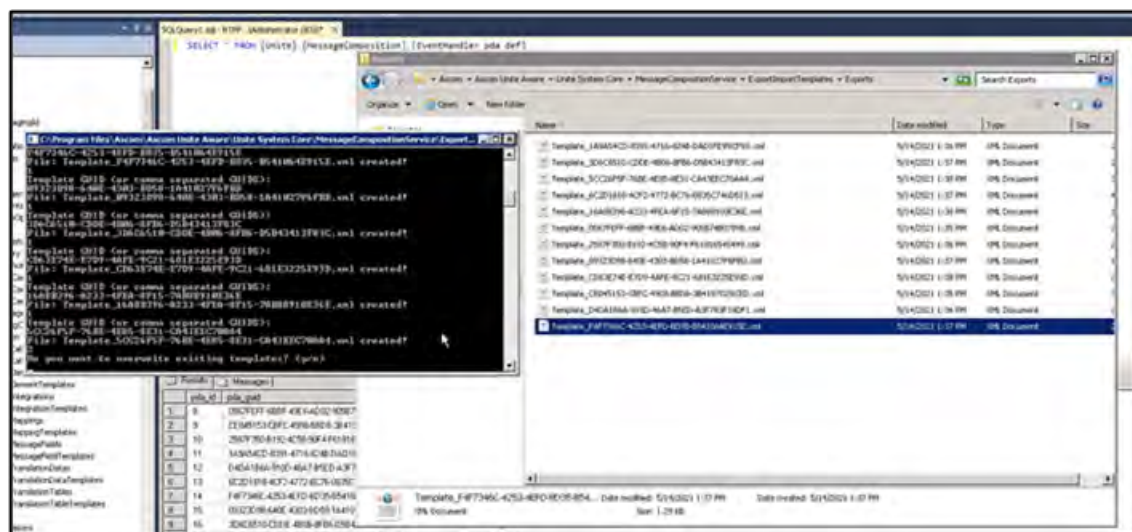
Export Workflows

Exporting Workflows allows for the specific configuration of all Activities and Conditions related to all Workflows to be exported to a file that can then be restored to the same or a different system. Exporting can be useful to maintain a separate backup of just the Workflows and is also useful if a specific set of Workflow configurations should be made available on a separate system.

To Export Workflows:

1. Select **Export**.
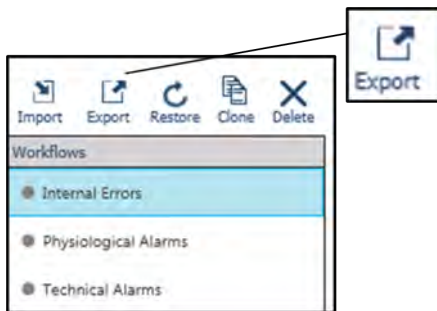
2. When prompted, provide a location and name to save the exported Workflow File. In this example it is being saved as "GE Unity C4CS_Workflows_2021-05-14_15-39.xml" in the Desktop folder.
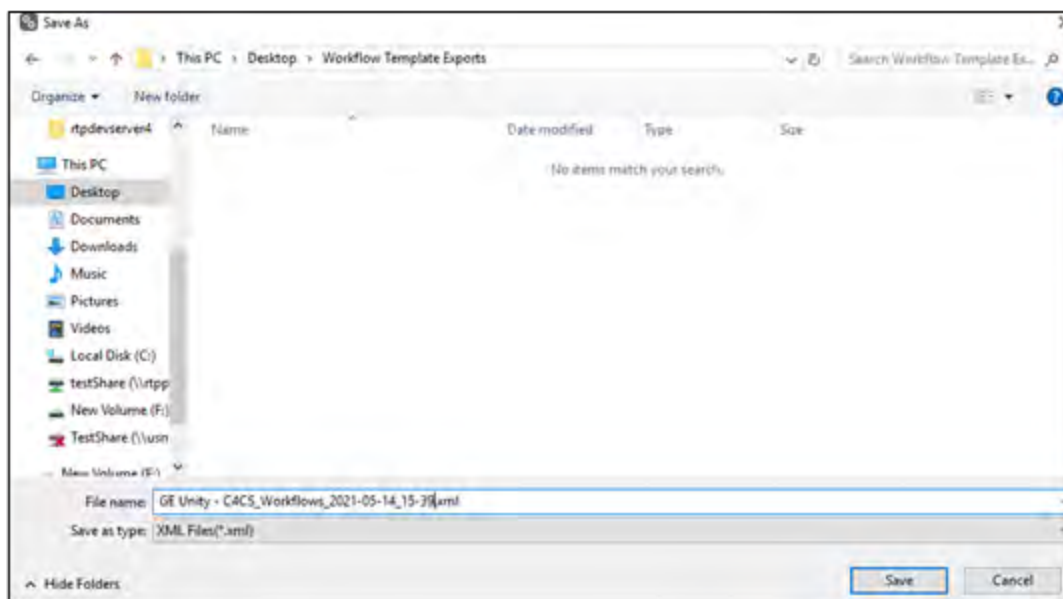
3. Click **Save**.

5.10.3   Import

Import an Integration Template

To import the integration template, which includes the Assignment Templates, follow the steps in .

Import Message Templates

The default location for the Message Templates for import is:`C:\Program Files\Ascom\Ascom Unite Aware\Unite System Core\MessageCompositionService\ExportImportTemplates\Imports \`.

> The user must have rights to modify, write, and read the folder.

Import message templates as follows:

1. Locate the Export Import Template utility (i.e., "ExportImportTemplates.exe") and double-click it. The default file path if the utility is: `C:\Program Files\Ascom\Ascom Unite Aware\Unite System Core \MessageCompositionService\ExportImportTemplates\`.
2. Double click the file to run the utility and to follow the instructions in the command prompt window.

3. Copy all the previously exported Message Templates from their location (see Export Message Templates, page 54) and paste them into the Import directory.
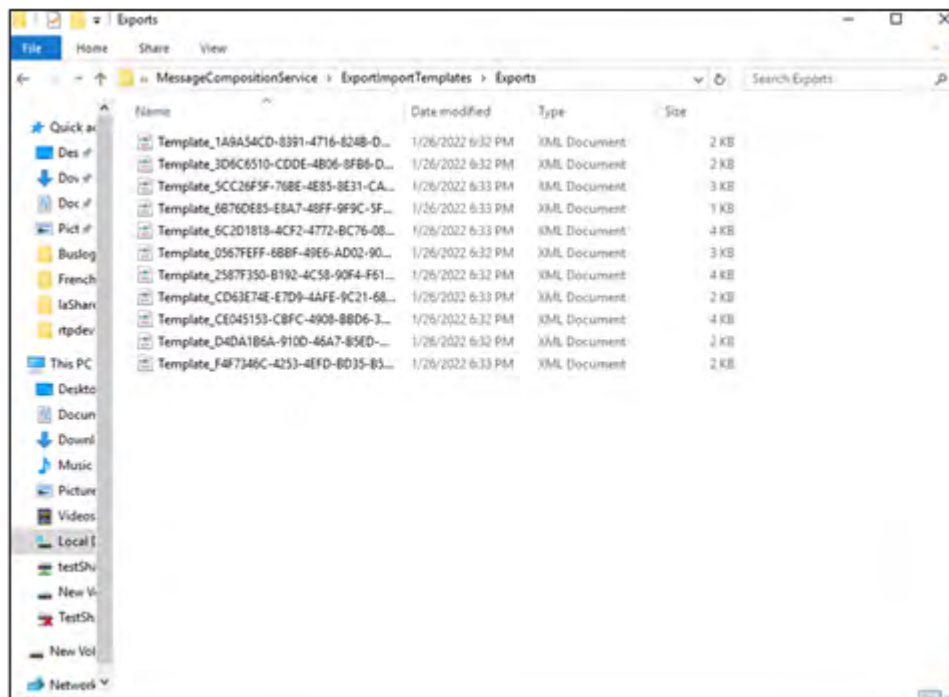
4. In the utility window, select **2** to import the files. If you want to override the files, select **y**.

Import Workflows

Importing Workflows allows for the creation of pre-configured Workflow to be added to a system. The imported Workflows are a result of the Export function described in Export Workflows, page 56. This is the final step in importing a configuration.

To Import Workflows:

1. Select Import from above the list of Workflows in the "GE Unity Integration C4CS." Integration.
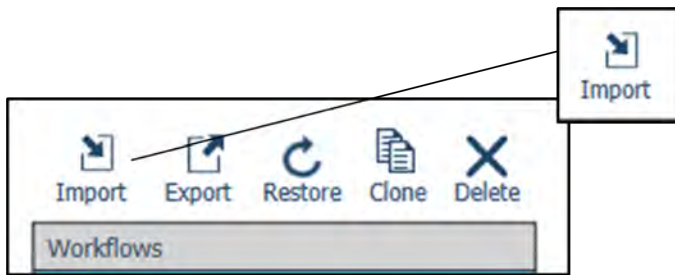
2. When prompted go to the Desktop folder location and select "GE Unity C4CS_Workflows_2021-05-14_15-39.xml."

3. Select **Open**. The following message appears and the imported Workflow that was exported in Export Workflows, page 56 shows up in the interface.
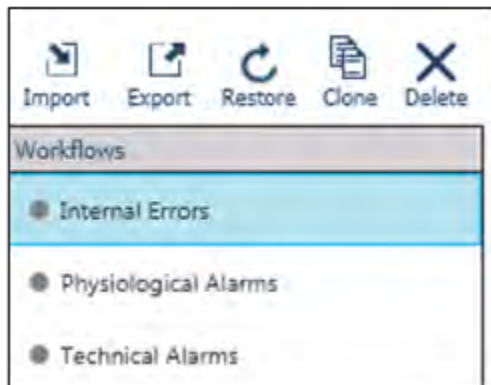
6   Workflows

Configurable Workflows define the behavior related to the distribution of alerts to display devices.

6.1   Global Filters

All filter settings and configurations are set up during installation and configuration and should reflect only those settings requested by the healthcare facility, the clinical user, and their operators.

Information related to configuration of each filter and its parameters must be recorded and provided for agreement and sign-off by the appropriate representative of the healthcare facility.

The Global Filters execute Stop, Group and Pass filters globally for each integration. The conditions added to the Stop, Group or Pass filter will determine which alarms will or will not be processed by Workflows.

Filters are provided as a method to prevent the unnecessary processing of those alarms that are NEVER intended to be distributed as alerts per Integration type.

⚠	**Caution**
	Operation of the product without adequate consideration of filtering can impact performance and negatively impact user adoption of the product.

Additionally, Global Filters do the following:

- Greatly simplify the configuration of Workflows so that only actionable alarms need to be considered.

- Prevent unwanted behaviors that may arise from persistent alarm conditions which may otherwise impact the starting and terminating of specific Workflows.

- Alarms and alarm updates filtered by Global Filters are not processed within Workflows. If there are no Stop, Group or Pass filters defined, all alarms and alarm updates will be processed.

- The Edit function disables the Global Filters tab until Save or Cancel is selected.

- When a Pass, Group or Stop Filter is selected for editing, it should be enabled with the slider as shown below in order to add edits and to save them:
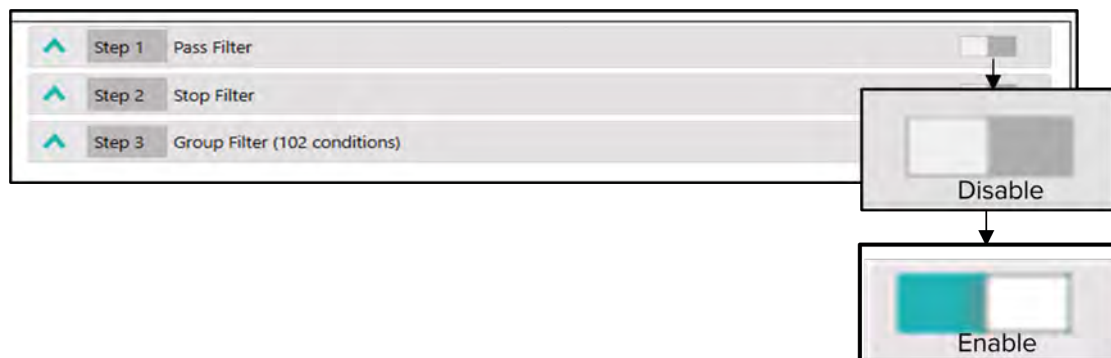
6.1.1 Pass Filters

All alarms with alarm text matching any of the pass filters are passed for further processing and if there are no matches, then that alarm is stopped. If no pass filters are configured, then all alarms are accepted for further processing. Failure to properly define parameters within the pass filter may impact performance and increase latency in the delivery of alarms to handsets. In a scenario where a hospital wants an alarm processed by some, but not all units, pass provide the ability to allow specific alarms to be processed by a subset of units.
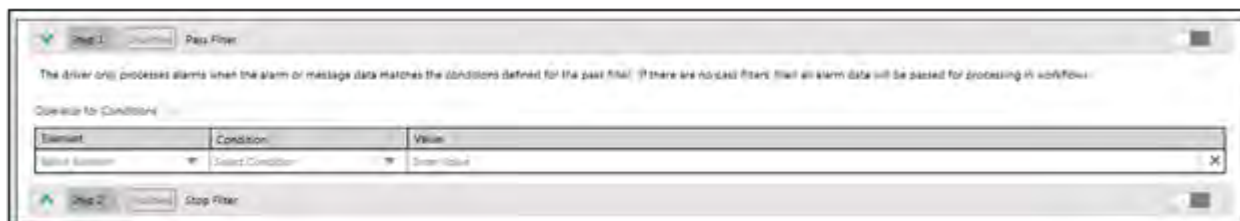
6.1.2 Group Filters

A healthcare facility may determine that certain alarm conditions do not require additional notifications to display devices. Group Filters reduce the number of unnecessary alarm updates that are delivered by comparing alarm updates to a previously delivered active alarm. Active alarms with updates that match a Group Filter will be stopped. If the alarm text does not match an active Group Filter that alarm will be passed on to the display device.

The **Restart on Higher Priority** setting has the following options:

- **Only Higher Priority** - if a filter expression is matched and an alarm update is received that matches the same expression but has a higher priority, the group filter allows it to pass to the display device.

- **Any Priority** - if a filter expression is matched and an alarm update is received that matches the same expression but has a higher priority OR a lower priority, the group filter allows it to pass to the display device.

When the **Restart on Higher Priority** setting is **Disabled** (default), if a filter expression is matched and an update is received that matches the same expression, the group filter will stop the update from being sent to the display device, even if the priority is higher or lower.

The **Update Rate** is the rate at which a display device will, after the onset of an alarm condition, continue to receive alarm updates for a physiological event that is handled by a Group Filter. The update rates available are: 30, 60, 75, and 90 seconds. If **Update Rate** is disabled, the group filter will only allow the distribution of the onset of an alarm condition and it will prevent any updates related to the ongoing alarm condition.

> **⚠ Caution**
>
> Operation of the product without adequate consideration for the impact of frequent alarm updates which may occur as a result of an improperly configured medical device can impact performance and negatively impact user adoption of the product.
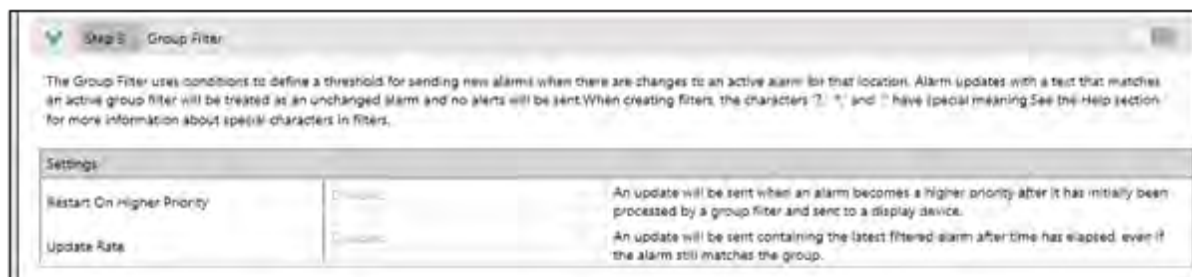
6.1.3   Stop Filters

All alarms with alarm text matching any of the stop filters will be stopped. If there are no matches to any stop filters, then that alarm is passed through. In a scenario where a hospital doesn't want an alarm processed by every unit, stop filters allow specific alarms to be ignored by a subset of units.
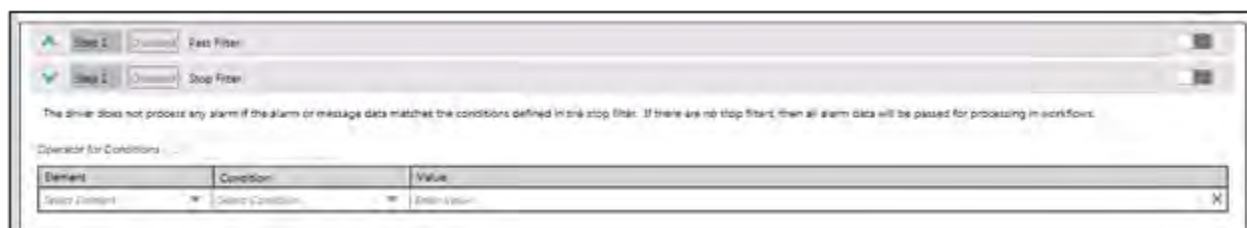
6.2   Workflow Configuration

When the **Workflows** tab is selected, the **Workflow Configuration** subtab is selected by default. Each Integration provides its own specific set of default Workflows specifically tailored to the Integration. The default configurations for all Connect for Clinical Systems Integrations utilize configurable Workflows. Each Workflow allows for configuration of assignment patterns for up to 3 levels of redirection and supports customizing of the alert content and redirection behavior, including but not limited to redirection timeouts.

6.2.1   Enable/Disable Aggregation in Workflows

When this feature is enabled, if multiple alarms occur simultaneously for one device at the same location and match the conditions for a workflow where alarm aggregation is enabled, the individual alarms are collected into a single alert or alert update. The "History Text" event element is updated and can be optionally added to the Message Body of an alert. The History Text will indicate any previously received alarms and any other active alerts for that location since the initial alert was delivered to a display device.

When this feature is disabled (the default for all integrations excluding Digistat), each alarm triggers a separate workflow instance and generates a separate alert that is handled independently as a separate driver event reported by the driver.

6.2.2   Clear a Workflow when Alarm Conditions are not Matched

A workflow can be configured to terminate when conditions no longer match the Workflow, while the device and location potentially remain in an alarm state. When the "Clear On Unmatched Update" option in

the General tab is enabled (disabled by default) and the highest priority alarm condition of the medical device no longer matches the conditions of a workflow, the workflow is terminated. This will (by default) generate an indication sent to display devices indicating the alarm condition cleared status.
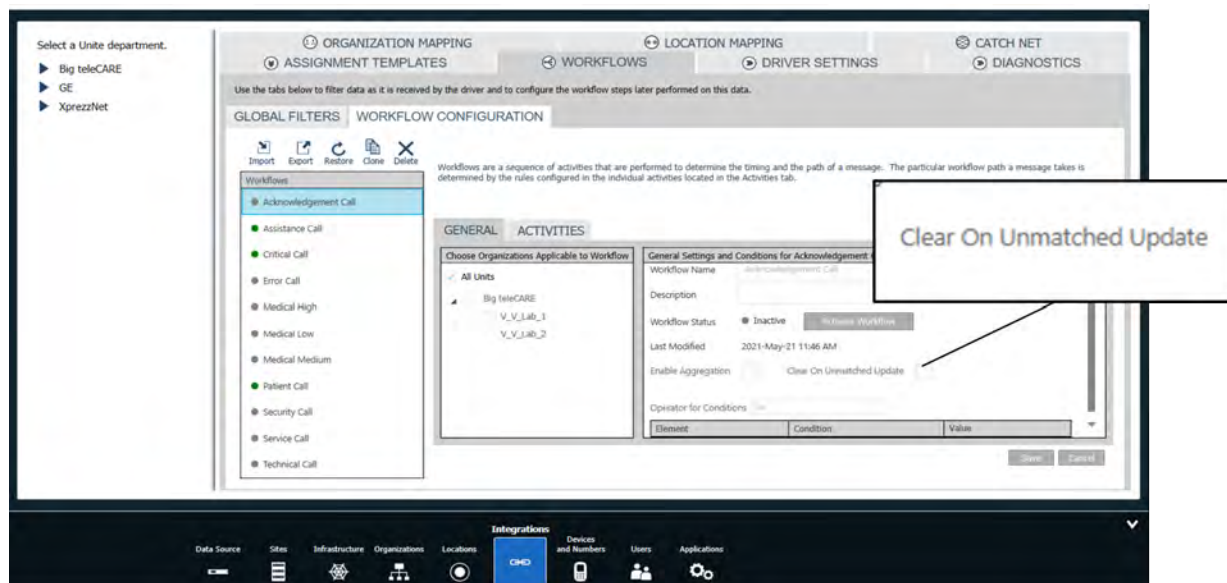
This feature allows alarm prioritization behavior where only the highest priority alert is visible (e.g., when making a patient call by pressing the red key, followed by making an assistance call by pressing the yellow key, without cancelling the patient call first, the patient call is cleared and an assistance call is active. This can be overruled by a higher priority alarm, like emergency call, which will make the emergency visible and clear the assistance call).

6.2.3 Default Workflows

Default Workflows – Digistat Driver	
Workflow	**Description**
Anesthesia	Processes alarms sent from Anesthesia Delivery Units.
Dialysis	Processes alarms coming from Dialysis.
Blood Gas Analyzer	Processes alarms coming from Blood Gas Analyzers.
Internal Errors	Processes device errors.
Heart Lung Machine	Processes alarms coming from Heart Lung machines.
Incubator	Processes alarms coming from Incubators.
Infusion Pump	Processes alarms coming from Infusion Pumps.
Patient Monitor	Processes alarms coming from Patient Monitors.
Ventilator	Processes alarms coming from Ventilators.
Default Workflows – GE Unity Driver	

Workflow	Description
Internal Errors	Processes device errors.
Physiological Alarms	Processes physiological alarms, i.e. alarms initiated by a physiological condition in the patient, such as tachycardia or asystole.
Technical Alarms	Processes technical alarms from the patient monitor, such as lead off or low battery.
Default Workflows – Infinity Gateway	
Workflow	**Description**
Internal Errors	Processes device errors.
Physiological	Processes physiological alarms, i.e. alarms initiated by a physiological condition in the patient, such as tachycardia or asystole.
Default Workflows – teleCARE IP	
Workflow	**Description**
Acknowledgment Call	Processes Acknowledgment Calls from the nurse call system.
Assistance Call	Processes a request for assistance through the nurse call, i.e., when the assistance button is pressed on the nurse call at the patient's bedside.
Critical Call	Processes the Critical Calls from the nurse call system.
Error Call	Processes device errors.
Medical High	Processes high-priority alarms coming from medical devices which are connected to the nurse call system via the high-priority auxiliary input.
Medical Low	Processes low-priority alarms coming from medical devices which are connected to the nurse call system via the low-priority auxiliary input.
Medical Medium	Processes medium-priority alarms coming from medical devices which are connected to the nurse call system via the medium-priority auxiliary input.
Patient Call	Processes nurse calls which are initiated by the patient or patient family using a button on the pillow speaker or nurse call system.
Security Call	Processes security calls coming from the nurse call system.
Service Call	Processes service requests or calls from the nurse call system.

Technical Call	Processes technical calls from the nurse call system.
Default Workflows – Telligence	
Workflow	**Description**
Assistance	Processes a request for assistance through the nurse call, i.e., when the assistance button is pressed on the nurse call at the patient's bedside.
Auxiliary Emergency	Processes Auxiliary Emergency calls from a nurse call system auxiliary input station.
Auxiliary Priority	Processes Auxiliary Priority calls from a nurse call system auxiliary input station.
Bath/Toilet Call	Processes a bathroom or toilet call from the nurse call system.
Bed Exit	Processes Bed Exit (bed empty) calls from the nurse call system.
Code Call	Processes a code call from the Nurse Call system patient station and linked stations.
Code Pink/Fire	Processes code pink (pediatric)/fire calls from the nurse call system.
Cord Pull	Processes cord pull calls from the nurse call system.
Emergency Call	Processes emergency Calls from the Nurse Call System.
Family	Processes family Calls from the Nurse Call System.
Housekeeping	Processes Housekeeping Calls from the Nurse Call System.
Lavatory Emergency	Processes Lavatory Emergency Calls from the Nurse Call System lavatory station.
Medical Call	Processes Medical calls from the Nurse Call System.
Nurse Call	Processes basic patient calls from the Nurse Call System.
Patient Emergency	Processes Patient Emergency Calls from the Nurse Call System.
Patient Normal	Processes Patient Normal Calls from the Nurse Call System patient station.
Patient Priority	Processes Patient Priority Calls from the Nurse Call System patient station.
Room Alarm	Processes Room Alarm Calls from the Nurse Call System.

Room Alarm 2	Processes Room Alarm 2 Calls from the Nurse Call System.
Rounding Task 1	Processes nurse call rounding tasks for roles with level 1.
Rounding Task 2	Processes nurse call rounding tasks for roles with level 2.
Rounding Task 3	Processes nurse call rounding tasks for roles with level 3.
Service Task 1	Processes nurse call service tasks for roles with level 1.
Service Task 2	Processes nurse call service tasks for roles with level 2.
Service Task 3	Processes nurse call service tasks for roles with level 3.
Staff Emergency	Processes staff emergency calls from the Nurse Call System staff emergency station.
Staff Normal	Processes Staff Normal calls from the Nurse Call System.
System Error	Processes System Error calls from the Nurse Call System.
Technical Call	Processes technical calls from the Nurse Call System.
Urgent	Processes urgent calls from the Nurse Call System.
Workflow	Processes Workflow (e.g., rounding, one-button dialing, room empty, Housekeeping required) calls from the Nurse Call System.

Default Workflows – XprezzNet Driver	
Workflow	**Description**
Internal Errors	Processes device errors.
Physiological	Processes physiological alarms, i.e. alarms initiated by a physiological condition in the patient, such as tachycardia or asystole.

Physiological Alert Workflows are intended to be used as a result of alarms triggered for alarms/events received from an external clinical system. The priority and the associated indication Physiological Alert Notification Events, are based on the priority event/alarm identified by the source of the alarm (i.e., the external clinical system).

Connect for Clinical Systems can distinguish between at least 3 distinct priority levels, High, Medium and Low, conforming to audible and visual alarm standards.

Technical Alert Workflows are intended to be triggered for other events related to the operation of the external system. These triggering events are directly communicated from the external clinical system. Additional information received from an external system related to the operational status of a device/system can also be communicated by a Technical Alert Workflow.

Internal Error Workflows occur as a result of events monitored & triggered internally by Connect for Clinical Systems. For example, loss of connectivity to an external clinical system (in whole or in part) will by default trigger an Internal Error Workflow or System Fault.

Once a Workflow is active for an Integration, Device and location within Connect for Clinical Systems it will remain in the Active state until it has been terminated by the alarm source.

A Workflow is a combination of configured Activities within Connect for Clinical Systems that can filter alerts, suppress alerting when silenced, request waveform snapshots to accompany an alert and define the redirection behavior. The collection of specific configurations of the Activities make up each Workflow, and each Workflow can be utilized by multiple units for an integration, or can be unique to a unit, device, priority or alarm/event received from an external clinical system.

Activities within C4CS allow an installation engineer to alter the behavior and distribution of alerts related to the individual events and alarms received from external clinical systems. The configuration of these individual Activities represents the desired Workflow and expectations of a specific clinical environment.

Activities can be used to discard, group, or delay certain incoming alarms before an alert is delivered to client display devices. Activities represent functions that, when enabled, provide intelligent handling of alarms and alerts.

Filtering Activities can be used to prevent unwanted events and alarms from passing through to clinical users and operators.

All Activities can be individually enabled or disabled. When one Activity is disabled, it will have no effect on the distribution of an alarm, while the remainder of Activities within the Workflow will remain enabled. Not all activities are enabled by default; therefore, when an activity is selected for editing, it must be enabled in order to add edits and save them.

The specific expectations and configuration of Activities, including filter logic, should be defined and discussed before the installation process begins. A thorough understanding of the configuration should be disclosed to all users and agreed upon before final acceptance testing and configuration sign-off.

6.2.4 Unit-Based Configuration

Connect for Clinical Systems allows an installation engineer to configure Workflows (and thus, Activities) for individual care units. Under the "Choose Organizations Applicable to Workflow" column, one or more care units can use a Workflow, and alarms in that care unit will be processed according to the Workflow configuration. If the installation engineer wants to configure the Workflows to be applicable to all the units, "All Units" can be selected to enable alarms in all the organization's care units to respond to the Workflow configuration. When "All Units" is selected, the care units under it cannot be selected individually. If configuring individual units, the "All Units" must be deselected.

Different care units can be assigned to specific Workflows (or, collections of Activities) with specific configurations, depending on the unit's needs. Multiple care units can be assigned to one Workflow.

To configure Workflows:

1. Choose the Workflow you wish to configure.

2. Prior to clicking Edit, ensure that the workflow is in the inactive state. Clicking Edit for an active workflow will prompt the message "Workflow must be inactive before modifications can be made."
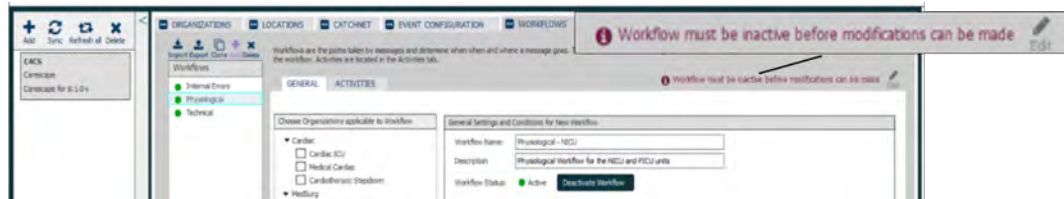
3. If a chosen Workflow is active, deactivate it for editing. Then click **Save**.

4. Click **Edit**, in the upper right-hand corner.

5. By default, **All Units** is selected. To configure a Workflow for a subset of units, deselect All Units. Select the unit checkboxes for units that will be using the existing Workflows. To select all the units in a department, select the Department-level box. To deselect all Units in a department, deselect the Department-level box.

6. If one or more hospital units would benefit from specific configurations not represented in the existing Workflows, then clone one of the existing Workflows (see 6.2.5.1 Cloning, page 70).

7. To modify the Workflow settings, such as Workflow name, description, or conditions, click **Edit**. When finished with modifications, click **Save**. If a Workflow change is made and not saved, a user will see the notice displayed below.
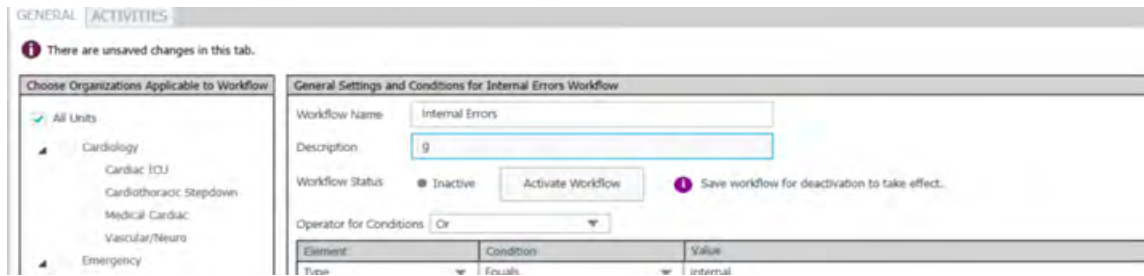
8. To configure an Activity within the Workflow, click the Activities tab.

9. Click **Edit.** Expand the Activities that need configuration by clicking the green arrow on the far-left end of each Activity bar. To configure conditions or settings within the **Activity** tab, see chapters below.

10. Click **Save**. If a change is made within an Activity and the change is not saved, a user will see the notice displayed below.
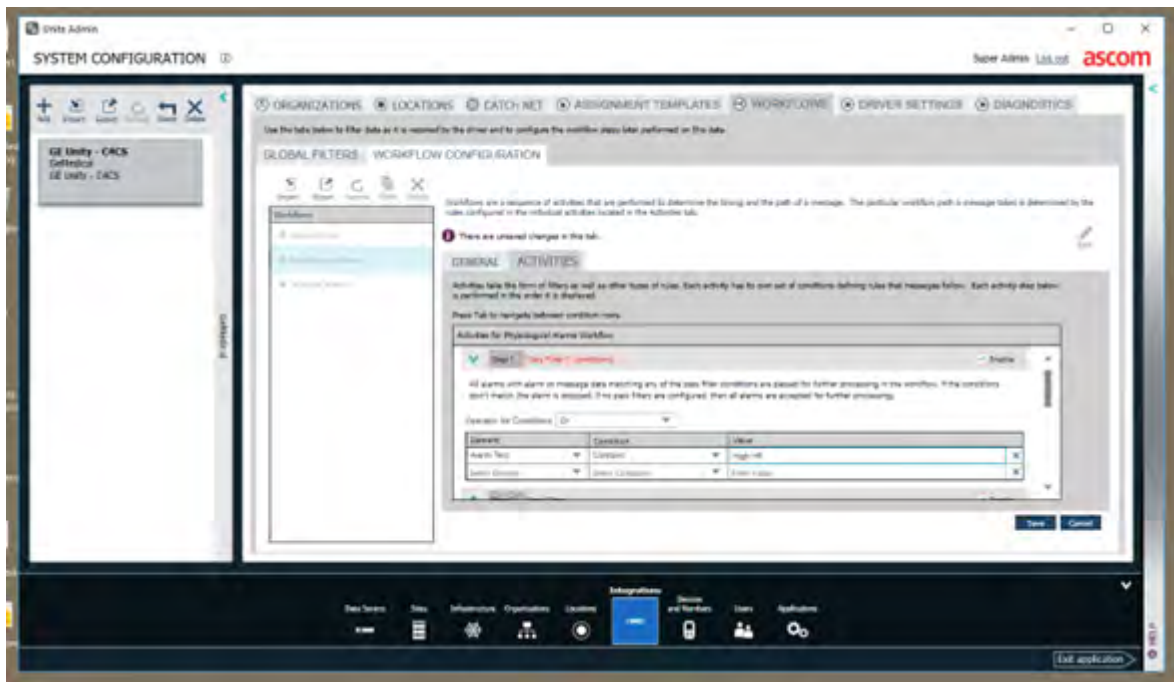
11. Ensure that the Activity is enabled.

12. Return to the **General** tab.

13. Activate the Workflow.

14. Click **Save**.

If no unit is selected, the following warning indicator will appear.
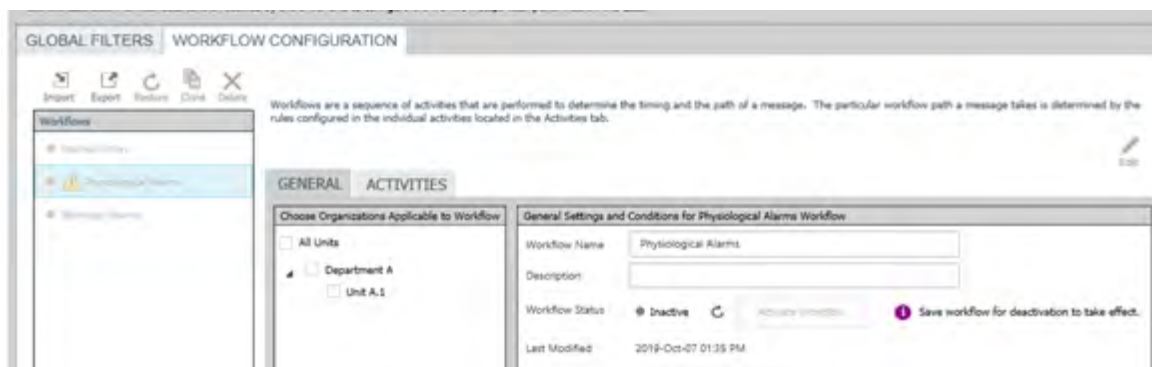
Active Workflows cannot be deleted. If a user attempts to delete the Workflow, the following hover-text will appear next to the Delete button: "Active Workflow(s) cannot be deleted."
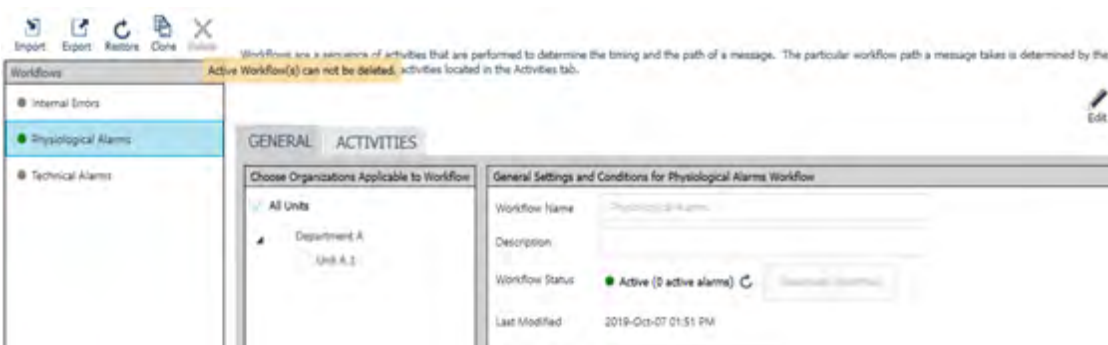
When in the Activities tab, a user can hover over the Workflow options to see which Units are active in that Workflow. In the example below, All Units are active in the Physiological Workflow:
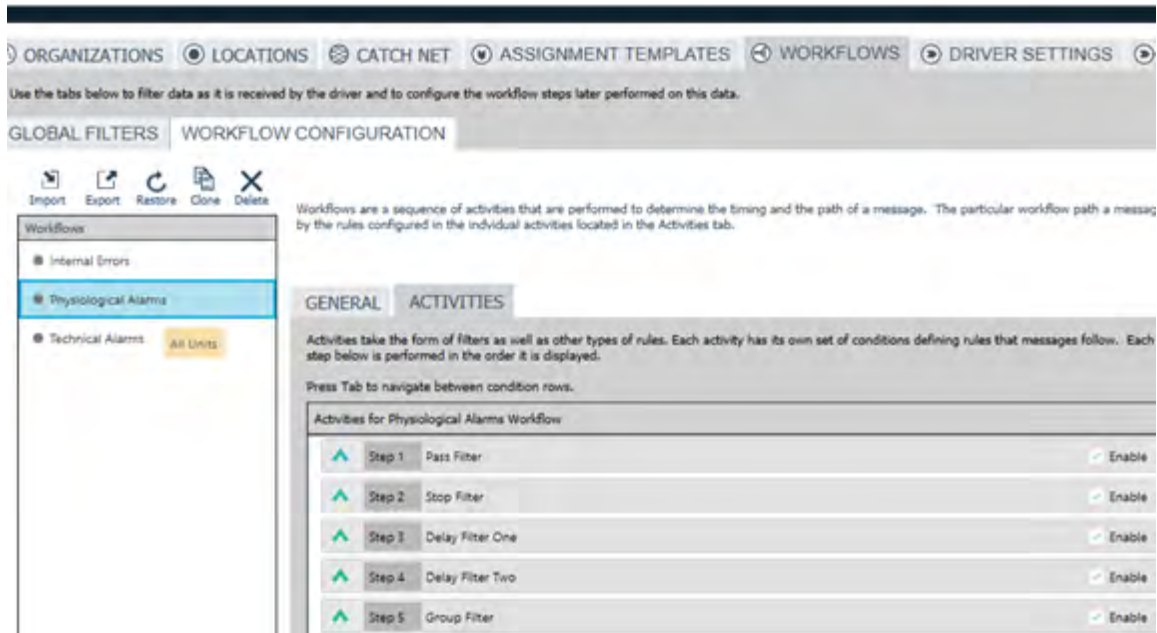
6.2.5 Workflow Management

Established Workflows within an integration can be managed for the purpose of Removing, Cloning, Exporting and Importing. These four features can help an installer maintain a system and safely enact change without interfering with the operation of an active system.

6.2.5.1 Cloning

Cloning is offered as a method to copy the configuration of an existing Workflow so that it can be used as a baseline of desired behavior which can then be adapted or modified without losing the configuration of the cloned Workflow. If one or more care units would benefit from specific configurations not represented in the existing Workflows, clone an existing Workflow to use as a template. Once you have cloned a Workflow, you can then customize it according to the needs of the specific care unit.

To clone a Workflow:

1. Select an existing Workflow.

2. Click **Clone**, above the Workflows column.

3. Provide a name (required) and a description (optional).

4. Select care unit(s) that should use the Workflow.

5. If needed, add conditions to the Workflow.

6. Click **Save**.

7. Click the **Activities** tab. Enable or disable and configure Activities desired for the Workflow. See chapters below for details.

8. Click **Save**.

9. Return to the **General** tab to activate the newly configured Workflow.

10. Click **Save**.

6.2.5.2 Deleting

Delete is offered as a method to completely remove one or more Workflows that are no longer active or are not to be used any longer as a template.

To delete one or more Workflows:

1. Select one or more existing Workflows. To select two or more workflows, select a Workflow, then hold down the keyboard Ctrl button while selecting the other workflows to delete.

2. Verify that the Workflow(s) are no longer Active.

3. Click **Delete** above the Workflows column.

6.2.5.3 Exporting

Exporting Workflows allows for the specific configuration of all Activities and Conditions related to all Workflows to be exported to a file that can then be restored to the same or a different system. See 5.10.2 Export, page 54.

6.2.5.4 Importing

Importing Workflows allows for the creation of pre-configured Workflows to be added to a system. See 5.10.3 Import, page 57.

6.2.5.5 Restoring

The Restore action can be used to restore the set of default Workflows provided with every Integrations. Restoring the Workflow does not remove existing Workflow configurations, but instead adds a new copy of the default Workflows. These default Workflows contain only the default configuration and provide a method to start over from a fresh copy of Workflows.

6.2.6 Workflow Status

Active/Inactive and Pending Inactive Workflows

When a Workflow is active, it will be used to distribute alerts. When a user has activated a Workflow, it cannot be edited. When a Workflow is active it will display a green indicator and show that it is "Active." In addition, it will also show an indication of how many "instances" (a count) of that Workflow are simultaneously processing other events. The actual count indicator does not automatically update but can be refreshed by using the button provided:
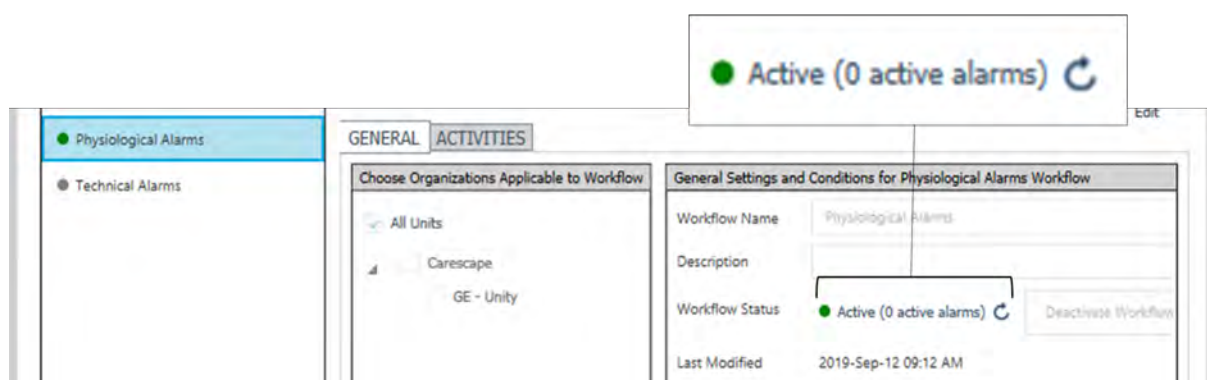
When a Workflow is Pending Inactive, it is in a state just before it is deactivated. In the pending inactive state, all active alerts will still be processed by the Workflow, however the Workflow will not accept new alarms. This means alerts will continue their normal redirection chain, including updates from the external source, until the alarm is cleared at the external source.

Example of a Pending Inactive Workflow with a yellow indicator is shown below:
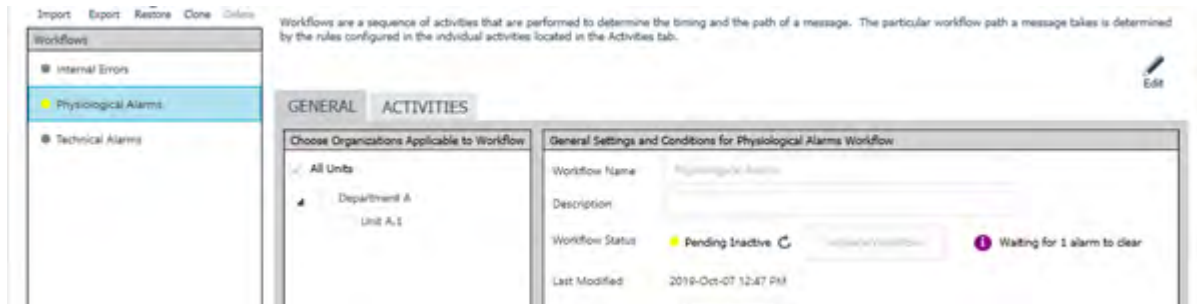
When a Workflow is inactive, it will not process alarms. A user must deactivate a Workflow to edit it. Example of a deactivated Workflow, with a grey indicator is shown below:
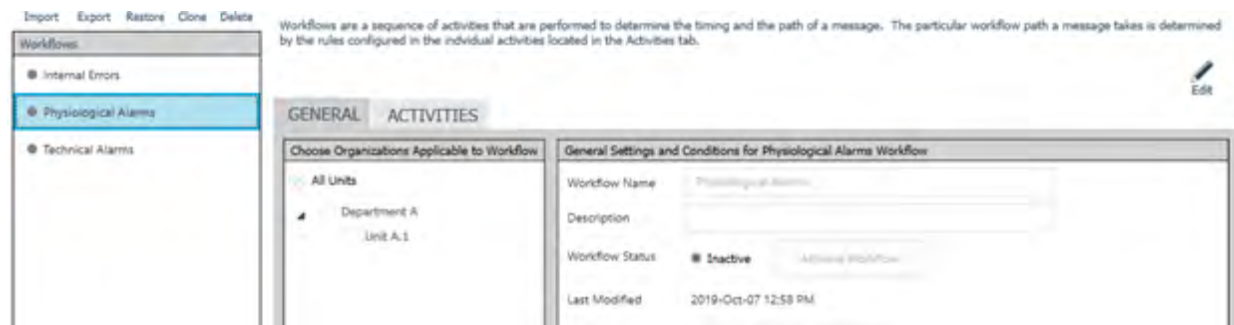
Last Modified Time

The Workflow screen with General selected shows the most recent time and date that a Workflow was updated. The date and time are updated when any of the following occurs:

- A Workflow's name and/or description is modified.

- A Workflow's units or conditions are modified.

- Any activity within the Workflow is modified.

When a Workflow is cloned, the time and date are set to that of the most recent time and date that it was cloned. When a Workflow is created (i.e., when an integration is created, or when Workflows are restored) the modified time and date are set to that of the most recent time and date it was created or restored.
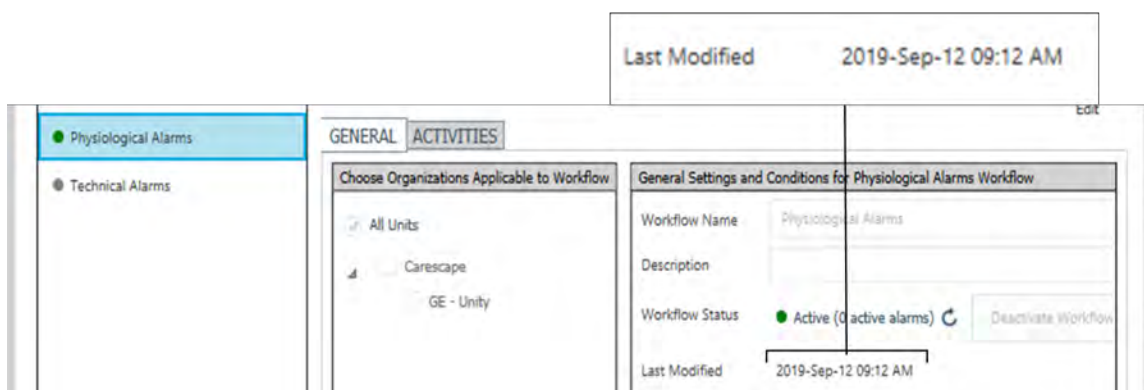
6.2.7 Conditions

Each Workflow and Activity includes the ability to define a number of conditions that are used to determine if a Workflow or Activity within a Workflow should be performed for a given acquired Alarm/Event. Each

Condition is composed of an Operator and a set of conditional expressions. The Condition Operator can either be an 'OR' or an 'AND' operator and will be used to logically combine the output of all expressions identified for the activity. Each conditional expression within a Workflow or Activity is composed of an Element, a Condition, and Value. The Elements available for each Conditional Expressions are made up of a predefined list of "Event Elements" which contain attributes of the received alarm/event. Each integration can support a unique set of Event Elements. The following table lists and describes the common elements available for conditions and that are supported by every integration.

Element Name	Description	Applicable Integration(s)
Active	Contains a true or false value indicating whether the alarm is active or not	All
Alarm Text	The description of the alarm as described by the external clinical system. Includes text for all alarms currently active at the location.	All
Digistat Device Model	The device model that generated the alarm, as defined and reported by Digistat.	Digistat
Digistat Device Type	The device type that generated the alarm, as reported by Digistat. Can be one of: • Monitor (MON). • Ventilator (VEN). • Blood Filtration (DIA). • Heart Lung Machine (HLM). • Incubator (INC). • Anesthesia Delivery Unit (ADU). • Infusion Pump (INF). • Blood Gas Analyzer (BGA). • Laboratory Information System. • User (User device type as described by Digistat).	Digistat
Digistat Event Code	The event code of the event as defined and reported by Digistat.	Digistat

Digistat Parameter Data	This element is used to trigger a workflow or activity within a workflow. It can also be used to include Digistat parameter data in the body of an alert in handsets. Parameter data from Digistat devices is concatenated and stored as text blocks; alarms are filtered using text patterns as the value to be compared: Example: HR ECG = 123 (.*)HR ECG: 123 (.*) The (.*) at the beginning and end allow this value to be anywhere among the parameters, HR ECG: 123 is the format of the text to match, and the space after the 123 is important because otherwise the text would match any number that starts with 123 (like 1238). The Parameter data contains parameter code numbers that can be used in Workflow conditions. Parameter code data is not shown in the parameter data message content.	Digistat
Digistat Translated Text	The translated, or alternate, text for the event, as defined and reported by Digistat	Digistat
Driver Status Type	Indicates whether an internally generated alert is due to a complete connection loss or loss of an individual location	All
ExternalUnitId	The text, provided by the external system, that describes the unit where the alarm occurred	GE Unity, Infinity Gateway
Latched	Contains a true or false value indicating whether the alarm is latched or not	Infinity Gateway
LimitValue	The text, provided by the external system, that describes the limit value that was violated	Infinity Gateway, XprezzNet
NurseCall Current Location Text	The nurse call name for the current location of the patient that initiated the call	teleCARE

NurseCall Event Type	The Type of the Event as reported by the Nurse Call system. Can be one of: • Call. • Workflow. • Reminder. • Recall. • Presence. • SpeechConnect. • ServiceTask. • RoundingTask. • Swing. • Capture. • SystemError.	teleCARE/Telligence
NurseCall Home Location Text	The nurse call name for the home (admitted) location of the patient that initiated the call	teleCARE
NurseCall Level	The authority level associated with a NurseCall event. For example, the service task level.	teleCARE, Telligence
ParameterValue	The text, provided by the external system, that describes the parameter value related to the alarm	Infinity Gateway, XprezzNet
Patient Admitted	Contains a true or false value indicating whether the external device has reported that a patient is admitted or not	GE Unity
Priority	The priority of the alarm. (Not Set, Alarm, High, Medium, Low, or Info).	All
Silenced	Contains a true or false value indicating whether the alarm is silenced at the source or not	GE Unity, Infinity Gateway, Digistat
teleCARE Event	The nurse call event identifier used to map the nurse call event to a specific workflow	teleCARE
Telligence Event	The nurse call event identifier used to map the nurse call event to a specific workflow	Telligence

Type	The type of alarm. Internal if generated by C4CS, otherwise defined by external system as either Physiological, Technical, or Other.	All
NurseCall Event Type	The type of the NurseCall event	teleCARE, Telligence

The Conditions are applied to the selected elements in combination with the Filter Text. The conditions available are dependent on the selected element. The following conditions are supported:

Comparison	Description
Equals	Used to indicate when the Event Element should contain a value that is EQUAL to the user provided value.
Not Equals	Used to indicate when the Event Element should contain a value that is NOT EQUAL to the user provided value.
Greater Than	Used to indicate when the Event Element should contain a value that is GREATER THAN the user provided value.
Less Than	Used to indicate when the Event Element should contain a value that is LESS THAN the user provided value.
Contains	Used to indicate that the user provided value is a PART OF the Event Element value.
Not Contains	Used to indicate that the user provided value is NOT PART OF the Event Element value.

Regular Expression	Used when the Event Element is being matched against a more complex programmer style "regex" pattern matching expression. Ascom Regular expressions are recommended, but when more extensive pattern matching is needed, Regular Expressions can be used.
Ascom Regular Expression	Used when the Event Element contains a string value, to indicate when the Event Element should contain a value that is EQUAL to the user provided expression which can contain specific portions of actual alarm description known to be generated from the external clinical system, as well as special characters.
	The special characters are defined to have specific behaviors when used in the composition of a filter.
	The special characters and their meanings are described below:
	• **?** Represents 1 character
	• ***** Represents 1 or more characters
	• **;** Ignores all alarm text strings after **;**
	• **I** can be used to join multiple expressions

The Condition Text must match the complete alarm text and the matching is case sensitive.

Caution

Special consideration must be paid to the configuration of filters and triggers that involve more than one care unit. Failure to take into account the configuration for all care areas may result in improper delays and/or suppression of notifications leading to potential patient harm.

6.2.8   Configuring Conditions

Conditions can be configured within each Activity.

To configure a Condition, do the following:

1.   Select the Activity and click **Edit**.

2.   Select an Operator.

3.   Select an Element.

4.   Select a Condition.

5.   Enter the Filter Text.

6.   Click **Enter** to add another row.

7.   Click **Delete** to remove a configured condition.

8.   Click **Save** to save changes.

6.2.9   Filters

Filtering capability at the Workflow configuration level allows an installation engineer to alter the distribution of alerts related to individual events and alarms received from external clinical systems. This will then represent the desired Workflow and expectations of a specific clinical environment.

Filtering activities are provided for the purpose of filtering the alarms that are determined by a health care facility and their clinical operators to be excessive or otherwise unnecessary to their specific Workflow procedures.

C4CS applies filters based on the originating location of alarm/event rather than the destination. Therefore, it is still possible for a handset to receive more than one alarm with the same priority from two locations in or around the same time period. It is up to the handset itself to properly manage the alert signaling in order to properly inform the recipient.

6.2.9.1   Pass Filters

Pass filters do not process any alarm if the alarm data does not match the syntax of a defined Pass Filter. If there are no Pass Filters, then all alarms are passed. See 6.1.1 Pass Filters, page 61 for more information.

In the scenario below, only the alarms with alarm text TACHY or AFIB would be passed. The use of the '*' character after the alarm text denotes that this filter should pass these alarms regardless of what follows the text TACHY or AFIB in the alarm description received from the external clinical system. Alarms with text that does NOT match this syntax are discarded allowing C4CS the ability to process requested alarm types more quickly

6.2.9.2   Stop Filters

Stop filters do not process any alarm if the alarm data matches the syntax of a defined Stop Filter. See 6.1.3 Stop Filters, page 62 for more information.

In the scenario below, only the alarms with alarm text PVC or INOP would be stopped. The use of the '*' character after the alarm text denotes that this filter should stop these alarms regardless of what follows the

text PVC or INOP in the alarm description received from the external clinical system. Alarms with text that does NOT match this syntax are passed through to the next set of filters (if configured) before triggering a Notification Event.

6.2.9.3 Delay Filters (1 and 2)

Delay filters reduce the number of unnecessary alarms delivered to a handset related to alarm conditions that correct themselves within a short period of time.

All alarms with alarm text matching any of the delay filters must be active for the period of time defined by the filter before an alarm is sent out. The delay values are configurable as settings within the rule for a period of 5s, 10s, 15s, 30s, 1m, 2m.

There are two delay filters that can be configured with different settings for different delay times. Each one of these filters supports up to 25 delay filter condition expressions.

In the above scenario, alarms that contain the text LEADS would not trigger a notification event unless it remained active for a period of time equal to 30 seconds. Alarms with text that do NOT match this syntax are passed through for further processing with no delay.

6.2.9.4 Group Filters

Group filters determine which alarm updates are considered equivalent to a previously delivered active alarm. Active alarms with updates that match a group filter will not be processed. If the alarm text does not match an active Group Filter, that alarm is processed. See for more information.

6.2.10   Operator Dispatch

Operator Dispatch allows a Unite View operator to evaluate specific events and determine if, and to whom, an alert should be dispatched. The alert displayed in Unite View includes the alarm text as well as indication of the location and priority of the alarm. The Unite View operator will receive feedback from Connect for Clinical Systems when an alert recipient accepts the alert, rejects the alert, or fails to respond to the alert during the configurable Dispatch Accept Timeout. As a function of Operator Dispatch the operator can optionally:

- Add a message accompanying the alert.

- Send a message notifying the alert recipient that the Dispatch Accept Timeout has expired.

- Override the preset redirection settings by forwarding the alert to any recipients inside or outside the redirection chain.

- Dismiss the alert, which prevents any actions being performed on the alarm (including dispatching to an individual or to redirection) and keeps the alert visible in Unite View until it is recalled or cleared.

- Recall a dismissed alert allowing for the resumption of Dispatch, which restarts Operator Mode and Operator Mode timeout.

- Dispatch to the automatic redirection chain.

- Interact with the alert after a recipient accepts the alert as follows:

  - Post accept dismiss (refer to Unite View, User Manual, TD 93008EN.

  - Post accept manual redirection (refer to Unite View, User Manual, TD 93008EN.

  - Post accept reminder configured to remind the Dispatch Operator that the alert is still active, and for the alert recipient (refer to Unite View, User Manual, TD 93008EN.

For additional information related to the specific operation of the Operator Dispatch please consult the Unite View User documentation - Unite View, User Manual, TD 93008EN.

A Workflow can be configured to allow Operator Dispatching using an appropriately configured and licensed Unite View client. Configuration of Operator Dispatch occurs within the Workflow Dispatch Activity.
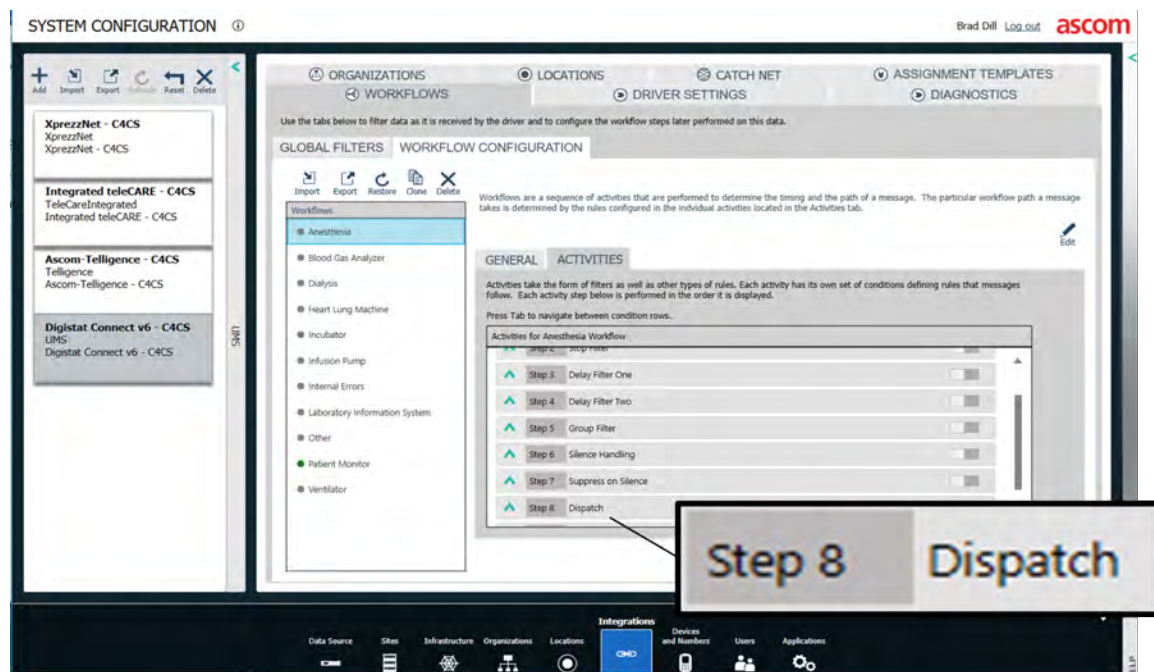
6.2.10.1 Dispatch Settings

The Dispatch Activity has the following configurable settings:

Setting	Description
Dispatched Accept Timeout Message Template	Automatically sent to the handset when the Dispatch Accept Timeout has expired.
Dispatched Accept Timeout (default 45 seconds)	Configured for the amount of time the alert recipient has to accept or reject the alert before the Dispatch process restarts.
Manual Redirection Allowed	Lets a Unite View operator manually cause redirection to occur before or after an alert has been accepted. The message will be redirected to the next level from where it was previously accepted. If dispatched to an individual, operator mode will restart.
Operator Timeout (default 45 seconds)	Configured per unit or Workflow for the amount of time the View operator has to interact with the alert before automatic redirection occurs.
Post Accept Dismiss Allowed	Lets a View operator dismiss the alert from their screen after the a user has accepted a dispatched alert. This removes the alert from the operator's screen so the operator can focus only on new alerts. A Dismissed alert can also be recalled.
Post Accept Operator Reminder Timeout	Starts a timer after a message is accepted and displays a reminder to View operator that an accepted alert has not been cleared and may require further action.
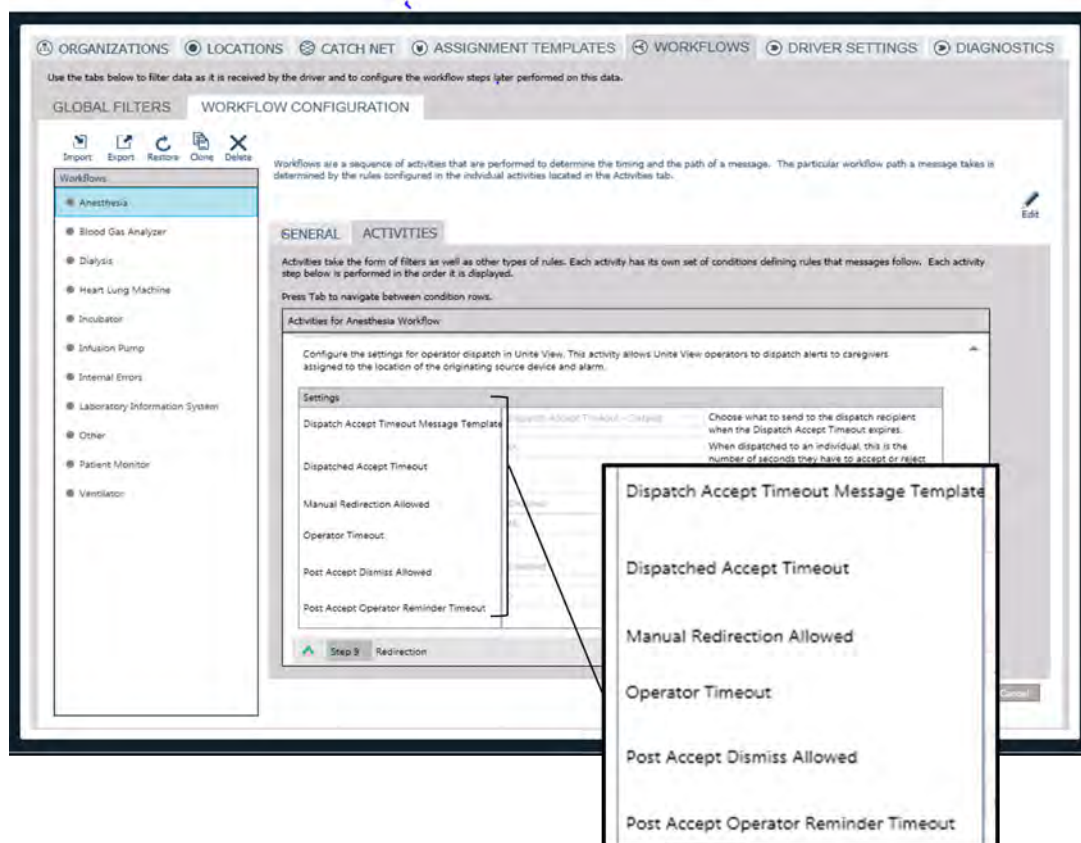
The following table summarizes the possible Dispatch Operator and recipient interactions with alerts, and subsequent outcomes.

Alert for Dispatch		
Dispatch Operator Action during Operator Timeout	**Recipient Action during Dispatched Accept Timeout**	**Outcome**

Dispatch to Individuals	Accept	Operator and recipient are notified and Dispatched Accept Timeout starts. Recipients other than the one who accepted the alert will be notified. See 6.2.10.2 Dispatch to an individual or multiple individuals, page 83 for the options.
	Reject	Operator is notified and Operator Dispatch and Operator Timeout restart and the alert becomes dispatchable again.
	Do nothing	Dispatched Accept Timeout expires and Operator Dispatch and Operator Timeout restart and the alert becomes dispatchable again. When the Dispatched Accept Timeout epxires, the recipients can be notified. See Dispatch to an individual or multiple individuals for the options.
Dismiss	–	Operator Timeout is stopped, preventing Operator Dispatch from timing out; alert is visible as dismissed until the operator recalls it or the corresponding alarm at the patient bedside is cleared. When the corresponding alarm is cleared, the dismissed alert is removed from Unite View.
Recall dismissed alert	–	Operator Dispatch and Operator Timeout restart – the alert can now be dispatched.
Do nothing	–	Operator Timeout eventually expires and automatic redirection starts.
Dispatch to redirection	–	Normal redirection begins, see 6.2.12 Redirection, page 86; Dispatched Accept Timeout is not involved any longer

6.2.10.2 Dispatch to an individual or multiple individuals

The View operator is able to override the preset redirection chain, determine who is best suited to handle an alert, and then dispatch an alert to one or multiple individuals. The recipients receive a notification and have the option to accept or reject the alert. The operator is then notified of which recipient accepted the alert and of the recipient's response.

6.2.10.3   Dispatch to Automatic Redirection

The View operator is able to send a Dispatch to Automatic Redirection Command to request that the alert be sent to the redirection chain, and the Operator Dispatch mode session ends. The View operator cannot perform any other actions on that alert when it is dispatched to automatic redirection. See 6.2.12 Redirection, page 86.

6.2.11   Persistence (GE Unity only)

A transient, non-latching alarm is typically of short duration, is self-correcting, and appears and disappears quickly. This type of alarm sometimes disappears from Unite View before the Unite View operator can discern what the issue was or the patient monitoring location where the alarm originated. Alerts configured as persistent remain visible on the Unite View screen after they are cleared by the monitor. An update is provided to Unite View to inform the operator that the alarm condition is no longer active on the monitor. The Unite View operator then has more time to decide if action should be taken and to determine a proper course of action.

Conditions in the Workflow Persistence Activity can be used to configure an alarm or a Workflow as persistent in Unite View for the GE Unity integration.

6.2.11.1   Persistence Timeout Settings

The Persistence Activity has two configurable timeouts - the Post-Clear Timeout and the Post-Accept Timeout. When the Persistence Activity is enabled, the alert remains active until either the Post-Clear Timeout or the Post-Accept Timeout expires. Alerts configured as persistent will not be automatically dispatched once the Post-Clear Timeout expires.

Persistence Timeout Settings		
Timeout	**Default**	**Description**
Post ClearTimeout	15	Configured per alarm or Workflow and starts once an alarm condition is cleared at the source. During this time the View operator is able to continue interacting with the alert and perform dispatch activities.
Post Accept Timeout	15	Configured for an alarm or Workflow and starts when a recipient accepts an alert regardless of whether the alert was dispatched to an individual or to automatic redirection. This ensures that the alert is visible to the View operator for a sufficient amount of time after the alert has been accepted by the recipient or after the alert becomes Unhandled.
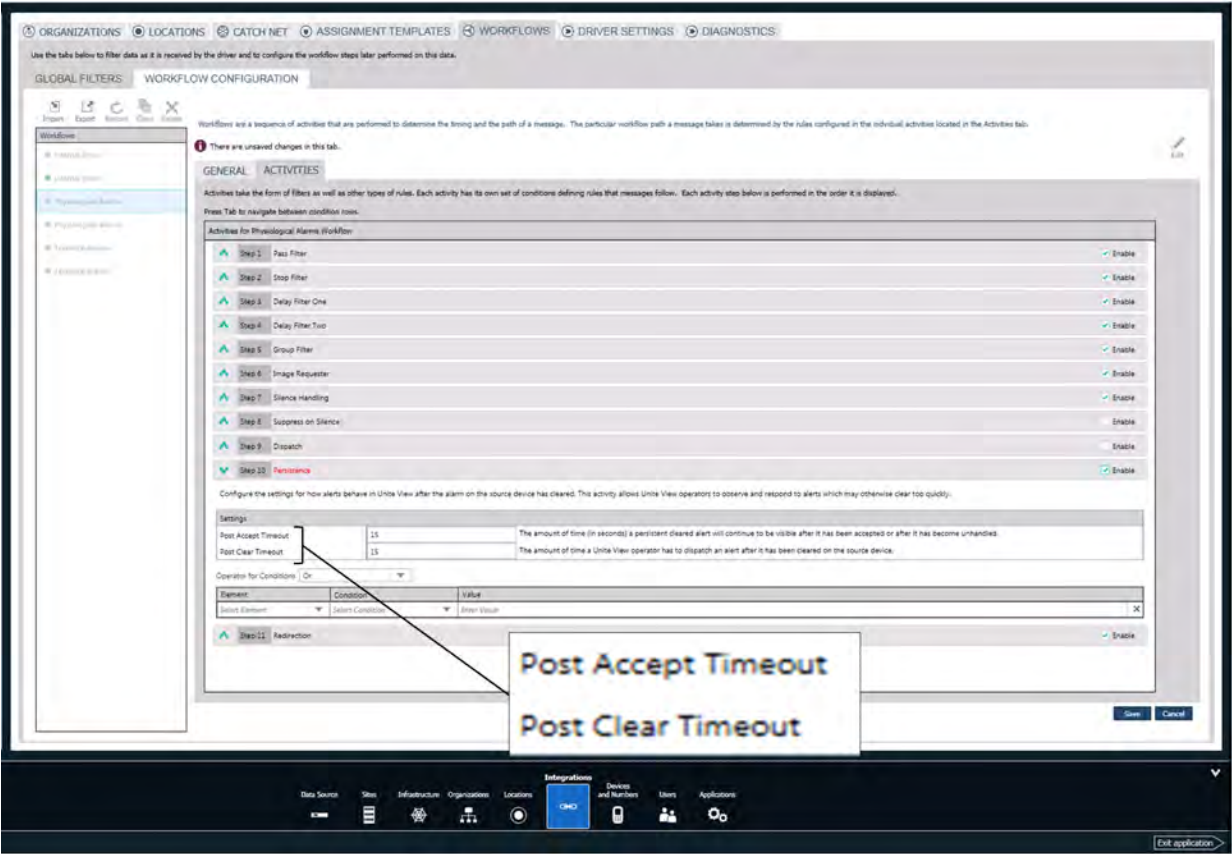
The following table summarizes the possible Dispatch Operator and alert recipient interactions with persistent and Cleared at Source alerts, and subsequent outcomes.

Persistent, Cleared at Source Alert		
Dispatch Operator Action during Post Clear Timeout	**Recipient Action**	**Outcome**
Dispatch to individual	Accept	Post Accept Timeout starts.
	Reject	Operator Dispatch and Post Clear Timeout restart and the alert becomes dispatchable again.
	Do nothing	Dispatch Accept Timeout expires, Operator Dispatch and Post Clear Timeout restart and the alert becomes dispatchable again.

Dispatch to redirection	Accept	Post Accept Timeout starts, and Operator Dispatch is terminated.
	Reject	Alert goes to next redirection level, see 6.2.12 Redirection, page 86.
	Do nothing	If no assigned caregivers accept on all 3 levels of redirection or Catchnet, the alert becomes Unhandled for the duration of Post Accept Timeout and is removed from Unite View after Post Accept Timeout expires.
Dismiss	–	If operator does not recall, alert is removed from Unite View after Post Clear timeout expires.
Recall dismissed alarm	–	Operator Dispatch and Post Clear Timeout restart for operator interaction; if Post Clear Timeout expires after being recalled, alert is removed from Unite View.
Do nothing	–	Post Clear Timeout expires, and the alert is removed from Unite View.

6.2.11.2   Persistence for Unhandled Alarms

If a dispatched alert is still active or has been configured as persistent and no display device has accepted responsibility for the Alert, it will remain at the "Unhandled" state, so it is visible in View to the operator during the Post Accept Timeout until the Unhandled state is resolved.

6.2.12   Redirection

The Redirection Activity within a Workflow includes settings that define how alerts are distributed to recipients and display devices (e.g., mobile devices and Unite View).

The Redirection Activity is common to all Workflows.

The table below describes the how redirection works and the purpose of each redirection level:

Levels of Redirection	
Level	**Description**
Level 1	This is the first level, or assigned staff member, that an alert will be sent to. The role assigned to this level depends on the type of device from which the alarm is coming. For example, the role assigned to Level 1 for a Patient Call might be a CNA, while the role assigned to Level 1 for a Patient Monitoring alarm might be an RN.
Level 2	This is the second level that an alert will go to if it was rejected by the Level 1 staff, OR if there was no response (accept/reject) to the alert before the configured timeout. The person assigned to this level is a backup to the first level.

Level 3	This is the third level that an alert will go to if it was declined by the Level 2 staff, OR if there was no response (accept/reject) to the alert before the configured timeout. The person assigned to this level is a backup to the second level.
Catchnet	If none of the staff assigned to levels 1, 2 or 3 respond to the alert, OR if there are no staff assignments for a location where there is an active alarm, the alert will go to the Catchnet level. By default, an alert in this level is sent to "All on Shift," that is, all staff on this shift who are assigned display devices. This is to ensure that every staff member in the unit who has a handset is aware that there is an active alarm condition in a patient which has not yet received attention from assigned staff. Catchnet exists as a safety measure to mitigate the risk of an alert receiving no response from staff.
Unhandled	If an alert has been rejected by everyone and it is no longer possible to get an acceptor, or if no staff has responded to the alert in Catchnet, a fault is triggered in the system. Unhandled is communicated to handsets, Unite View and the activity logger. The fault is also communicated to any status indicator connected to the system that monitors the system status. When an Unhandled alert is received on the handset, the user does NOT have the option to accept the alert. **Fault Details:** • Fault Level — "Error" • Fault Code — "Quality of Service" (13) • Application Specific Info — "Unhandled Alarm" • Persistent — "False" Please see details on configuring Fault Handling in the Unite System: • Fault Handling Unite Platform Server, Configuration Manual, TD 93280EN • Fault Handling Unite Connectivity Manager, Configuration Manual, TD 92735EN • Fault Handling Unite Communication Server, Configuration Manual, TD 92761EN **⚠ Caution** Proper installation of the product includes configuration of the unite supervision node and unite fault handler to inform responsible individuals of failures in the notification systems that may be preventing alerts from being received by the intended recipient.

The table below describes the Redirection Activity settings that allow the customization of alert behavior on display devices.

Redirection Settings
Settings

Settings	Setting Description	Default Setting Option	Option Description
Unique ID per Level	The setting that allows the same message ID for all levels of redirection or a unique message per level of redirection. See 6.2.12.2 Redirection Level Message ID, page 93.	Disabled	Disabled – Configures the same message ID for all levels of redirection. Enabled – Configures a unique message ID for each level of redirection.
Visible in View	The setting that provides the ability to enable all or only certain alerts, handled by this Workflow, to be displayed in Unite View.	Enabled – Default configuration	Alerts are visible in Unite View.
		Disabled	Alerts are not visible in Unite View

Alert Notifications			
Settings	**Setting Description**	**Default Setting Option**	**Option Description**
Alarm Message Template	The message sent to display devices on the current level when an alarm occurs.	Alert Notification - Default	The default alert message template determines the initial information, interactive messaging options and beep code included in an alert when sent to the display device.
Escalated Message Template	The message sent to users on the current level when redirection occurs.	Escalated - Default	The default escalated message template determines the information, interactive messaging options and beep code to include in an alert sent to notify users on the current level that the alert has been redirected to the next level. Any user who rejects an alert will not be notified of any further redirection status messages for that alert.

Escalated Message Includes Rejectors	Setting to choose whether or not to send an escalated message to the recipient who rejected the alert.	Enable	• Enable – send an escalated message to the recipient who rejected the alert. • Disable – do not send an escalated message to the recipient who rejected the alert.
Unhandled Message Template	The message sent to users when the alert becomes Unhandled. When an Unhandled alert is received on the handset, the user does NOT have the option to accept or acknowledge the alert.	Unhandled - Default	After an alert enters the Unhandled state, the alert recipients are notified on the handset.
Cleared Message Template	The message sent to display devices on the current level when an alarm is cleared.	Cleared – Default	The default cleared message template determines the information, interactive messaging options and beep code to include in an alert sent to notify users on levels 1-3 that the alarm on the origin device has been cleared.
Level 1 Timeout (s)	The amount of time (in seconds) a user assigned to Level 1 has to accept an alert before it redirects to Level 2.	Numeric	An integer.
Level 2 Timeout (s)	The amount of time (in seconds) a user assigned to Level 2 has to accept an alert before it redirects to Level 3.	Numeric	An integer.
Level 3 Timeout (s)	The amount of time (in seconds) a user assigned to Level 3 has to accept an alert before it redirects to Catchnet or repeats.	Numeric	An integer.

Level 3 Repetitions	The number of times Level 3 will repeat the notification, after the initial notification is sent, before starting the next level.	0	An integer value <n> that specifies the number of times a Level 3 alarm notification is sent.
Assignment Template			
Settings	**Setting Description**	**Default Setting Option**	**Option Description**
Assignment Template	Associates the Assignment Template with the redirection behavior in this Workflow.	Integration/Alert-Specific – populated by the column in the Assignment Templates table	A pre-populated list of default or user-created Assignment Templates (from the column in the Assignment Templates tab).
Catchnet			
Settings	**Setting Description**	**Default Setting Option**	**Option Description**
Catchnet Message Template	The message that defines the format of the Alert Content displayed on wireless devices.	Catchnet – Default	The default Catchnet message template determines the information, interactive messaging options and beep code to include in an alert sent to notify users on the Catchnet level.
Timeout (s)	The amount of time (in seconds) users assigned to Catchnet have to accept an alert before it redirects to Catchnet or repeats.	Numeric	An integer.
Catchnet Repetitions	The number of times Catchnet will repeat the notification, after the initial notification is sent, before the alert becomes unhandled.	0	An integer value <n> that specifies the number of times a Catchnet alarm notification is sent.
Post Accept			
Settings	**Setting Description**	**Default Setting Option**	**Option Description**

Accepted Message Template	The message sent to recipients after they have accepted the alert.	Accepted - Default	The default accepted message template defines the format including the information, interactive messaging options and beep code to include in an alert sent to notify users that they have successfully accepted the alert.
Taken Message Template	The message sent to other recipients assigned to the current level when a recipient has accepted the alert.	Taken by Other - Default	The default accepted message template defines the format including the information, interactive messaging options and beep code to include in an alert sent to notify users on the current level that the alert has been accepted by another caregiver.
Timeout (s)	The amount of time (in seconds) a user has after accepting an alert to clear the corresponding alarm on the medical device before it redirects to the next level.	0	An integer.
Undo Allowed	Allows a user who has previously accepted an alert to withdraw acceptance, and the alert goes to the next assigned caregiver at the next level of redirection.	Disabled	• Disabled– The alert recipient cannot undo acceptance from the handset. • Enabled – The alert recipient can undo acceptance from the handset.
Undo Occurred Text	This message is added to the bottom of the body of the Alert Notification - Default message and is populated only after a recipient accepts an alert and then pushes "Undo."		The <!UndoOccurred-Text> text informs a recipient that someone has previously accepted the alert, but has since un-accepted the alert, causing it to be redirected to them.

It is recommended that the default message templates be updated with additional information in the subject of the alert if you have a system with legacy DECT or VoWiFi handsets (e.g., Ascom d63 or Ascom i63), as you otherwise will not be able to see statuses like "Cleared" and "Taken by Other" in the handset message list. This recommendation also applies to systems where you have Unite Analyze for reporting purposes, as there are reports that include the subject of a sent message to trace activities for an event in the system.

Default Message Templates	
Message Template	**Description**
Accepted - Default	The default accepted message template determines the information, interactive messaging options and beep code to include in an alert sent to notify users that they have successfully accepted the alert.
Accepted w/ Image - Default	The default accepted w/ image message template determines the information, interactive messaging options, beep code and waveform snapshot to include in an alert sent to notify users that they have successfully accepted the alert.
Alert Notification - Default	The default alert notification template determines the initial information, interactive messaging options and beep code included in an alert when sent to the recipient. When an alert is accepted and undone, the <!UndoOccurredText> element is added to the bottom of the body of this message.
Catchnet – Default	The default Catchnet message template determines the information, interactive messaging options and beep code to include in an alert sent to notify users that the alert has been redirected to the Catchnet level due to previous redirection levels not responding.
Cleared – Default	The default cleared message template determines the information, interactive messaging options and beep code to include in an alert sent to notify users on levels 1-3 that the alarm on the source device has been cleared.
Do Nothing	When this template is selected, the alert will show no additional behavior in the display device, i.e., no redirection, no beep code behavior, no updates, etc.
Erase	This template can be configured to erase a message from a handset when certain actions are met, i.e., if the alert redirects from Level 1 to Level 2, erase the alert from Level 1's display device.

Escalated - Default	The default escalated message template determines the information, interactive messaging options and beep code to include in an alert sent to notify users on the current level that the alert has been redirected to the next level.
Taken by Other - Default	The default Taken by Other template determines the information, interactive messaging options and beep code to include in an alert sent to notify users on the current level that the alert has been accepted by another caregiver.

6.2.12.1 Alert Delivery Redirection Timeout

Connect for Clinical Systems will wait for 10 seconds to receive confirmation of delivery of an alert to a wireless device. If an alert is not confirmed as delivered in that time (i.e., due to a handset being out of range, or powered off) it is automatically redirected to the next level and any responses potentially arriving later from devices on the previous level are not accepted.

In addition to this behavior Connect for Clinical Systems can extend the alert Delivery timeout for the following scenario:

- When the handset is recognized as utilizing a DECT carrier, for which the alert delivery time may be greater than the default Alert Delivery Timeout of 10 seconds, an additional delivery time of 10 seconds is allowed. This will also extend the time by which acceptance of responses will also be allowed.

6.2.12.2 Redirection Level Message ID

When the Message ID originating from Unite does not change per redirection level, third-party wireless devices may be unable to distinguish if an alert represents an update or new notification. The alert can be configured in the Settings area of the Redirection Node to use the same ID for all levels of redirection (default and typical), or if an ID unique to each level of redirection should be used. By default, the messages that are sent use the same ID on all redirection levels.
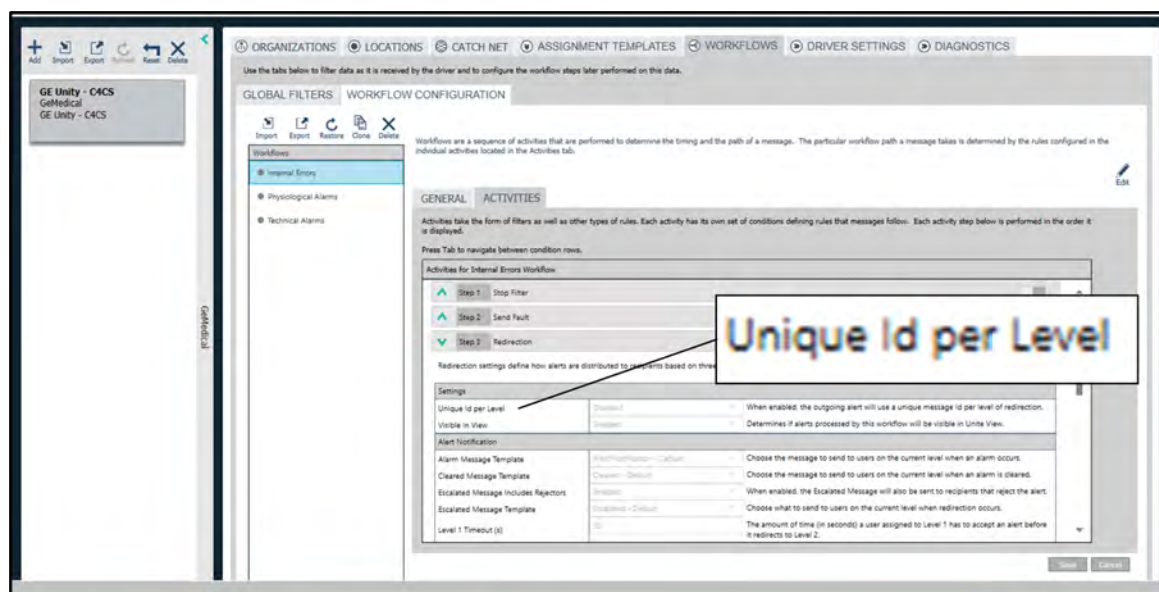
6.2.12.3 Redirection Level 3 Repetitions

Repetitions can be set to a specified number <n>, and an alarm notification is sent the additional number of times. By default, with a default value of 0. Level 3 will not repeat unless a value is specified. No escalation message is sent until all repetitions are complete.

The following occurs during Level 3 repetition:
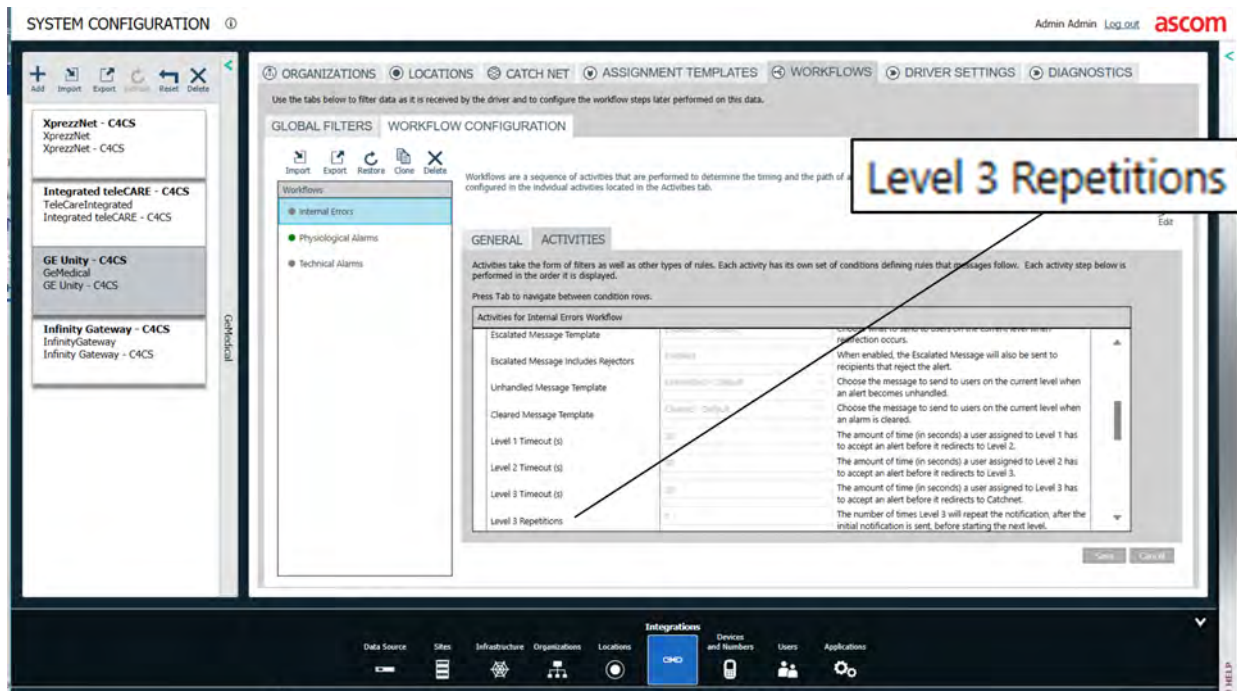
- At each repetition, Level 3 continues to repeat after the level timeout.

- Updates continue to be sent to the handsets even when they are sent a repeated message.

- Recipients who reject the alert WILL NOT be re-notified during a repetition.

- Unite View will continue to show the alert at the same level.

- The level timeout will not occur until repetitions cease and the alert is redirected to Catchnet.

The redirection level is no longer repeated:

- If there are no assignees.

- When a recipient accepts an alert.

- When all recipients reject at Level 3; the alert will then go to Catchnet.

- When every handset fails at Level 3; the alert will then go to Catchnet.

- When all assignees reject, or their handsets fail; the alert will then go to Catchnet.

- When the alert has been repeated the configured number of times.

6.2.12.4 Catchnet Repetitions

When an alert reaches the Catchnet redirection level, a Catchnet repetition is set to a specified number <n> and a Catchnet notification is sent the additional number of times specified until a recipient accepts the alarm. No Unhandled message will be sent until all repetitions are complete. If no recipient accepts the alarm after the configured repetitions occur, the alarm will go to Unhandled. Repetition continues at the Catchnet level when an alert is rejected or has a failed delivery.
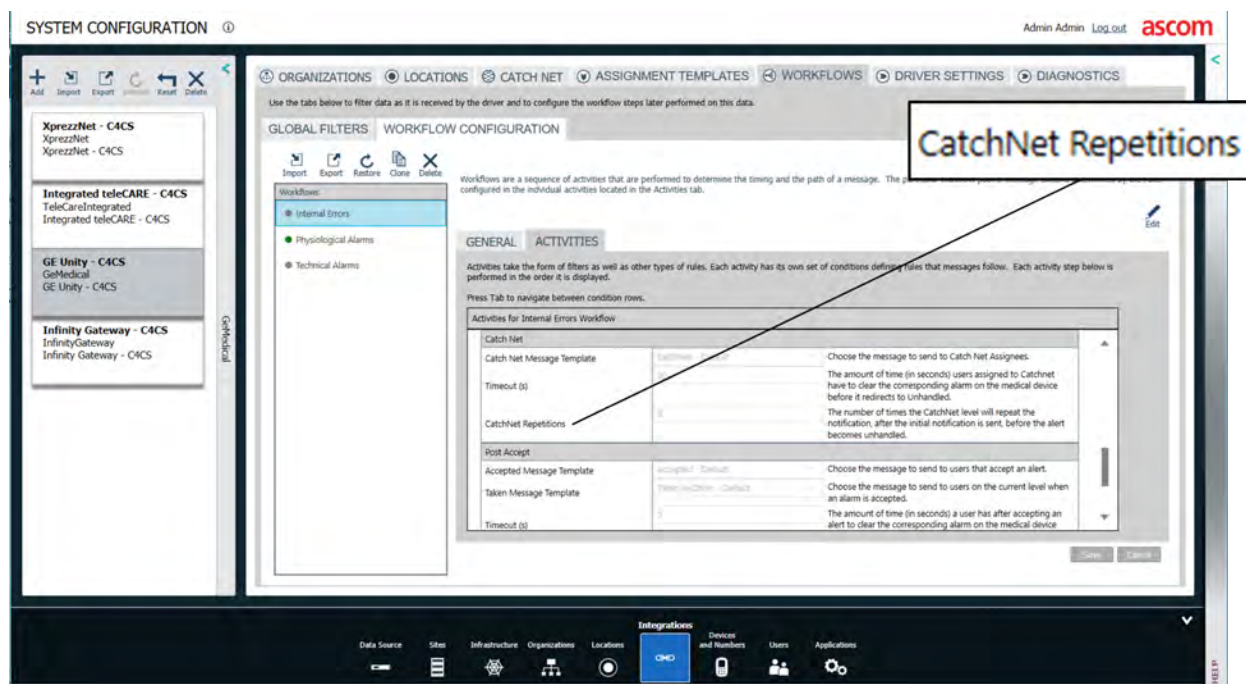
The following occurs during Catchnet repetition:

• If no recipient accepts the alert, the message is repeated at the level timeout.

• Updates continue to be sent to the handsets even when they are sent a repeated message.

• All assignees (including those who have rejected the alert or with previously failed handsets) will be re-notified at each repetition.

• Unite View will continue to show the alert at the same level.

• The level timeout will not occur until repetitions cease and the alert is redirected to Catchnet.

• At the next repetition, notifications will be sent to assignees that may have previously not responded or whose handsets had failed.

The redirection level is no longer repeated:

• If no-one is assigned.

• When someone accepts an alert.

• When the alarm is cleared.

6.2.12.5 Message Templates

In the Message Composition client, messages are pre-defined in the form of message templates, which in turn can be associated with events. The association between the events and the message templates is done in the application that receives the events. Message Templates in the Message Composition client are distributed as part of the Unite PS. See Unite Platform Server, Configuration Manual, TD 93280EN.

The following table shows elements that are available for Message Composition:

Element Name	Description	Applicable Integration(s)
CommentText	Comments to be included in the message.	All

DialString	Callback Dial digits provided by the Nurse Call enabling the ability to call back to a room (for rooms that support voice).	teleCARE, Telligence
DigistatAlarmId	The ID of the alarm sent from Digistat	Digistat
DigistatImageCaption	The caption for images sent from Digistat	Digistat
DigistatImageUrl	The url for images sent from Digistat	Digistat
DigistatParameterData	Parameter data from Digistat devices is concatenated and stored as a text block. The Parameter data contains the parameter name and value.	Digistat
DigistatTranslatedText	The translated, or alternate, text for the event, as defined and reported by Digistat.	Digistat
ExternalBedId	The text provided by the external system that describes the bed where the alarm occurred.	Infinity Gateway, GE Unity
ExternalLocationName	The name of the external location used in the location condition.	All
ExternalUnitId	The text provided by the external system that describes the unit where the alarm occurred.	Infinity Gateway, GE Unity
ExternalUnitName	The name of the external unit used in the location condition.	All
HistoryText	Text displaying a history of updates to an alert along with a timestamp for each update.	All
Image1Available	Contains a true or false value indicating whether Image1 is available as part of the message.	XprezzNet, GE Unity, Infinity Gateway
LocationText	The name of the Unite location.	All
ManualRedirectionOccurred	When an accepted alert is manually redirected this element is set to a string value of "RDR".	GE Unity, teleCARE, Digistat

NumericPriority	The numeric value of the alert priority.	All
NurseCallHomeLocationText	The nurse call name for the home (admitted) location of the patient that initiated the call	teleCARE
NurseCallCurrentLocationText	The nurse call name for the current location of the patient that initiated the call	teleCARE
OperatorComment	The optional text provided by the View operator when dispatching an alert.	GE Unity, teleCARE, Digistat
Paused	Contains a true or false value indicating whether the alerting of silenced alarms will be suppressed.	Digistat, Infinity Gateway, GE Unity
Priority	The priority of the alarm. (Alarm, High, Medium, Low, or Info).	All
PrioritySymbol	The symbol representing the alert priority can be one of the following: Alarm, High => "!!!" Medium => "!!" Low => "!"	All
RedirectionLevel	The text displaying the current redirection level (1-3).	All
ReminderComment	The text provided by the Unite View operator when sending a reminder.	GE Unity, teleCARE, Digistat
ShortText	Specifies the text to be included in the message. Typically, a subject text.	All
SilencedText	Text that can be displayed when the alert is silenced.	Digistat, Infinity Gateway, GE Unity
StateText	The current state of an alert.	All
Text	Specifies the text to be included in the message. Typically, body text.	All
UndoAllowed	Contains a true or false value indicating whether a user who has previously accepted an alert can withdraw acceptance.	All

UndoOccurredText	The text that informs an alarm recipient that someone has previously accepted the alert, but has since un-accepted the alert, causing it to be redirected.	All
UniteLocationId	The text provided by Unite that describes a location.	All
UnitText	The name of the Unite Unit.	All
CancelAllowed	Contains a true or false value indicating whether a user can request cancellation of an alarm	teleCARE, Telligence

6.2.12.6 Patient Data in Alerts

Patient data can be added to alerts in Connect for Clinical Systems. This patient data may contain information that includes the patient name, age, and/or gender. However, availability of patient data is controlled by configurable Patient Handler settings within Unite PS. These settings can be configured to determine which users have access to view patient information, which handsets can display patient information, and the format and type of patient information that is visible on the handset. For more information, refer to the Unite EHR Integration, Installation and Operation Manual, TD 93417EN..

6.2.13 Terminate on Latched (Dräger only)

A latched alarm is an alarm that is left active on the monitor, but the physiological condition in the patient corresponding with the alarm condition has ended. When the Terminate on Latched setting is configured and enabled, the state of a latched Info, Low or Medium alarm is treated as "cleared" in Unite. Also, the ClearedText element is populated with the configured setting and added to the activity result's elements. Lastly, the active element is set to false and added to the activity result's elements.

Terminating Info, Low, or Medium alarms on Latched prevents High priority alarms from being treated as alarm Updates in Unite, since all changes in alarm conditions while there is an active latched alarm are treated as updates rather than new alarms. With Terminate on Latched enabled, Unite will process any new incoming alarm from the patient monitor as new.

When any alert is terminated due to the alarm transitioning from the Active state to the latched, a "Latched Text" setting configures the contextual text that accompanies the terminated alert. This provides a visual distinction between an alarm terminated because it is latched, and an alarm terminated because it was acknowledged at the monitor.

6.2.14   Image Requester

In the Image Requester activity, ECG waveform snapshots for the selected lead are attached to an alert. The waveform snapshot included in the alert will contain a caption that contains the name of the location where the alarm occurred and the name of the selected lead.

The Image Requester has the following settings:

Settings		
Name	**Default**	**Details**
ECG Test Image	Disabled	When enabled, a fictitious waveform will be requested. ⚠️ **Important** This parameter shall only be enabled for test purposes.
Lead to Display in ECG Waveforms	I	The default lead to display in ECG waveforms.
TimeAfter	4	The time period, in seconds, to collect waveform data after the alarm occurs, to be included in the snapshot.
TimeBefore	8	The time period, in seconds, to include in the snapshot image before the alarm occurred.
Timeout	1500	The timeout in milliseconds for the snapshot request.
External Waveform Server		
Use External Waveform Server	Disabled	When enabled, requests will be sent to an external server.
External Server Waveform Address		The adress(es) of the external waveform server(s). Multiple addresses must be delimited with a ; If no port is provided, a default port of 8000 is used to connect to the External Waveform Server.

> The interactive message properties to include an image must also be set.

> Waveform Monitoring should be enabled in **Settings** tab.

The Connect for Clinical Systems GE Carescape Unity integration can connect to multiple gateways and support a greater number of monitors than can be supported by a single gateway. The IP Addresses of multiple gateways can be entered by separating them by semicolons. Up to five gateway addresses can be entered.

6.2.15   Send Fault

When an alert is unacknowledged at all levels of redirection, it is sent to Catchnet. When unacknowledged at Catchnet, it becomes Unhandled and triggers a fault in Unite. At this point, the Send Fault Activity sends a fault to the configured Unite Fault Handler Address.

For example, in the screenshot above, when this node executes it will send a 'No Connection to External Equipment' fault with the code set to 'Communication' to the fault handler address '127.0.0.1/FaultHandler.'

> The Fault Handler Address must be in the format IP/ServiceName such as: 127.0.0.1/FaultHandler.

6.2.16   Silence Handling

> The following feature is supported for Digistat, Dräger and GE Unity alerts only.

> This feature is applicable to Digistat only for specific devices that support the ability to report audio level (silenced).

When an active alarm is silenced at the alarm source, Connect for Clinical Systems can be configured to notify users of the current audio state of the alarm via updates sent to their display devices. Additionally, Unite View operators are provided an informational update indicating the audio state of the alarm.

The configuration available within this Activity determines the additional text displayed on the display device when an alarm condition has been silenced at the alarm source.

6.2.17   Suppress on Silence

> **Warning**
>
> This product provides methods to temporarily suppress alerting and redirection for the duration of a silenced alarm and (optionally) for the duration of all active alarms after the alarm is silenced. Failure to take into account operation of the silence feature of the Patient Monitor by unqualified or un-trained personal may lead to improper delays and/or suppression of notifications leading to potential patient harm.

> The following feature is supported for Digistat, Dräger and GE Unity alerts only.

> This feature is applicable to Digistat only for specific devices that support the ability to report audio level (silenced).

By utilizing the silence feature on the Patient Monitor, it is possible to suppress alerting & temporarily discontinue redirection of alerts. This capability is not enabled by default and requires additional configuration per unit.

The capabilities of the feature are managed via the parameters defined within the Suppress on Silence Activity. It is important to understand the purpose and interaction of each of these settings in order to safely and properly configure this Activity as part of a Workflow

When configured properly, this Activity provides a means by which alerting, and redirection may be temporarily paused during the period of time that the Patient Monitor is silenced. Upon expiration of the silence feature on the Patient Monitor or the onset of a new alarm, alerting and redirection will resume. Optionally, this Activity can be configured to persistently pause alerting and redirection for the duration of all active alarms, after the silence feature has been engaged on the Patient Monitor.

After the silence feature on the patient monitor has expired (or upon the onset of a new alarm), if Suppress on Silence is enabled, and Re-alert After Silence Expires is enabled, alerting will restart at the same redirection level as when the alert was initially silenced.

Alternatively, after the silence feature on the Patient Monitor has expired, if Suppress on Silence is enabled, and Re-alert After Silence Expires is disabled, alerting will NOT restart until all alarms are inactive on the Patient Monitor.

Recipients of alerts which have been silenced will receive notification related to the current audio state of the alarm via an update sent to their display device. This update can contain a configurable description (see image below). This is similar to what would be provided if responsibility for the Alert were to have been initially accepted.

The description accompanying silenced alerts can be configured by modifying the content of the setting Suppressed Alerting Notification Text. This description is provided as part of the updates to display devices.

Use Case:

A nurse is preparing to perform a simple procedure that requires removing the leads from the patient in their care. The removal of the leads from the patient will trigger an alarm on the Patient Monitor. The nurse presses Silence on the Patient Monitor. Enabling Silence on the Patient Monitor stops its audible alerts and additionally, prevents alerting and redirection to display devices. This allows the nurse to continue to focus on the patient's care without the interruption that would otherwise occur due to alerting and redirection.

If the Patient Monitor is silenced after redirection and alerting has begun, nurses in the same care unit will receive an update on their display devices indicating acknowledgement of the alarm condition by another nurse. To the nurse not at the alarm source, this scenario will appear as if the nurse at the alarm source had pressed "Accept" on their display device.

> This feature is not recommended for general care units due to a higher probability that improperly trained individuals such as patient family members and visitors may interact with the device. For this reason, it is also not recommended to configure this feature globally in a hospital facility. Confirm the units listed in the CDW (Clinical Design Worksheet) to be configured for this feature.

The screenshot below demonstrates the warning a user will receive if Suppress on Silence is active and a unit is added.
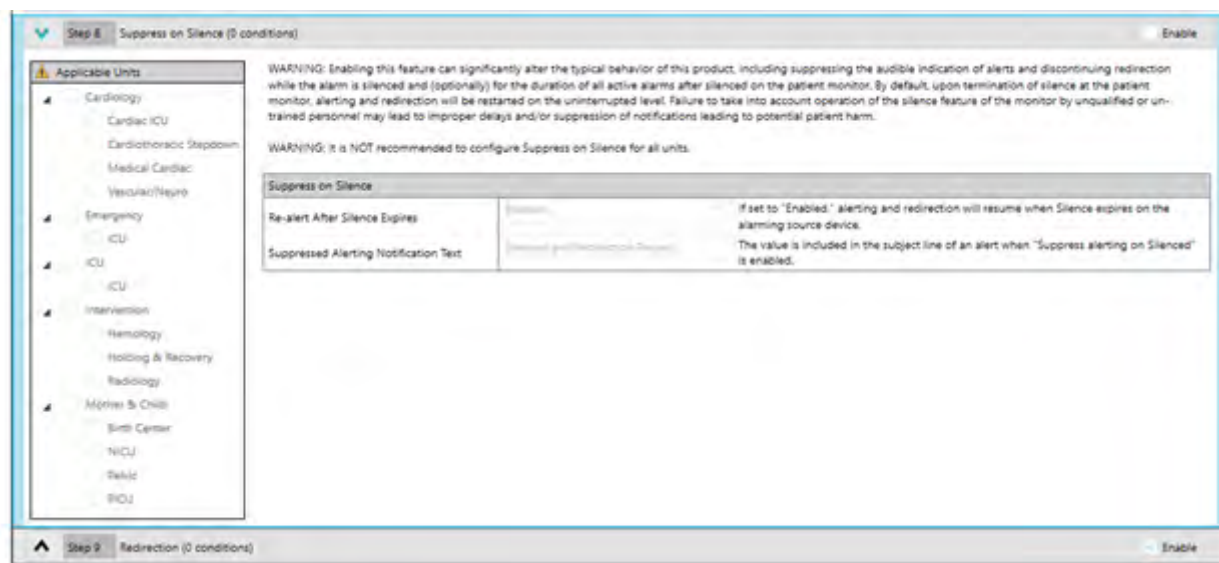
Suppress on Silence Activity - Configuration		
Setting	**Setting Options**	**Description**
Applicable Units	All units applicable to the Workflow are available in the list.	The Unit Selector within the Suppress on Silence activity allows the user to select a subset of units to which the Suppress on Silence activity applies. This enables the configuration of Suppress on Silence for specific units.
Suppress on Silence		
Setting	**Setting Options**	**Description**
Re-alert after Silence expires	Disabled.	If set to "Enabled," alerting and redirection will resume when Silence expires on the alarming source device.
	Enabled.	
Suppressed Alerting Notification Text	Alpha-Numeric – user can enter text, but default is "Silenced."	The content is included in the alert when Suppress Alerting on Silenced is enabled.

6.2.18   Indication Options

The Indication Options has a Sound Set setting that can be configured to determine which audible priority notifications are sent in outgoing alerts. The Beep Codes setting is the default setting that maps the beep code with the alert priority. With the Ascom Medical setting, the alert priority is indicated by a sound file audible indicator sent to handsets that replicates the Digistat sounds.

ℹ️ When using the Ascom Medical setting, the sound files are only played on handsets that support the sound files. If handsets do not support the Ascom Medical sounds, they will use beep codes.

6.3   Workflows Triggered from External Events

Workflows can be triggered by information updates when Connect for Clinical Systems is connected to driverless integrations. A driverless integration is represented by solutions like the RTLS and EHR integrations that rely on Connect for Clinical Systems in order to distribute alerts. Defined Workflow elements and conditions relevant to the type of information provided by the driverless integration can determine workflow triggers and alert content. Integrations like RTLS and EHR that do not have dedicated C4CS drivers do not show Global Filters or Driver Settings tabs in the user interface.

6.3.1   RTLS and EHR Integrations

If the RTLS or EHR integration is installed, updates to RTLS or EHR-based patient data (i.e. ADT & LAB) can trigger Connect for Clinical Systems workflows. Information can be configured by going under the Workflows tab under General, selecting one of the default workflows (Admit, Discharge, Pushbutton, Zone Alarm, etc.) and utilizing the elements available for that integration (as shown below for the Unite EHR Integration).
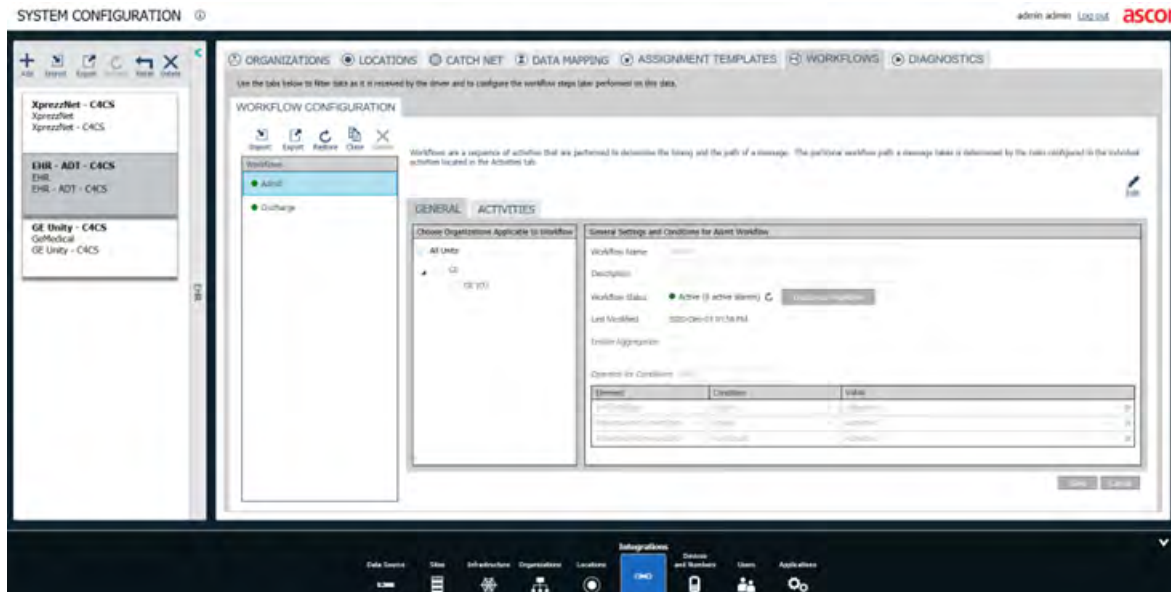
6.3.2 Response Team Alerts

Unite PS supports the configuration of dedicated Response Teams consisting of staff with competencies and skills required to address various emergency situations. Multiple disciplines within the Response Team have roles assigned to each discipline that are filled by staff members with a specific training level and skill set (e.g., a cardiac arrest response team member carries a pager that is dedicated to only receiving a cardiac arrest call).

Unite PS can be configured with a Response Team Integration that utilizes a non-medical installation of C4CS to deliver alerts, including redirection, for each discipline in the response team. When these response teams are triggered, some attributes of the alerts and redirection are determined by content provided to C4CS by UnitePS. This includes:

- Alert Icon.
- Alert Text (including the Named Team).
- Alert Priority.
- Alert Color.
- User Assignments.

Alerts are sent to each Response Team role as a separate event, and redirection stops when a user accepts the alert or the alert becomes unhandled.

6.3.3 Unite External Event API

A non-medical installation of Connect for Clinical Systems can be configured and used together with the Unite Event API to support custom integrations. Connect for Clinical Systems can process events from these integrations and distribute alerts. These integrations are capable of:

- Creating events
- Cancelling events
- Associating a color indication to an event
- Associating a priority indication to an event
- Making use of event orchestration for these events

For the events triggered by these integrations, it is possible to:

- See the state of the event in Unite View

- Set up assignments and redirection chains in Unite Assign

- Log the events in Activity logging

The Unite Event API can be used in single-node Unite deployments as well as in multi-node (High Availability) Unite deployments.

7 Drivers

Drivers are used by Connect for Clinical Systems to communicate with external equipment in order to acquire alarms elements waveform data. Each received alarm is stored in a database and handled by Workflows. Each Driver also records the status of its connection with the external system and with all external devices and triggers a Technical Workflow if any of these connections are lost.

Connect for Clinical Systems can support multiple instances of each Driver within one Integration, where each instance is capable of connecting to one external gateway. These instances are created on the Driver Settings tab under each Integration. Each Instance maintains a set of settings that can be modified independent of the other instances.

When a C4CS integration is created, one driver instance will automatically be created. To add a second driver instance, where supported by the driver, click the Add button above the list of driver instances.

The Driver Instances are listed on the left side of the Driver Settings tab. To switch between Driver Instances, select the instance in the list. To edit the settings for that instance, select the Edit button after selecting the instance.

After the Edit button is pressed the name of the Driver Instance can be changed, as well as the driver instance settings, along with other parameters.

For example, in the screenshot below, there are two XprezzNet driver instances and the second instance is selected.
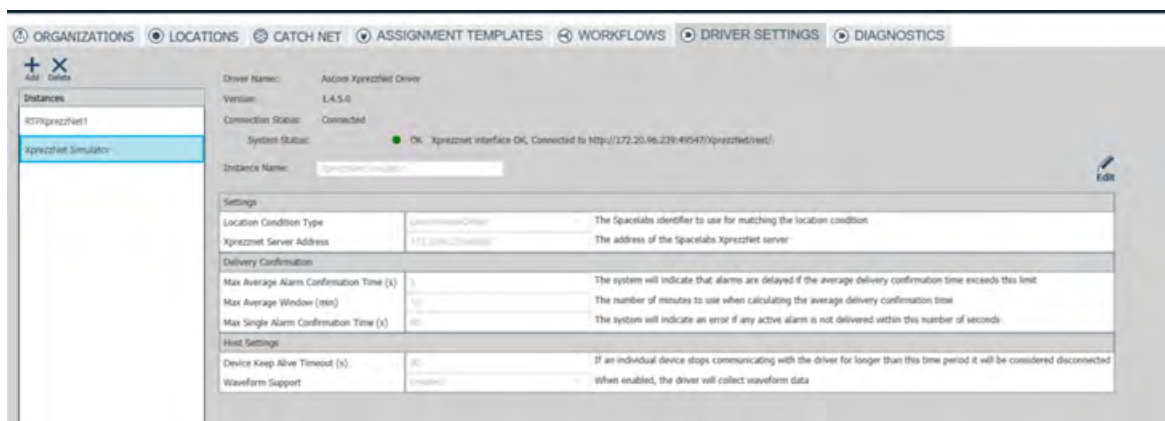
7.1 Common Driver Settings

Common driver settings are those settings that are common to all C4CS driver types, such as the driver Instance Name, and those that are found under Host Settings for each Driver Instance on the Driver Settings tab.

> While each driver instance has a copy of these settings, the values of those settings are unique to that instance and may differ between instances.

7.1.1 Driver Status

The Driver Settings tab displays the status of various components within Connect for Clinical Systems:

Connection Status	
States	**Description**
Connected	The driver is connected to the source system.
Disconnected	The driver is not connected to the source system.

System Status & Internal Component Status		
States	**Color Code**	**Description**
OK	Green	The system and its components are functioning with no issues.
Warning	Yellow	There is an issue with one or more components in the system, but the system is still partially functional – reason text is displayed with this state.
Error	Red	There is a failure in one or more components in the system and the system is not functional – reason text is displayed with this state.

7.1.2 Report Reliability Faults

Connect for Clinical Systems can report system reliability faults to the Ascom system supervisor. The error information is unit-specific and errors are uniquely defined so that appropriate action can be taken to ensure patient safety. Faults are always reported in the following scenarios:

- Loss of connectivity to the database.
- Loss of connectivity to the RabbitMQ broker.
- Self Test failures (when self test is enabled).

In addition to the scenarios above, when "Report Reliability Faults" is enabled, these fault scenarios can also be reported:

- When connectivity to the external system is lost.
- When an alert is unable to be delivered to any mobile device, either due to missing assignments or delivery failure.
- When an alert is delivered but never accepted by a mobile device.
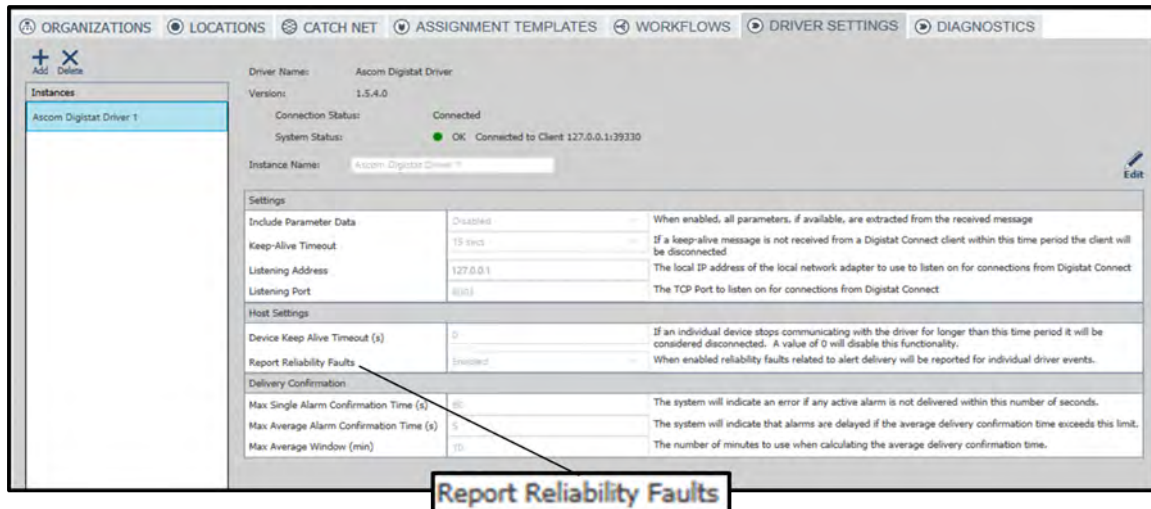
7.1.3 Delivery Confirmation Performance Monitoring

Connect for Clinical System can monitor how long it takes for an alert to reach a display device. Therefore, it can also determine if the delivery time is acceptable or if the system is unavailable to perform the task of distributing alerts within an acceptable time range.

> Delivery confirmation of an alert is not dependent upon user acknowledgement.

> Delivery Confirmation Time is the number of seconds between when an alert is dispatched and when it is delivered to a display device. Delivery Confirmation Time does NOT consider the amount of time it may take the user to acknowledge an alarm.

To configure the limits for the Delivery Confirmation performance monitoring, the following settings must be configured for each driver instance:

Delivery Confirmation	Details
Max Single Alarm Confirmation Time (s)	Enter the amount of time in seconds. If a single alarm takes longer than the time specified to be confirmed by the device, then the system will be in a faulted state until that alarm is cleared.
Max Average Window (min)	Enter the time in minutes to use for averaging confirmation time. All alarms delivered in the previous number of minutes defined will be averaged and if the average time exceeds the Max Average Alarm Confirmation Time, then supervision of the care unit will be in a warning state until the average drops below the limit.
Max Average Alarm Confirmation Time (s)	Enter the limit for the average amount of time, in seconds, for alarm confirmation. The average is calculated over the time period defined by the Max Average Window setting. If the average confirmation time exceeds this time limit the unit will be in a warning state until the average drops below this limit.

Connect for Clinical Systems will monitor the Delivery Confirmation Time of each alert for each configured unit. If the Max Single Alarm Confirmation Time is exceeded in ANY Unit, then C4CS will be in a faulted state. If the Max Average Alarm Confirmation Time is exceeded in a unit then that single unit will be in a warning state. Below is a description of the Fault and Warning states:

Message Delivery Confirmation – States of Monitoring	
State	Description
OK	The system is performing normally and requires no additional attention.
Warning	While alerts are still being delivered, they are delayed.
Fault	There is a fault present in the system that may be prevent alerts to be delivered to recipients.

Connect for Clinical Systems is also equipped with the capability to provide additional methods of notifying users of the status and performance. The method for notification is through the use of additional software in the form of external Status Indicators. These Status Indicators are intended to be installed and operated within the individual healthcare units utilizing the Ascom system. The Status Indicators are a separate component of the system which are able to receive and interpret the current status and performance metrics of the messaging system and communicate them to users through visual and audible indications.

When configured, each individual status indicator is made aware of the network location (URL) of the installed Connect Clinical Systems platform and will receive regular updates identifying the current system status and indication of the performance of the messaging systems ability to deliver alerts to display devices within that unit.

7.2   Dräger Infinity Gateway Driver

Dräger Infinity Gateway Driver serves as the Integration for Dräger monitors connected to the Dräger Infinity Gateway and is capable of receiving alarms and ECG waveforms.

> The Dräger driver requires the Microsoft Visual C++ redistributable 2010 x86 (bundled with installer).

7.2.1   Settings

The Dräger Infinity Gateway Driver has the following settings. To learn about the additional settings, see .
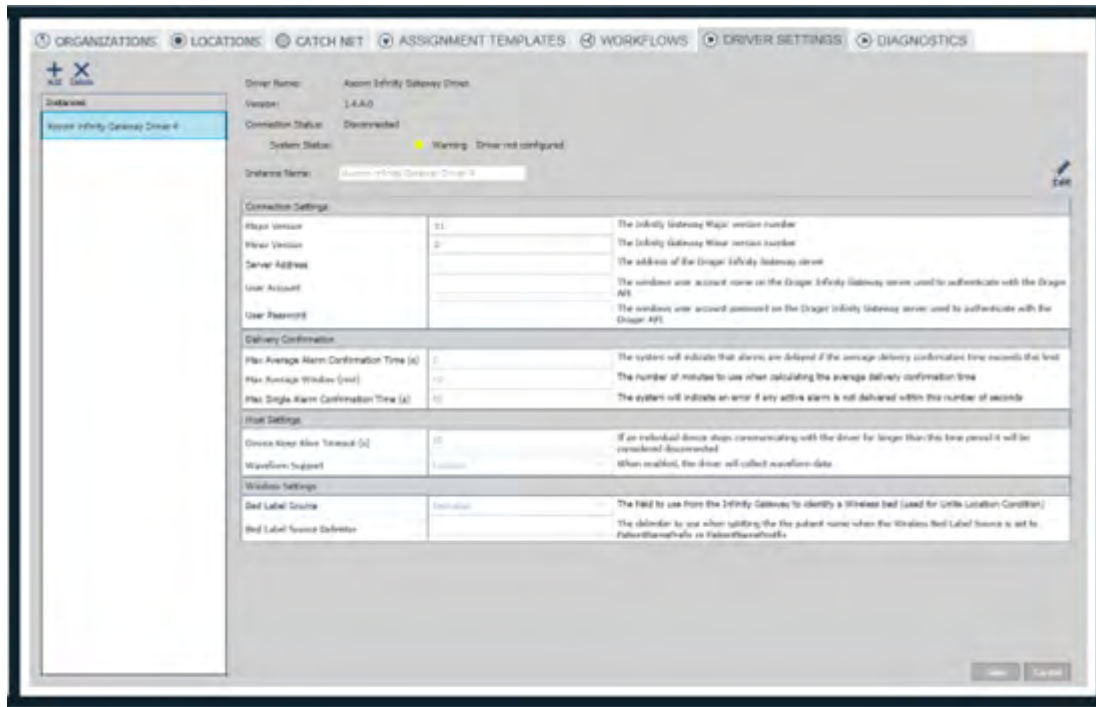
Setting	Default	Details
Major Version	11	The Infinity Gateway major version number.
Minor Version	0	The Infinity Gateway Minor version number.
Server Address	<empty>	The address of the Dräger Infinity Gateway server.
User Account	<empty>	The MS Windows user account name on the Dräger Infinity Gateway server used to authenticate with the Dräger API.
User Password	<empty>	The MS Windows user account password on the Dräger Infinity Gateway server used to authenticate with the Dräger API.
Device Keep Alive Timeout (s)	30	Clinical devices should regularly communicate with the driver. This setting configures the number of seconds during which communication should happen. If communication does not happen within this timeframe, the driver will generate a technical alarm.
Waveform Support	Enabled	Support for monitoring waveforms, which may be enabled or disabled.

| Bed Label Source | BedLabel | The field to use from the Infinity Gateway to identify a Wireless bed (used for Unite Location Condition). |
| Bed Label Source Delimiter | {Space} | The delimiter to use when splitting the patient name when the Wireless Bed Label source is set to PatientNamePrefix or PatientNamePostfix. |

7.3 XprezzNet Driver

The Spacelabs XprezzNet driver is used to communicate to the Spacelabs XprezzNet server to receive alarms and ECG Waveforms.

7.3.1 Settings

Spacelabs XprezzNet driver has the following settings. To learn about the additional settings, see .
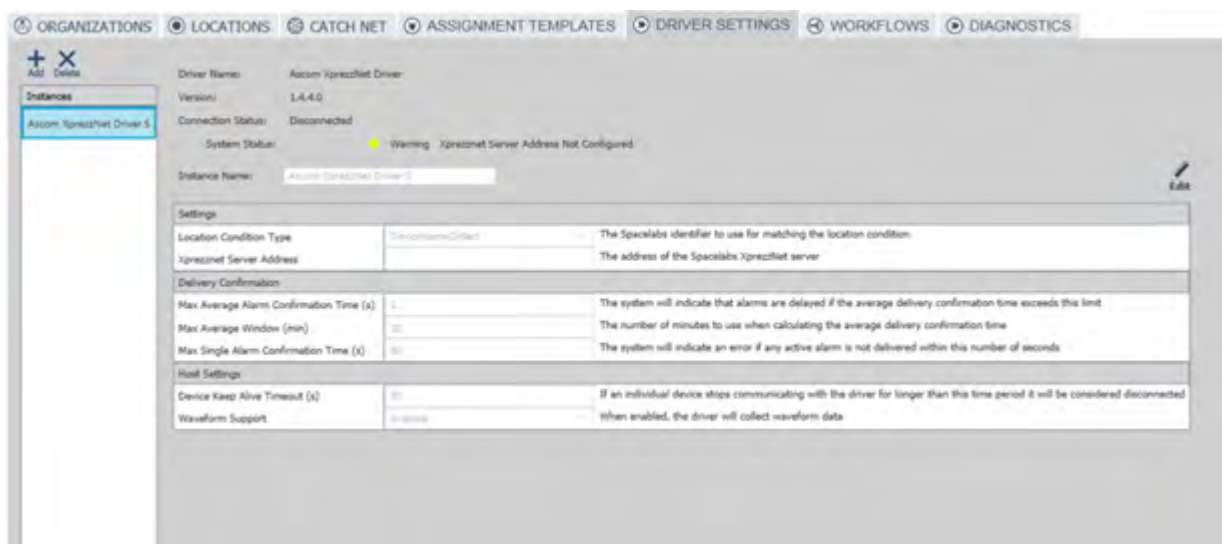
Settings	Default	Details
Location Condition Type	DeviceNameOrBed	The Spacelabs identifier to use for matching the location condition.
XprezzNet Server Address	<empty>	The address of the Spacelabs XprezzNet server.
Device Keep Alive Timeout (s)	30	Clinical devices should regularly communicate with the driver. This setting configures the number of seconds during which communication should happen. If communication does not happen within this timeframe, the driver will generate a technical alarm.
Waveform Support	Enabled	Support for monitoring waveforms, which may be enabled or disabled.

7.4 Digistat Suite Driver

The Digistat Suite Driver is used to communicate with Digistat Suite and to receive alarms from devices connected to the Digistat Suite server.

Connect for Clinical Systems supports receiving a waveform snapshot from Digistat for inclusion in alerts. The waveform snapshots are enabled and configured within the Digistat Suite, and no Connect for Clinical Systems settings needs to be configured. The waveform snapshot includes a link to the image, which is hosted within Digistat, and a caption for the image that is used when displaying the image. When the Enable Aggregation feature is enabled, the waveform link will match the highest priority alarm condition, including cases where a lower priority alarm condition is updated with a higher priority alarm condition.

The Enable Aggregation feature is enabled by default for Digistat. When the Enable Aggregation feature is disabled each alarm/event Digistat receives/acquires can trigger a separate instance of the Workflow and generate a separate alert that is handled independently as a separate driver event detail reported to the Driver Host.

Up to three instances of the Digistat Suite driver are supported

The Driver Host provides event feedback to Digistat for the following alert states:

• Technical Ownership.

• Delivery (to the first recipient).

• Accepted.

• No Delivery (filtered).

• Accept Undo.

• Last Reject (Unhandled).

7.4.1 Settings

The Digistat Suite Driver has the following settings. To learn about the additional common driver settings, see .

Settings	Default	Details
Keep-Alive Timeout	15 secs	If a keep-alive message is not received from a Digistat Connect client within this time period, the client will be disconnected.

Listening Address	127.0.0.1	The local IP address of the local network adapter to use to listen on for connections from Digistat Connect.
Listening Port	8001	The TCP Port to listen on for connection from Digistat Connect.
Device Keep Alive Timeout (s)	30	Clinical devices should regularly communicate with the driver. This setting configures the number of seconds during which communication should happen. If communication does not happen within this timeframe, the driver will generate a technical alarm.

7.5   GE CARESCAPE Unity Driver

The GE CARESCAPE Unity Driver is used to communicate with the GE CARESCAPE Unity network to receive alarms from GE patient monitors. Only ONE instance of this driver is supported.

Unity traffic received from the GE CARESCAPE network is available as unsolicited data to any configured UDP client. It is possible to configure the IP Address and Port of a Client which received a "mirror" of the data received by the Connect for Clinical Systems from the GE Unity CARESCAPE alarm router.

7.5.1   Ability to Disable Lost Device Alerts when a Patient is Not Admitted

GE can report patient admitted status so that when a device is lost, alerts will not be issued at locations where patients are no longer admitted. Workflow conditions can be configured using Patient Admitted and Driver Status Type elements (see 6.2.7 Conditions, page 72).

When a workflow condition is configured as a Stop Filter that includes the expressions Patient Admitted and Driver Status Type="Location Lost" the following behaviors can be observed:

- When a patient is admitted (Patient Admitted=true) and a location is lost, location lost internal alerts are sent

- When a patient is not admitted (Patient Admitted=false) and a location is lost, location lost internal alerts are not sent.

7.5.2   Raw Logging support for GE Waveforms

The GE Unity driver supports logging to a file all TCP communication sent to and received from the GE Carescape Gateway. Raw logging is enabled with the waveform supporting GE Unity driver setting. The verbosity level can be modified in the log4net configuration file (log4net.config) located at: C:\ProgramData\Ascom\Ascom Unite Connect\Driver Host\Drivers\Unity\log4net.config. After any modifications are made, the driver must be restarted. Log files will then be generated and saved to the C:\Ascom\GEC\Logs directory.

Warning

After enabling logging, it should be monitored to verify there is available disk space and to ensure the disk space does not reach capacity.

7.5.3   Settings

The GE CARESCAPE Unity driver has the following settings. To learn about the additional settings, see 7.1.1 Driver Status, page 106.

Settings	Default	Details
Combo Mode	Enabled	When enabled, telemetry monitors with trailing asterisks will be treated as the same location as fixed monitors. i.e., ICU|BED1* will be treated as ICU|BED1.
Inactive Time(s)	6 secs	The amount of time, in seconds, that must elapse between receipt of alarm packets for an alarm to be considered inactive.
Max Time Difference	60 secs	The maximum allowable time difference, in seconds, between the Unity network and the driver.
Notify on Silent State Changed	Enabled	When enabled (default) the silenced state is evaluated to determine if an update is sent notifying staff if a patient monitor is silenced. If disabled the silenced state is not evaluated and updates are not sent to display devices.
Carescape Gateway IP	0.0.0.0	The IP address of the Carescape Gateway to connect to for waveform data.
Carescape Gateway Port	2027	The TCP port of the Carescape Gateway to connect to for waveform data.
Carescape Gateway UDP Port	4446	The UDP port for receiving waveform data from the Carescape Gateway.

Waveform Support	Enabled	When enabled, the driver will collect Waveform data if the Carescape Gateway IP setting is configured.
Device Keep Alive Timeout (s)	30	If an individual device stops communicating with the driver for longer than the time period it will be considered disconnected, A value of 0 will disable this functionality.
Report Reliability Faults	Enabled	When enabled reliability faults related to alert delivery will be reported for individual driver events .

7.6 Nurse Call

Connect for Clinical Systems supports integrating with teleCARE IP and Telligence Nurse Call systems. Three installations are supported for NurseCall integrations where each installation can operate simultaneously on the same hardware. See 7.6.1 teleCARE IP Nurse Call, page 115 and 7.6.2 Telligence Nurse Call, page 117 for details on gateways and locations that are supported per installation.

Connect for Clinical System with teleCARE IP Nurse Call or Telligence Nurse Call integrations installed supports importing locations, triggering alerts and synchronizing active events. Other features include:

- Support of cancellation requests from handsets - the Cancel option appears on the handset in the Accepted message. When the cancel option is selected, C4CS sends a request, and nurse call system evaluates and decides whether or not to cancel.

- Support for distributing the color accompanying a nurse call event - if a nurse call event includes the dome light color that the Nurse Call System utilizes, the color is communicated and propagated in the alert to the display devices.

- Support for speech communication to the event source - if a nurse call event includes a dial string, the handset can initiate a speech connection using that dial string.

- Support for reporting alert status back to the Nurse Call system, including the state of alert delivery (success or failure), user acceptance, indication when an alert becomes unhandled, or indication when an alert will not be delivered.

- Support for generating a fault for unknown locations or unknown events in the following scenarios:
  - When an alert is sent from a location that has not been mapped to a Unite location.
  - When an event has not been configured with a corresponding workflow.

  This fault can be utilized to notify staff of configuration issues in cases where the system is not fully configured, or if the Nurse Call system adds additional locations and/or events without corresponding configuration within the Unite Connect for Clinical Systems Integration.

- Support for multiple Nurse Call organizations to be mapped to a single Unite organization - when this occurs, locations from all mapped Nurse Call organizations will be available to map to locations within the Unite Organization on the **Location Mapping** tab.

- Support for smaller facilities with Connect for Clinical Systems installation in an SFU deployment with a single teleCARE or Telligence integration. See 1.6 Software Requirements, page 9, 2.6 Small Footprint Unite (SFU) Deployment, page 15, teleCARE IP Nurse Call, page 123 and Telligence Nurse Call, page 123.

7.6.1 teleCARE IP Nurse Call

The Ascom teleCARE IP Driver is used to communicate with the teleCARE IP Nurse Call System.

The teleCARE IP NISM can added as infrastructure to the Unite Platform Server so that additional information can be shared to expedite configuration. Specific information related to these features are discussed previously related to 5.8 Location Importing, page 46.

Wireless teleCARE IP Nurse Call

When using the wireless teleCARE IP Nurse Call system, the location where an alarm originates may be different from where the patient was admitted. The features described in the following paragraphs are used with the wireless teleCARE IP Nurse Call system to ensure that alerts reach the correct nurse, and that the nurse receives accurate information on the patient's identity, location and alarm source.

Staff can receive alerts on handsets that contain patient location information associated with a triggered alarm. Alert text, configurable in Unite, includes message composition elements containing patient home and/or current location information provided by the teleCARE event. This determines the patient location message content that staff receives on the handset. The home location is the bed where patient is admitted, and the current location is the approximate location where the event occurred.

To include the home location of an event in the alert text, the NurseCallHomeLocationText element can be added to the body of the alert in the Message Composition Client. To include the current location of an event in the alert text, the NurseCallCurrentLocationText element can be added to the body of the alert. It is possible to include both elements in the body to provide the recipient information about where a patient is admitted and where a patient is currently located.

In addition, a "Prefer Home Location" driver setting can be configured for a preferred location. If the setting is enabled and if teleCARE provides a home location for the event, the event is triggered at the home location. When this setting is disabled (default setting), the home location string is ignored in favor of the current location string. See Settings, page 116 below.

The teleCARE system has the ability to include the badge ID of the transmitter used by the patient to generate the wireless Nurse Call event. If Connect for Clinical Systems is configured to include patient data in alerts, this badge ID, when provided by teleCARE, is forwarded from Connect for Clinical Systems to Unite PS to be utilized by Unite PS to identify the patient data to be included in alerts. This can ensure that wireless teleCARE IP Nurse Call alerts include the correct patient data associated with the patient that generated the alert.

Settings

The process for setting up communication between Connect for Clinical System and teleCARE IP is managed by adding the teleCARE IP Nurse Call System Manager (NISM) to the Unite Admin Infrastructure and completing the steps of Location or Nurse Call Event Mapping to the Workstation. See 5.7 Nurse Call Location Mapping, page 45, 5.8 Location Importing, page 46, 5.9 Assignment Templates, page 47 and 6.2.12 Redirection, page 86. The screenshot below shows the "Prefer Home Location" setting, which is described in Wireless teleCARE IP Nurse Call, page 116. There are no additional settings specific to this integration available per the Driver Configuration.
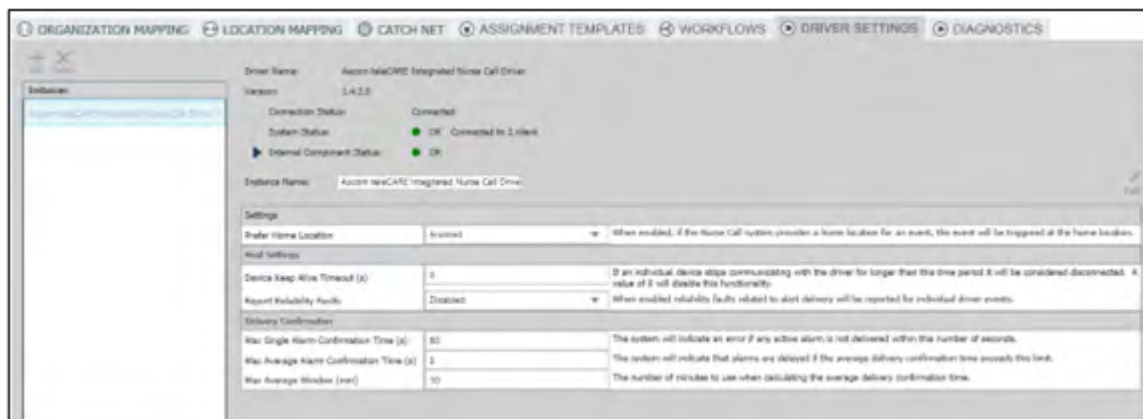
7.6.2 Telligence Nurse Call

The Ascom Telligence Driver is used to communicate with the Telligence Nurse Call System.

The Telligence IMT can be added as infrastructure to the Unite Platform Server so that additional information can be shared to expedite configuration. Specific information related to these features are discussed previously related to 5.8 Location Importing, page 46.

Rounding and Service Tasks

Connect for Clinical Systems supports redirection for Telligence Rounding and Service tasks. C4CS triggers alerts to mobile devices when the following event type requests are received from Telligence:

- Rounding tasks - initiated from a console and trigger alerts containing information for assigned staff to complete routine patient services on a pre-configured round schedule.
- Service tasks - initiated from a console and trigger alerts containing information for assigned staff to provide pre-configured patient services.

These tasks are visible in the Unite View Task view while they are active, and staff are assigned in Unite Assign. Associated Connect for Clinical Systems workflows send these alerts to handsets through automatic redirection.

Settings

The process for setting up communication between Connect for Clinical System and Telligence is managed by adding the Telligence Nurse Call IMT to the Unite Admin Infrastructure and completing the steps of Location or Nurse Call Event Mapping to the Workstation. See 5.7 Nurse Call Location Mapping, page 45, 5.8 Location Importing, page 46, 5.9 Assignment Templates, page 47 and 6.2.12 Redirection, page 86. There are no additional settings specific to this integration available per the Driver Configuration.
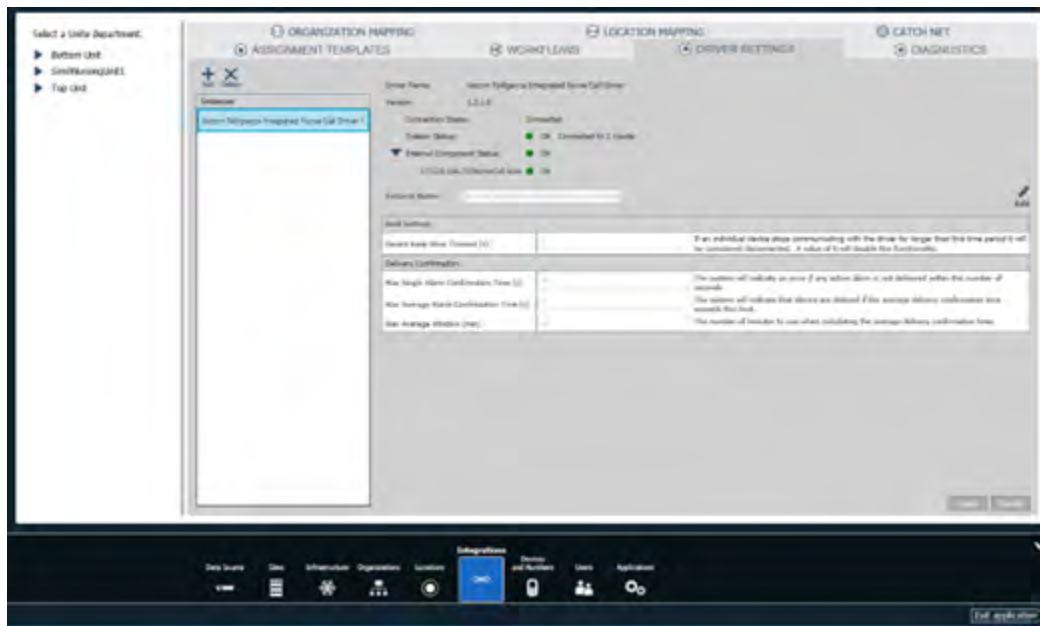
8 Catchnet

When a Unite alert has not been addressed by the assigned staff on a shift, it is sent to Catchnet as a final redirection level before being sent to Unhandled. Catchnet is an Ascom Unite function in which unacknowledged alerts are automatically distributed to additional recipients independently of the current location's user assignments. You can set up which users to include in the Catchnet for each alarm/event type.

This feature mitigates the risk that alarms are missed if none of the recipients who are assigned to a location with an active alarm respond to it within the configured timeouts. By default, Catchnet distributes an alert to "All on Shift" (all staff members on the shift who are assigned a display device) if the alert has not been acknowledged on assignment levels 1, 2 and 3. You can copy any configuration of Catchnet which has been completed for different units in two ways:

8.1 Copying from another Unit

1. Click **Option** for the unit to copy Catchnet settings into.

2. From the **Copy Catchnet from** drop-down list, select the unit from which to run copy Catchnet settings.

3. Click **Copy**.
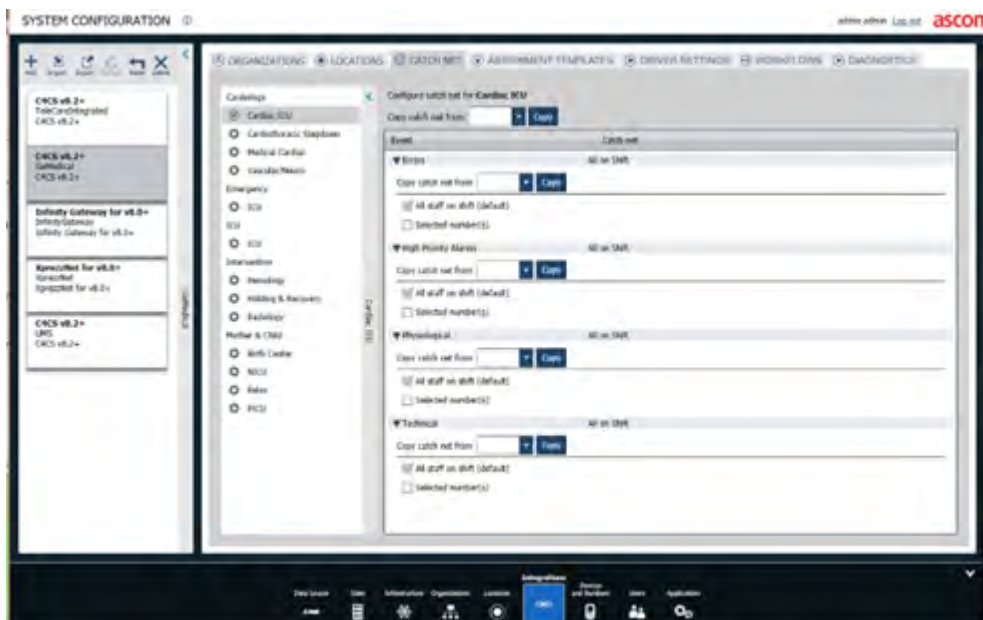
8.2 Copying from Another Unite Event

1. Press **Option** to copy a unit.

2. Expand the Unite event node in which to copy Catchnet settings.

3. From the **Copy Catchnet from** drop-down list, select the event from which to run copy Catchnet settings

4. Click **Copy**.

9   Logging

Activity generated within the Connect for Clinical system, including the dispatching of Alerts as a result of incoming alarms are all distributed via the System Activity Logging function of Unite. This mechanism along with the Unite Analyze product provides centralized persistent logging of all notifications transmitted by the Connect for Clinical system, enabling troubleshooting and efficiency reports to be generated as needed.

The system activity log shows alert traffic including all generated alerts that have been delivered to, and accepted by, remote devices. See Unite Analyze 6.x, Configuration Manual, TD 93244EN and Unite Analyze, 6.x User Manual, TD 93168EN.

The system activity log can be viewed by launching the "Ascom Unite Activity Viewer" from Unite PS. See Unite Platform Server, Configuration Manual, TD 93280EN

Appendix A　　　Clinical System Protocols

This appendix describes the functionality of clinical systems and any protocol-specific limitations.

Dräger Infinity

- Protocol Version: Dräger Infinity Gateway VF7.2 and VF9.0.1.

- Maximum Number of Monitors: 256 with or without waveforms.

- Maximum Number of Gateways: 2 (one gateway per driver instance).

- Connectivity: API over TCP Socket

Delays	
Physiological alarm condition occurs till reported by Patient Monitor.	< 6 seconds (Asystole)
Physiological alarm Delivered to Display Device (handset).	< 2 second
TOTAL Physiological Alarm (High Priority).	**< 8 seconds**
Technical alarm condition occurs till reported by Patient Monitor.	<1 second
Technical Alarm Delivered to Display Device (handset).	< 1 second

Spacelabs XprezzNet

- Protocol Version: XprezzNet 1.3.0 & 1.3.1.

- Maximum Number of Monitors: 128 per driver instance.

- Maximum Number of Gateways: 2 (one gateway per driver instance).

- Connectivity: TCP Web API.

Delays	
Physiological alarm condition occurs till reported by Patient Monitor.	~ 5 seconds (Apnea)
Physiological alarm Delivered to Display Device (handset).	< 1 second
TOTAL Physiological Alarm (High Priority).	**< 6 seconds**
Technical alarm condition occurs till reported by Patient Monitor.	~1 second
Technical Alarm Delivered to Display Device (handset).	< 1 second
TOTAL Technical Alarm (Medium Priority).	**< 2 seconds**

Digistat Suite

- Maximum Number of Locations: 1,000 per driver instance.

- Maximum Number of Connections: 4.

- Connectivity: TCP.

Delays	
Physiological alarm condition occurs till reported by clinical device.	Dependent on clinical device refer the specific Digistat MD Driver device details
Physiological alarm Delivered to Display Device (handset).	< 2 second
TOTAL Physiological Alarm (High Priority).	**Typically less the 8 seconds**
Technical alarm condition occurs till reported by Patient Monitor.	Dependent on clinical device refer the specific Digistat MD Driver device details.
Technical Alarm Delivered to Display Device (handset).	< 2 second
TOTAL Technical Alarm (Medium Priority).	**Typically less the 8 seconds**

⚠️ **Caution**

It can take up to two seconds between the alarm generation and the alarm sending on the Digistat Suite. The Digistat Suite then waits for an acknowledgement from the Product. If such acknowledgement is not received within two seconds a timeout occurs. Therefore, the maximum delay after which an alarm notification is provided is 4 seconds. If there is a timeout:

  A connection alarm is triggered. The alarm can be canceled by the user. It is also canceled if a new connection with Confirmed Delivery is established.

  Digistat Suite data sending and Confirmed Delivery is stopped until a new connection is established. If Digistat Care is not in Reliable state, it immediately attempts to restore connection without Confirmed Delivery.

GE CARESCAPE Unity

- Protocol Version: 0 and 1.

- Maximum Number of Monitors: 1,000 per driver instance.

- Connectivity: UDP.

Delays	
Physiological alarm condition occurs till reported by Patient Monitor.	< 5 seconds (Asystole)
Physiological alarm Delivered to Display Device (handset).	< 1 second
TOTAL Physiological Alarm (High Priority).	**< 6 seconds**
Technical alarm condition occurs till reported by Patient Monitor.	< 2 seconds

Technical Alarm Delivered to Display Device (handset).	< 1 second
TOTAL Technical Alarm (Medium Priority).	**< 3 seconds**

teleCARE IP Nurse Call

- Maximum Number of Locations:
  - 6000 Locations (Rooms/Beds) divided across up to 10 NISMs/vNISMs, where no single NISM/vNISM exceeds 2000 locations.
  - 500 locations in a single NISM/vNISM (Small Footprint Unite deployment).
- Maximum Number of Gateways: 10 per installation, with 30 teleCARE IP systems and 18,000 locations supported across 3 installations on the same node.
- 1 gateway and 1 installation on the node (Small Footprint Unite deployment).
- Connectivity: UDP (Unite Protocol).

Delays	
Physiological alarm condition occurs till reported by Nurse Call.	< 5 seconds (Medical High)
Physiological alarm Delivered to Display Device (handset).	< 1 second
TOTAL Physiological Alarm (High Priority).	**< 6 seconds**
Technical alarm condition occurs till reported by Nurse Call.	< 2 seconds
Technical Alarm Delivered to Display Device (handset).	< 1 second
TOTAL Technical Alarm (Medium Priority).	**< 3 seconds**

Telligence Nurse Call

- Maximum Number of Locations:
  - 6000 Locations (Rooms/Beds) divided across up to 10 IMTs, where no single IMT exceeds 2000 locations.
  - 500 locations in a single IMT (Small Footprint Unite deployment).
- Maximum Number of Gateways: 10 per installation, with 30 Telligence systems and 18,000 locations supported across 3 installations on the same node.
- 1 gateway and 1 installation on the node (Small Footprint Unite deployment).
- Connectivity: UDP (Unite Protocol).

Delays	
Physiological alarm condition occurs till reported by Nurse Call.	< 5 seconds (Medical High)
Physiological alarm Delivered to Display Device (handset).	< 1 second

TOTAL Physiological Alarm (High Priority).	**< 6 seconds**
Technical alarm condition occurs till reported by Nurse Call.	< 2 seconds
Technical Alarm Delivered to Display Device (handset).	< 1 second
TOTAL Technical Alarm (Medium Priority).	**< 3 seconds**

Appendix B   Troubleshooting

A number of tools can be used to view the health, status and operation of the installed system and to help diagnose problems should they arise.

With multiple instances installed, each installation instance logs to the Windows Event Log and to Buslogger independently. These diagnostics logs are used for troubleshooting and diagnostics that enable independent troubleshooting of each instance, with independent log configurations.

B.1   Connect Supervisor

The Connect for Clinical Systems Supervisor is a windows service that is used to monitor the status of all installed C4CS components as well as the status of message delivery in each nursing unit.

The C4CS Supervisor can be opened within a web browser application on the server at the address: `http://ServerName:8190`. It can also be accessed via a RESTful API at `http://ServerName:8190/api/status`. Port 8190 represents the default port number for the current installed instance. With the addition of other installed instances, this port number automatically increments (8290, 8390, etc.) as described in . The C4CS Supervisor monitors all installed components necessary for delivery of alarms, including Unite View and/or Unite Axess if they are installed. Each component has an individual status indicator that shows if it is 'OK', or is reporting a 'Warning', or 'Error' condition. This status indicator for each component can be clicked to see details on the status of that component.


B.1.1   Connect for Clinical Systems Self Test

A self test is generated by the driver host for each integration with a driver instance. The self-test ensures that the system is operational at all times and detects connectivity issues. It is performed at regular intervals

that can be configured, and the default is 60 seconds. If a response is not received within that time period, an error is reported.

The Connect for Clinical Systems Self Test is found under Infrastructure tab. Select Unite Platform Server, Settings, and under Connect for Clinical Systems select Self Test.
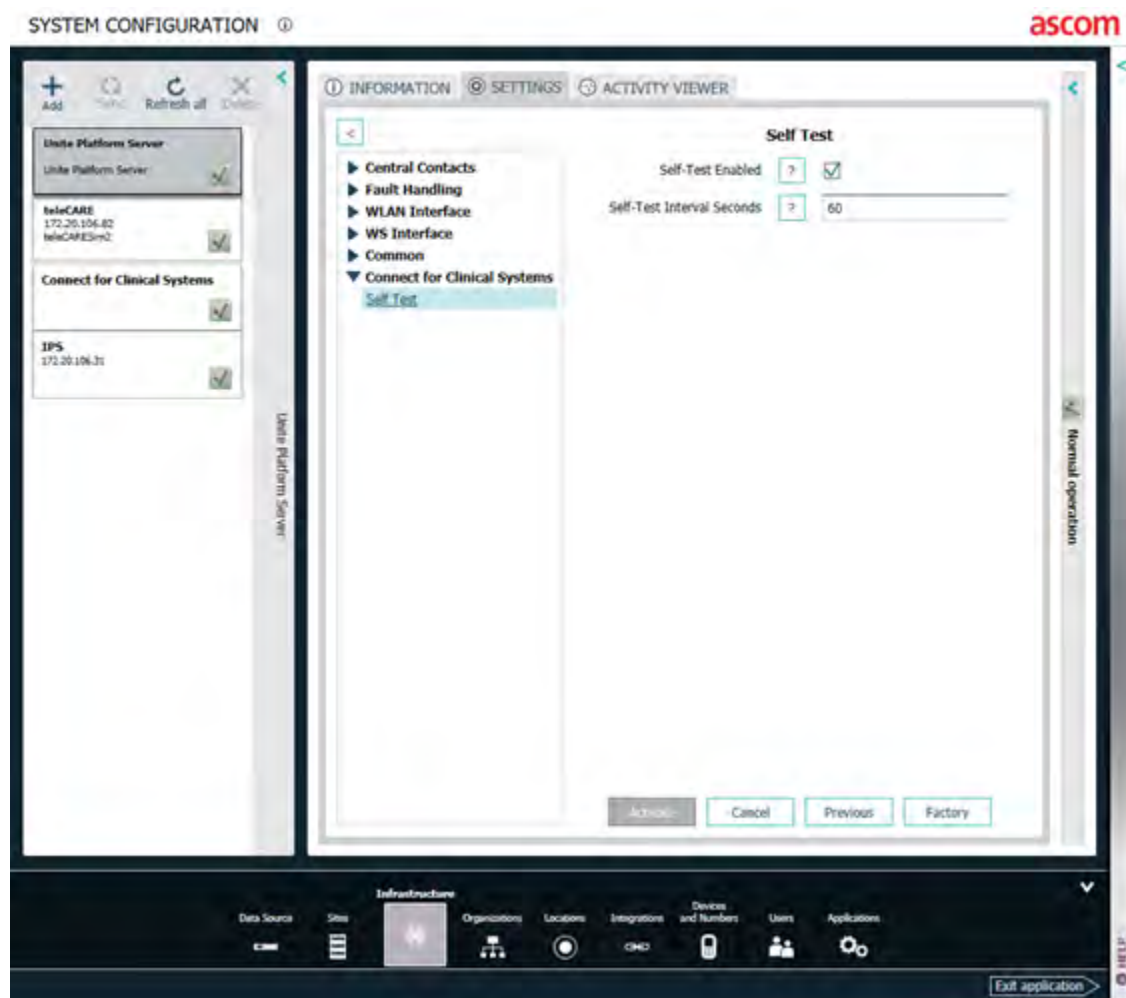
B.2   Supervision Hub

The supervision hub is an in-browser web tool that monitors the status of installed Unite Server Applications. It can be opened within a web browser application on the server at this address: `http://localhost:8181`.

A hyperlink allows navigation from the :8181 page to the :81XX page, which provides access to a status page with driver status details.

The Connect Application has 3 components: Alarm Service Engine, Drivers and Event Manager. Each component has an individual status indicator that shows if it is 'OK', or is reporting a 'Warning', or 'Error' condition. Each application has an aggregate overall status indicator as well, according to the status of the components it comprises.

Connect for Clinical Systems reports the status of its components to the Unite Supervision Hub. This status includes an indication of the severity of faults within the components (OK, Warning, or Error). Each component informs the supervision hub when a new error or warning condition starts as well as the end of

those conditions. The Unite Supervision Hub reacts to this information by initiating Unite Faults that can be forwarded to local or remote fault handlers.

The Unite Application Server dashboard has three views showing **Current** status, the **History** of status changes over time and **Diagnostics** information that contains a real-time graph of server CPU and memory resource loading.
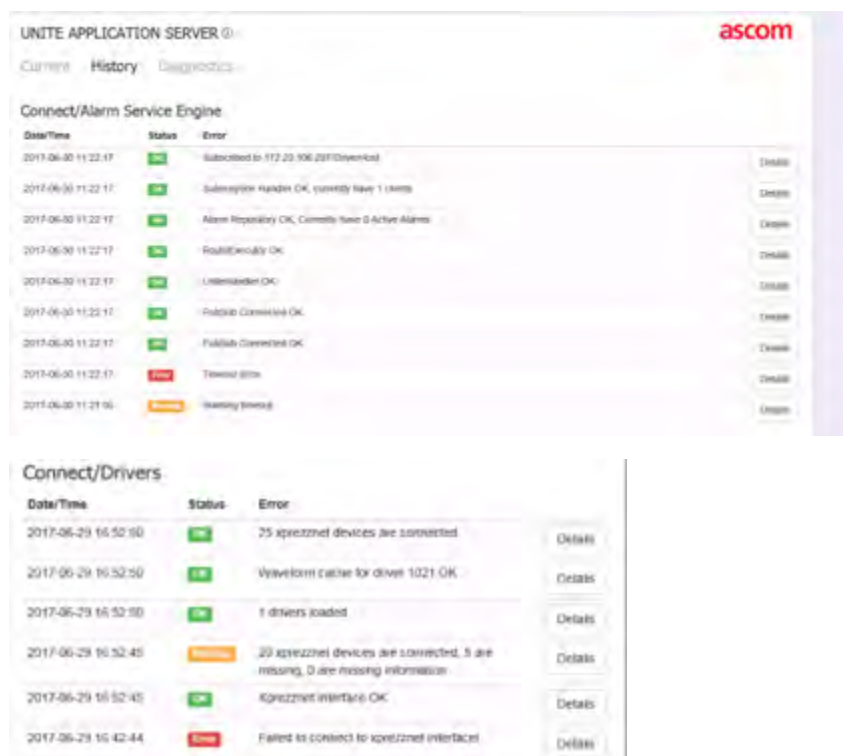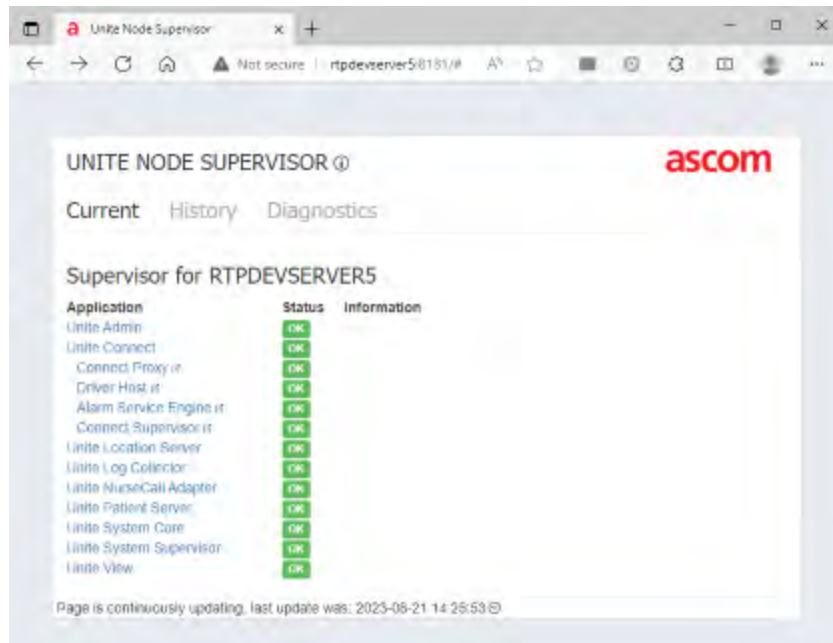
B.3   Event Viewer

The Event Viewer application can be used to view more detailed information and errors in the Application event logs. Log entries specific to Connect for Clinical Systems applications can be found by selecting "Applications and Services Logs\Unite Connect" from the tree view.
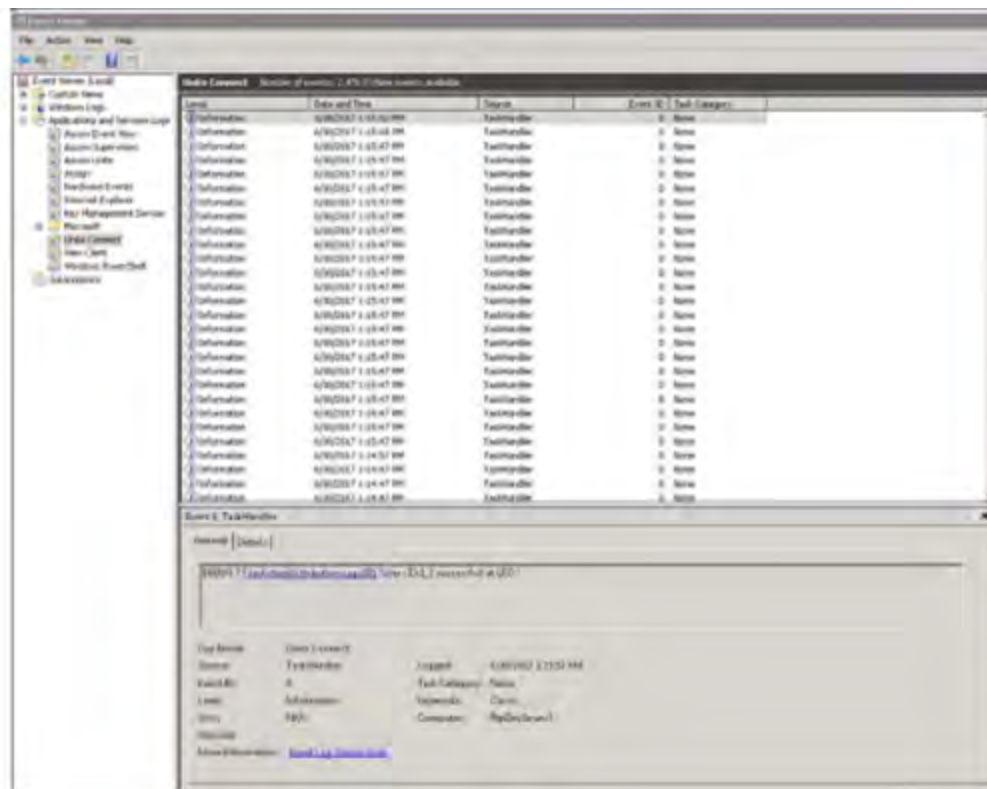
B.4   Buslogger

The Buslogger application can be used to view detailed network message traffic between C4CS applications. The minimum version of Buslogger required to support Connect for Clinical Systems is 4.02

To monitor and capture traffic from Connect for Clinical Systems, desired elements from the following Applications must be selected: Driver Host, and Alarm Service Engine.
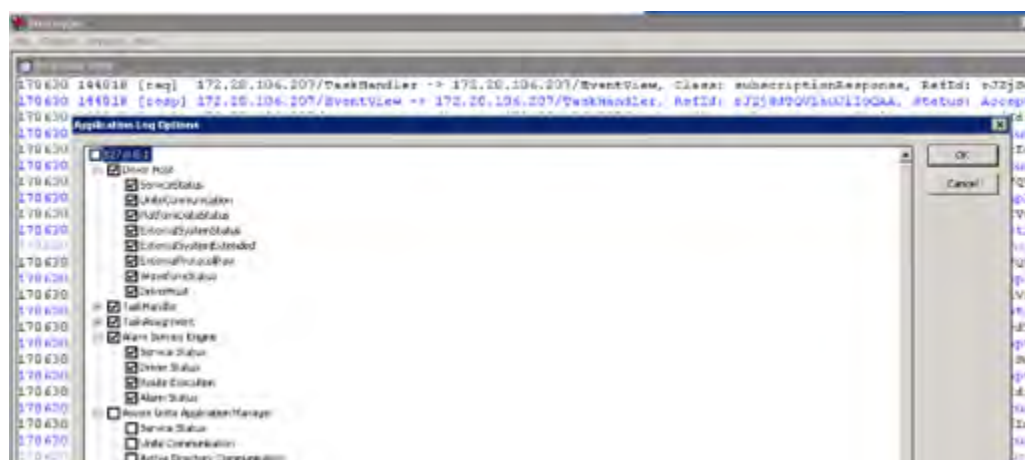
B.5   Raw Logging

It is possible to mirror all traffic that the drivers receive from external systems by enabling raw logging. Raw logging can be enabled for event traffic as well as waveform traffic. The raw logs will be forwarded as UDP packets to a configurable IP address and Port. To enable raw logging, open the Driver Host config file located in the installed location and change the content in the following fields and save the config file. The changes will take effect when the file is saved.

RawEventLogEnabled (change to 'true' to enable and 'false' to disable).

RawWaveformLogEnabled (change to 'true' to enable and 'false' to disable).

DestinationAddress (IP address of the UDP destination).

DestinationPort (the Port to send the UDP data to).
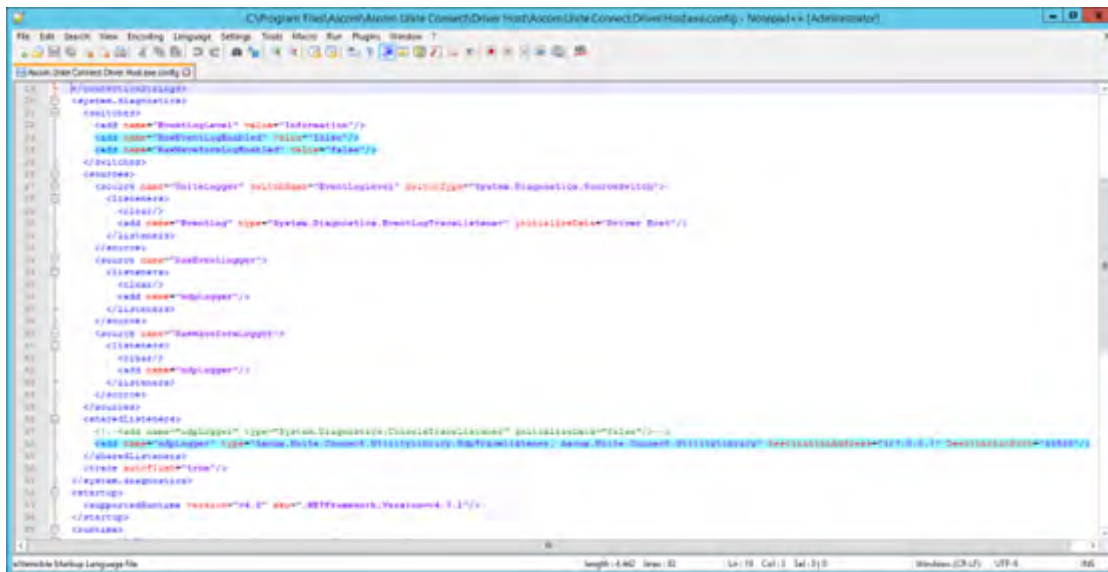
Appendix C   URL for launching Airstrip and Digistat Smart Central Mobile

URLs/URIs can be embedded in an alert message that trigger the launch of an application that is installed on a smart device. The Airstrip and Digistat applications can be opened dynamically on a smart device by including a softkey in the alert message that contains the following formatted URLs/URIs:

- Airstrip: `airstripone://ascom/pm-mon?siteid=1&bed=<!ExternalBedId>&unit= <!ExternalUnitName>`
  Where:

  - ExternalBedId and ExternalUnitName are already Elements that C4CS dynamically maintains for every event.

  - siteId is a variable which can be set statically when defining the Interactive option and should correspond to the site id defined by Airstrip for the customers installation. If there is a different siteId required per Unit, it is necessary to define a separate message template and Workflow specific to the individual Units where the siteId may differ.

- Digistat: `digistatmobile://query?module=SMARTCENTRALMOBILE&command=<!UniteLocationId>`

Appendix D   Acceptance Test

The acceptance test ensures that the functionality of the Ascom messaging system installed, complies with the expectations of the customer. Acceptance testing should be performed after installing, configuring and/or revising the system. This includes any event that alters a previously approved system configuration (e.g., introducing and/or handling additional locations or events that were not present during the previous acceptance test).

The approval sheets, found on the following pages in this appendix, should be completed to record that the system configuration conforms to established installation standards.

When the test is completed and verified according to customer requirements, the approval sheets are to be signed by both parties, i.e. the installer from Ascom and the customer.

By signing the approval sheets, the parties agree that the equipment meets the requirements after installation and configuration. The intended functionality should be operational to a degree only limited by needs associated with adjunct or supporting peripherals that Ascom has no control over. Operational deficiencies should be noted, and appropriate actions specified, in the approval sheets.

> **Warning**
>
> Acceptance testing must be performed for each location supported by this product. Failure to complete acceptance testing may result in failed or delayed notification, resulting in potential patient harm. Functional verification of the products should occur before the product is used in a clinical environment with a live patient. Additionally, this testing should be repeated after any changes to the configuration or system upgrades. The following needs to be tested and verified:

Locations[1]	Perform a function check for each location
Alert types:	All alert types, possible to send from a location, need to be tested.
Alert priorities:	Ensure that the alert priorities are in accordance with the customer.
Redirection chains:	Verify that the redirection chains operate according to the customer's requested Workflow.
Default destination:	Verify that a default destination has been configured in the redirection chains.
Filter settings:	Verify that filtering settings work as intended. Filters are used for reducing the number of non-relevant alerts and thereby minimizing the number of messages sent to clinicians.

1.   A location is a place from where an alert can be sent.

Unit	Location	Filter	Filter Setting	Tested	Comments
e.g. CCU	e.g. BED 1	e.g. STOP	e.g. *PVC	e.g. Ok, NOk	

Assigned	Delay (in secs)	Accept & Busy	Repeat	Escalation time	Escalation time	Recipient Level 3	Recipient Level 2	Recipient Level 1	Escalation Levels	Alert Choice
e.g. Per	e.g. no	e.g. Yes/No/Other	e.g. Yes/No	e.g. 60 seconds	e.g. 60 seconds	e.g. Charge RN	e.g. Backup co-	e.g. Primary CG		e.g. Tachy

D.1   Acknowledgment

Alert specifications are used for configuration programming and post-installation testing. This alert configuration is active in the production system unless otherwise noted in superseding documentation such as the post installation checklist.

Date										
Facility name:	Unit(s)									
Site Representative										
Name										
Signature	Date									
Title	Phone/email									
Ascom project manager										
Name										
Signature	Date									
Title	Phone/email									
Ascom Clinical Application Specialist										
Name										
Signature	Date									
Title	Phone/email									

Appendix E   Related Documents

Unite View, Installation Guide, TD 93068EN

Unite View, User Manual, TD 93008EN

Connect for Clinical Systems, Data Sheet, TD 93252EN

Unite Platform Server, Configuration Manual, TD 93280EN

Unite Platform Server, Data Sheet, TD 93266EN

Unite Platform Server, Installation Guide, TD 93273EN

Unite Assign Client, Installation Guide, TD 93200EN

Pre-configuration of Windows for Unite Applications, Configuration Notes, TD 92993EN

Unite EHR Integration, Installation and Operation Manual, TD 93417EN.

Unite Communication Server, Configuration Manual, TD 92761EN

Unite Connectivity Manager, Configuration Manual, TD 92735EN

Unite Analyze 6.x, Configuration Manual, TD 93244EN

Unite Analyze, 6.x User Manual, TD 93168EN

Appendix F   Document History

Version	Date	Description
P	18 September 2023	The following features were added for this release: 1.6 Software Requirements, page 9 – updated RabbitMQ versions, updated "Framework," and added SFU information.\ Small Footprint Unite deployment updates: 2.6 Small Footprint Unite (SFU) Deployment, page 15, teleCARE IP Nurse Call, page 123 and Telligence Nurse Call, page 123. New subsections 1.11 Download the Connect for Clinical Systems Software, page 12 and 1.11.1 Validate Downloaded Software File, page 12. 4.2 RabbitMQ Settings, page 23 — added note. 4.4 Component Selection, page 26 – added information on Upgrade and Keep Version options. 5.7.1 Organization Mapping, page 45 – added information about the ability for multiple Nurse Call organizations to be mapped to a single Unite organization. 5.9 Assignment Templates, page 47 – updated icon table. 6.2.3 Default Workflows, page 63 – updated table with new Telligence default workflows. 6.2.7 Conditions, page 72 – updated element table and added "I can be used to join multiple expressions" to "Ascom Regular Expression" in Comparison table. 6.2.12.5 Message Templates, page 95 – updated table. New section 6.3.3 Unite External Event API, page 104. 7.4 Digistat Suite Driver, page 112 – added Device Keep Alive Timeout(s) setting. 7.6 Nurse Call, page 115 – added bullets with information for multiple Nurse Call organizations to be mapped to a single Unite organization and SFU support. 9 Logging, page 120 – Updated information about how to view the system activity logs using Unite PS. B.2 Supervision Hub, page 126 – Added information about navigation from the :8181 page to the :81XX page and how internal errors and faults are reported.

O	26 January 2023	The following features were added for this release:
		Identification of patients based on wireless badge ID's received from teleCARE nurse call systems.
		Location information in alerts to mobile devices,
		Assignment based on home location for wireless teleCARE nurse call events,
		Support for events generated by Unite backend
		Telligence Service tasks.
		Telligence Rounding tasks.
		Fault reporting for events at unknown locations or unknown events.
		Support for Reliability Status Output Protocol.
A — N		Released versions prior to the Document History were added to the document.

ascom