**Covidien**

System Requirements Specification

V1.2

Document Control

* Issued May 22, 2011
* Version 1.2
* Author John Dougherty
* Status: ready for final sign-off
* All contents are confidential.

Table of Contents

[Document Control 2](#_Toc325474365)

[1. Introduction 5](#_Toc325474366)

[1.1 Purpose of document 5](#_Toc325474367)

[1.2 Scope of document 5](#_Toc325474368)

[1.3 Structure of document 5](#_Toc325474369)

[2. Applicable and Reference Documents 5](#_Toc325474370)

[2.1 List of documents [move to architecture doc] 5](#_Toc325474371)

[Document 5](#_Toc325474372)

[Status 5](#_Toc325474373)

[Definitions 6](#_Toc325474374)

[3. General Description 6](#_Toc325474375)

[3.1 Perspective 6](#_Toc325474376)

[3.2 Related projects 7](#_Toc325474377)

[3.3 System Environment 7](#_Toc325474378)

[3.4 General constraints [ move to architecture doc] 8](#_Toc325474379)

[4. Specific Requirements 8](#_Toc325474380)

[4.1 Functional Requirements 8](#_Toc325474381)

[User Login 8](#_Toc325474382)

[Users 10](#_Toc325474383)

[Roles 11](#_Toc325474384)

[Access Policy 11](#_Toc325474385)

[Laptop Agent 12](#_Toc325474386)

[Device Identification 15](#_Toc325474387)

[Server Business Rules 16](#_Toc325474388)

[Device State Verification 22](#_Toc325474389)

[System Activity Tracking 23](#_Toc325474390)

[Laptop Agent Maintenance 24](#_Toc325474391)

[Notifications 25](#_Toc325474392)

[Reporting 26](#_Toc325474393)

[4.2 Interface Requirements 27](#_Toc325474394)

[4.3 Operational Requirements 27](#_Toc325474395)

[Operating Location 27](#_Toc325474396)

[Geography / Language 28](#_Toc325474397)

[4.4 Resource Requirements [to be moved to the SRD] 29](#_Toc325474398)

[Hardware 29](#_Toc325474399)

[4.5 Verification Requirements [ to be moved to the SRD ] 30](#_Toc325474400)

[Verification Requirements 30](#_Toc325474401)

[4.6 Documentation Requirements [to be moved to the SRD] 32](#_Toc325474402)

[Control system documentation, distribution, access, and use. 32](#_Toc325474403)

[4.7 Quality Requirements [move to SRD] 32](#_Toc325474404)

[Quality Requirements 32](#_Toc325474405)

[Control system documentation, distribution, access, and use. [move to SRD] 32](#_Toc325474406)

[4.8 Safety Requirements 33](#_Toc325474407)

[Safety Requirements 33](#_Toc325474408)

[4.9 Reliability Requirements 34](#_Toc325474409)

[Reliability Requirements 34](#_Toc325474410)

[Performance and Scalability Requirements 34](#_Toc325474411)

[4.10 Maintainability Requirements [to be moved ot the SRD] 34](#_Toc325474412)

[Maintainability 34](#_Toc325474413)

[The system shall have 70% unit test coverage. 34](#_Toc325474414)

[The system shall use pattern based designs. 34](#_Toc325474415)

[The source code shall be documented. 34](#_Toc325474416)

[The system shall have an E/R diagram for the database. 34](#_Toc325474417)

[The system shall have a systems architecture document capturing the overall system design. 34](#_Toc325474418)

[The system shall use static code analysis to catch and prevent coding errors. 35](#_Toc325474419)

[Schedule A [ move to SRD] 36](#_Toc325474420)

[Schedule B 36](#_Toc325474421)

[Schedule C 36](#_Toc325474422)

# Introduction

The system requirements are mostly complete and are ready for collaboration discussions with the Covidien team. Other sections will be completed in April in various meetings with the Covidien team.

## Purpose of document

This System Requirements Specification (SRS) contains the set of system requirements for the Covidien release 1 communication Gateway. This document is provides sufficient guidance to the development team to allow them to begin software development. While hardware will be specified, the focus is on software development.

## Scope of document

The focus for release one is the PB980 Series Ventilator Remote Service solution and related infrastructure. This SRS lays the ground work for the development of the full Gateway solution over three phases of release.

## Structure of document

The next two sections will provide the background needed to understand the specific requirements in section four.

# Applicable and Reference Documents

## List of documents [move to architecture doc]

|  |  |
| --- | --- |
| Document | Status |
| User Requirements Document (URD) version information | in process |
| Covidien System Proposal | in process |
|  |  |

## 

## Definitions

**GA** – General Availability meaning that the product is now in general release and orders are being actively taken and delivered to customers.

**Entity** – for the purposes of this document, an entity is a first class object of the problem domain. It can be uniquely identified; plays an important role in the system; and has data attributes. Examples include device, user, role, and report. [see canonical class form for entities]

**Design by Contract (DbC)-** also known as contract programming, programming by contract and design-by-contract programming, is an approach for designing software. It prescribes that software designers should define formal, precise and verifiable interface specifications for software components, which extend the ordinary definition of abstract data types with preconditions, postconditions and invariants. These specifications are referred to as "contracts", in accordance with a conceptual metaphor with the conditions and obligations of business contracts.

**Software Manifest –** the listing of all software files. The name of the files or applications that are packaged together.

**Test Driven Development - (TDD)** is a software development process that relies on the repetition of a very short development cycle: first the developer writes a failing automated test case that defines a desired improvement or new function, then produces code to pass that test and finally refactors the new code to acceptable standards. Kent Beck, who is credited with having developed or 'rediscovered' the technique, stated in 2003 that TDD encourages simple designs and inspires confidence.

**Viking**- Viking is the code name for Covidien RMS next generation ventilator project.

**Enterprise One** – From the perspective of this project, E1 is the next generation service management system which is replacing the existing service management system.

# General Description

## Perspective

This project will automate much of the service activities, data collection, and tracking for Covidien’s field services. From an infrastructure perspective this initial release provides the communication backbone for field service and related management activities. This is a Covidien wide development project and other devices will build on this infrastructure.

Release 1 of the Gateway will interface with Covidien’s PB980 Ventilator Test System (VTS) client application in support of the PB980 Ventilatortm. It will be used in the field by both certified client personal like hospital-based Biomedical-Technicians and by the Covidien Customer Support Engineer (CSE). It will provide functionality for software updates to the Ventilator; manage the catalog of software; provide a mechanism to acquire the Ventilator logs; produce web-based reports; and track service history through a web interface. The software catalog is a collection of software versions which is searchable by the important device configuration attributes, including model hardware version, installed options and current software configuration. For the Covidien Service Managers and Sales staff it will provide service management reports.

The Covidien ForceTriad will be the next device to follow in the second release. It will be important to isolate the field service technician’s access to the system based on the division they support.

## Related projects

|  |  |  |
| --- | --- | --- |
| Project | Expected Release | Contact |
| Viking -developing the  PB980 Series Ventilator | EMEA Beta 1 – October 2012  December 2012 (end of beta 1) | Gail Upham |
| PB980 VTS update | December 2012 | Sid Jacobi |
| Enterprise One – complete redeployment of existing back end infrastructure | Q1 FY13 | Jeff Wysocki |
| ForceTriad next generation development | May 2013 | Maureen Richard |

## System Environment

This is an overview of the system. The approach is based on enterprise systems architecture. The focus is on the deployment of enterprise scale web application and infrastructure. The backend systems will connect to an agent running in the Covidien laptops in the first version. The system consists of a DDS gateway, data loggers, an end user web application, a software revision catalog and update service, configuration and transactional database, role based authentication and authorization services, reporting services, cloud based communication and storage services, and system maintenance configuration and status.

The gateway agent will eventually run on multiple end user devices including laptops running Windows XP, 7, iOS, and handheld devices running Android O/S. It will interface with the next version of the VTS software running on a Windows laptop in Release 1.

For safety and data reliability reasons, the system will capture an acknowledgement from the installer once an update of the Ventilator software is complete. This will allow the gateway to verify the state of the Ventilator.

## General constraints [ move to architecture doc]

The software in release 1 must be GA ready by December 2012.

# Specific Requirements

## Functional Requirements

| **Req. #** | **Requirement** | **Priority** | **Use Case Reference** |
| --- | --- | --- | --- |
|  | User Login |  |  |
|  | The systems web interface shall start with a login screen for both the customer and internal employees.  [This is the web interface to the backend server.] |  |  |
|  | The system shall support user authentication via the web interface. |  |  |
|  | The system shall prompt with user-name and password credentials. |  |  |
|  | System shall support username and password authentication. |  |  |
|  | The system shall support user authorization. |  |  |
|  | The system shall support role based authorization. |  |  |
|  | The system shall support the following roles:  System Administrator  Application Support  CSE  Sales Rep  RandD  QA  Service manager  Biomed |  |  |
|  |  |  |  |
|  | The system shall move to the ‘home’ screen if the user’s authentication and authorization test pass. |  |  |
|  | The system shall return to the login screen if the user’s authentication and authorization tests fail. |  |  |
|  | The system shall respond with a failed user login message.  [It is a security risk to provide any response here and it makes it easier to be successfully using a DOS attack against the site. Given that we may respond to the user with a login failed ] |  |  |
|  | The system shall provide no information to the user in the case of a failed login attempt. |  |  |
|  | The system shall lock out the user’s account for a time span if it fails the login five times. |  |  |
|  | The system administrator role shall have the right to configure the lock-out period for failed logins. |  |  |
|  | The system shall provide help desk contact information on the login page.  [Who’s help desk information on the login page] |  |  |
|  | The system shall log failed login attempts including time, username, and hostname. |  |  |
|  | Users |  |  |
|  | The system shall allow the creation of new users. |  |  |
|  | The system shall send the user IDs and Passwords separately. |  |  |
|  | The system administrator role shall oversee and confirm new users. |  |  |
|  | User Data shall include:  First Name  Last Name  Role/Titile  Login Name  Password  Password expiration  User e-mail  Is Covidien Employee  Covidien Business Unit  Covidien Location  Covidien Department  Company Name |  |  |
|  | Customer data shall include:  Customer Account Number  Customer Name  Customer Address  Customer Contact Name |  |  |
|  | The system shall identify the customer hospital, distributor or third-party a user works for if they are not a Covidien employee. |  |  |
|  | The system shall allow the editing of user credentials based on role.  [which roles have this right is configurable by setting the access policy associated with the role. This gives the system the flexibility to change over time as needs change.] |  |  |
|  | The system shall allow the disabling of user credentials based on role. |  |  |
|  | The system shall allow the assignment of user credentials to a role. |  |  |
|  | Roles |  |  |
|  | The system shall allow the creation of new roles. |  |  |
|  | The system shall assign the right to create new roles through the access policy. |  |  |
|  | Role Data shall include  Role Name  Description  Covidien Department |  |  |
|  | The system shall allow the editing of roles based on access policy. |  |  |
|  | The system shall allow the disabling of roles based on access policy. |  |  |
|  | The system shall allow the assignment of access policies to roles. |  |  |
|  | They system shall allow the review of users assigned to a role. |  |  |
|  | They system shall allow the review of access policies assigned to a role. |  |  |
|  | The system shall define device types. (PB 980, ForceTriad, etc.) |  |  |
|  | They system shall include device type as part of the access policy. |  |  |
|  | The system shall allow user access based on device type. |  |  |
|  | Access Policy |  |  |
|  | All system users, agents, or tasks shall run under an access policy. |  |  |
|  | The system shall allow the creation of access policies. |  |  |
|  | The system shall allow the editing of access policies. |  |  |
|  | The system shall allow the deleting of access policies. |  |  |
|  | The system shall log the use of access rights granted by the policies. |  |  |
|  | The system shall use access policies to manage access to administration activities. |  |  |
|  | The system shall use access policies to manage access to user workflow activities.  [here user workflows are the screens and menu items that a role has access to throught the web interface. They are created in development. If your role does not have access the menu item will be disabled. ] |  |  |
|  | The access policies shall govern create rights across entities. |  |  |
|  | The access policies shall govern read rights across entities. |  |  |
|  | The access policies shall govern update rights across entities. |  |  |
|  | The access policies shall govern delete rights across entities. |  |  |
|  | The access policies shall govern access privileges to workflows within the system. |  |  |
|  | Laptop Agent |  |  |
|  | The system shall provide a laptop agent. |  |  |
|  | The laptop agent shall run on the operating systems defined in schedule B.  [We are using schedule B to allow the documented list of operating systems to grow over time. ] |  |  |
|  | A single instance of an agent shall be able to communicate with and update software on one device. |  | \* |
|  | The system shall operate through http on port 80. |  |  |
|  | The system shall operate through https on port 443. |  |  |
|  | The laptop agent shall provide an API for the PB980 Vent Test Software (VTS). |  |  |
|  | The laptop agent shall collect device identifying information through the PB980 VTS API. |  |  |
|  | The laptop agent shall accept logs from the PB980 VTS through the API. |  |  |
|  | The laptop agent shall manage the download of software from the server. |  |  |
|  | The system shall notify the PB980 VTS of completed software downloads via the API. |  |  |
|  | The laptop agent shall cache the software package locally. |  |  |
|  | The laptop agent shall check the package cache before downloading software packages to avoid duplication. |  |  |
|  | The system shall encrypt the software manifest. |  |  |
|  | The encrypted components of the package shall be decrypted in memory prior to installing on the device. |  |  |
|  | The laptop agent shall delete the software package from the laptop when a configurable expiration time has expired. |  |  |
|  | The laptop agent shall completely delete the package. |  |  |
|  | The laptop agent shall completely delete a package when instructed to by the server. |  |  |
|  | The laptop shall support scripting languages. |  |  |
|  | The installation application shall be allowed to run pre installation scripts. |  |  |
|  | The installation application shall be allowed to run post installation scripts. |  |  |
|  | The laptop agent shall support the execution of scripted commands with or without any accompanying software updates. |  |  |
|  | The system shall allow files to be transferred to the laptop from the server with or without any accompanying software update. |  |  |
|  | The system shall provide secure communication channels for sending data.[like https] |  |  |
|  | The system shall provide secure communication channels for receiving data. |  |  |
|  | The system shall automatically compress transmitted data. |  |  |
|  | The laptop agent shall cache its data during a download. |  |  |
|  | The laptop agent shall cache its’ data during upload. |  |  |
|  | The laptop agent shall keep cached log files for 24 hours after receipt of a successful upload of the log files.  [This is a Disaster Recovery (DR)provision to help protect the system from data loss.] |  |  |
|  | The laptop agent shall be able to resume download to its download cache if communication is interrupted. |  |  |
|  | The agent shall provide status notification of the software download process. |  |  |
|  | The agent shall provide status notification of the logs upload process. |  |  |
|  | The laptop agent shall provide status notification of errors. |  |  |
|  | The laptop agent shall provide notifications identifying problems and solutions as they occur in the process. |  |  |
|  | Device Identification |  |  |
|  | The system shall accept device identification. |  |  |
|  | The system shall enumerate devices by device type. |  |  |
|  | The device types shall include those identified on schedule C. |  |  |
|  | Device identifying information shall include:  Device Type  Device serial number  Device hardware  Device hardware version  Device hardware option(s)  Device software  Device software version  Device software option(s)  Device software option version(s) |  |  |
|  | The system shall maintain a map between the device type, serial number and the customer.  [Serial numbers are not guaranteed to be unique across business units so its important to qualify then with Device Type.] |  |  |
|  | The system shall receive an initial upload of existing registration data for device and customer information. |  |  |
|  | The system shall maintain software entitlement per customer and serial number |  |  |
|  | Device identifying information shall be exchanged in XML format. |  |  |
|  | Server Business Rules |  |  |
|  | The system shall be 21CFR Part 11 compliant to the extent that each upgrade record is considered an electronic record. |  |  |
|  | The system shall not delete records or data rows that are part of the audit trail. |  |  |
|  | The system shall mark data records as inactive when asked to delete them. |  |  |
|  | The system shall provide for segmentation of PHI and PII from non-protected data. |  |  |
|  | The system shall determine most current software for the device based on the device configuration information. |  |  |
|  | The system shall schedule software updates. |  |  |
|  | The system shall be capable of automatically grouping devices according to a device type for viewing at the server. |  |  |
|  | The system shall recognize a new device through device identification. |  |  |
|  | The system shall add new devices to the device list. |  |  |
|  | The system shall characterize any new device added to the system by device type. |  |  |
|  | The system shall support a multidimensional lookup to determine the current software for a device. |  |  |
|  | The system shall maintain regulatory approval of a software package by country.  [This is done based on the device table tracking the approval of the product by country] |  |  |
|  | The system shall only allow software updates for devices in countries where regulatory approval exists. |  |  |
|  | The system shall provide a means to track entitlement to software updates. |  |  |
|  | The system shall check customer entitlement to software updates privileges before allowing access to the software updates. |  |  |
|  | The dimensions of the lookup shall include:  Country  Regulatory Approval  Customer Entitlement  Device model  Device hardware  Device hardware version  Device hardware options [plural]  Device software  Device software version  Device option software [plural]  Device option software version [plural] |  |  |
|  | The system shall provide a user interface to users to view device information stored on the server. |  |  |
|  | The system shall allow the up load of software manuals for distribution by administrative staff. |  |  |
|  | The system shall allow the up load of pdf documents for distribution by administrative staff. |  |  |
|  | The system shall classify documents by software version, device type and software package status. |  |  |
|  | The system shall allow the independent download of software manuals based on role and access policy |  |  |
|  | The system shall allow the download of other documents. |  |  |
|  | The system shall classify up loaded documents by document type. |  |  |
|  | The document type enumeration shall include:  Software  Release Notes  User Guides  Service Manual  Other |  |  |
|  | The system shall support software package status. |  |  |
|  | The software package status shall include:  Testing  In Production |  |  |
|  | The system shall display available software upgrades to the user. |  |  |
|  | The software package at the agent (laptop)shall have an expiration time. |  |  |
|  | The software package expiration time shall be configurable per device type. |  |  |
|  | The system shall allow users to download software packages for entitled customers only. |  |  |
|  | The system shall pull device logs from the device before updating the software. |  |  |
|  | The system shall store the device logs on the server. |  |  |
|  | The system shall retain the logs for a minimum of seven (7) years. |  |  |
|  | The system shall provide a records archive for records over two years old. |  |  |
|  | The system shall associate the logs with the particular device serial number. |  |  |
|  | The system shall capture service type with uploaded service information. |  |  |
|  | The service type enumeration shall include:  Install  De-install  Inspection  Repair  Log Retrieval  Preventive maintenance  Upgrade |  |  |
|  | The system shall identify all logs that contain patient information. |  |  |
|  | The system shall store logs that contain patient information separately from other logs. |  |  |
|  | The system shall allow the retrieval of all logs related to a device’s usage in a clinical setting. |  |  |
|  | Users shall be able to execute software deployments to devices via VTS. |  |  |
|  | A software package shall be comprised of both encrypted and unencrypted content. |  |  |
|  | The software manifest shall always be encrypted. |  |  |
|  | The system shall confirm successful updates of device software through user interaction.  [Devices like the vent require manual testing to verify that the software was correctly deployed. This is due to the need for test hardware and system verifications.] |  |  |
|  | The system shall prevent download of the package in ‘Testing’ status by users in ‘end user’ roles. |  |  |
|  | The system shall provide a user interface to allow administrative users to upload software packages to the system. |  |  |
|  | The system shall default to setting the status of new software packages to ‘Testing’. |  |  |
|  | The system shall allow the administrator to set the software package status of a software package. |  |  |
|  | The system shall provide a user interface to allow users to subscribe and unsubscribe to categories of notifications per device type. |  |  |
|  | The system must have secure, computer generated, time stamped audit trails to independently record the date and time of operator entries and actions. |  |  |
|  | Record changes shall append to previously recorded information. |  |  |
|  | Audit trails must be retained for as long as the underlying records as required for the records. |  |  |
|  | Access to modify the system or records must be limited to authorized roles. |  |  |
|  | The laptop agent shall provide a user interface to capture service details. |  |  |
|  | The service details shall include  Date Time  CSE (user)  Service Type  Region  Customer  Device model  Device serial number  Description of service completed |  |  |
|  | The system shall calculate Mean Time Between Repair MTBR on a per device basis. |  |  |
|  | The laptop agent shall send service details to the server in XML format. |  |  |
|  | The laptop agent shall store data collected locally on the laptop. |  |  |
|  | The laptop agent shall forward all data collected when connected to the network. |  |  |
|  | The laptop agent shall use a store and forward strategy for data management. |  |  |
|  | The system shall store the service records for each device on the server. |  |  |
|  | The system shall default to reverse chronological order for the display of device service information. |  |  |
|  | The system shall provide a user Interface to review service records. |  |  |
|  | Device State Verification |  |  |
|  | The system shall verify that device information sent from the laptop agent matches Covidien records for the device.  [The comparison data comes from existing service records that will be inported.] |  |  |
|  | The system shall flag devices that have configurations that differ from Covidien records. |  |  |
|  | The system shall support reporting discrepancies.  [Differences between what is actually found in the field verses what was expected to be on the device. Potentially a failure to update the data or software piracy just going to flag so it can be reported] |  |  |
|  | System Activity Tracking |  |  |
|  | The system shall maintain an audit trail of system activity. |  |  |
|  | The system shall keep activity logs that track logins. |  |  |
|  | The system shall keep activity logs tracking software upgrades. |  |  |
|  | The system shall keep activity logs tracking user activity through the laptop agent. |  |  |
|  | The system shall enumerate user Action Type which will include:  Device inquiry  Device software upgrade  Device log upload |  |  |
|  | The system shall include the following in non-software update audit data:  Date and time  User identity  Device type  Device serial number  Action type |  |  |
|  | The system shall capture and store each software update that was performed. Information to be included in this record will include at a minimum:  Model of device updated  Serial number of device updated  Institution where update occurred  Date/time of upgrade  Name of person performing the upgrade  Name of the software package  Filename of each software image installed on the device  Configuration of device prior to the update (hardware and software versions)  Configuration of device following the update (hardware and software versions)  Logs collected from the device prior to the update  Logs collected from the device following the update  success or failure status of the update |  |  |
|  | Laptop Agent Maintenance |  |  |
|  | The system shall support laptop agent software version verification on connection. |  |  |
|  | The system shall provide a means to up load new laptop agent software. |  |  |
|  | The system shall maintain a repository of laptop agent software. |  |  |
|  | The system shall detect outdated laptop agent software. |  |  |
|  | The system shall automatically download the laptop agent software when it is discovered as outdated. |  |  |
|  | Notifications |  |  |
|  | The system shall send email. |  |  |
|  | The system shall support sending email to user accounts by Region. |  |  |
|  | The system shall support sending email to user accounts by device serial numbers. |  |  |
|  | The system shall support sending email to user accounts by device type.  [So for example it could be sent to all ForceTriad customers notifying them of new software.] |  |  |
|  | The system shall provide a means to filter discrepancy notifications. |  |  |
|  | The system shall classify notifications. |  |  |
|  | The enumeration text shall be in the subject line of the email. |  |  |
|  | The enumeration of Notification Type shall include:  Software version discrepancy  Country code violation  Attempt to update software without upgrade privileges  Failure to upgrade device  New device registration |  |  |
|  | The system shall generate an email if a software update is started but not completed within a configurable time limit. |  |  |
|  | The system shall provide a UI to display discrepancy lists. |  |  |
|  | The system shall allow users to subscribe to notifications. |  |  |
|  | The system shall allow users to unsubscribe to notifications. |  |  |
|  | Reporting |  |  |
|  | The system shall provide a report containing devices and their current software version number. Here called Report 1. |  |  |
|  | At the end of the Report 1, there shall be a section for total number of each device type at each software version, for each country. |  |  |
|  | Report 1 shall be grouped by country, device type, software version, and customer. |  |  |
|  | The system shall allow users in the Service Manager role to run preventive maintenance reports by account. Report 2. |  |  |
|  | The system shall allow users in the Service Manager role to run preventive maintenance reports by region. Report 2. |  |  |
|  | The system shall allow users in the Service Manager role to run preventive maintenance reports by device. Report 2. |  |  |
|  | The system shall allow users in the Service Manager role to run device configuration reports by account. Report 3. |  |  |
|  | The system shall allow users in the Service Manager role to run device configuration reports by region. Report 3. |  |  |
|  | The system shall allow users in the Service Manager role to run device configuration reports by device. Report 3. |  |  |
|  | The system shall allow users in the Service Manager role to run service events reports by account. Report 4. |  |  |
|  | The system shall allow users in the Service Manager role to run service events reports by region. Report 4. |  |  |
|  | The system shall allow users in the Service Manager role to run service events reports by device. Report 4. |  |  |
|  | The system shall allow users in the Service Manager role to run MTBR reports by account. Report 5. |  |  |
|  | The system shall allow users in the Service Manager role to run MTBR reports by region. Report 5. |  |  |
|  | The system shall allow users in the Service Manager role to run MTBR reports by device. Report 5. |  |  |
|  | The system shall provide users in the Service Manager role with a report listing all failed software upgrades by region, account, time period, and status. Report 6. |  |  |

## Interface Requirements

- See SRD

## Operational Requirements

|  |  |  |  |
| --- | --- | --- | --- |
|  | Operating Location |  |  |
|  | The system shall operate in Biomedical Technical Laboratories where network connectivity may be compromised.  [This is the source of the disconnected operational modes for the laptop agent and the store and forward strategy. ] |  |  |
|  | The system shall operate - across the globe where connectivity to world-wide-web is available.  [This is the other reason for a store and forward strategy, to provide robustness in uncertain environments.] |  |  |
|  | The system shall operate in Covidien office spaces across the globe. |  |  |
|  | Geography / Language |  |  |
|  | The system shall only provide software to users in countries where the software has - -regulatory approval |  |  |
|  | The system shall track dependencies between software versions and countries in which regulatory approval has been received. |  |  |
|  | The system shall provide an English user interface. |  |  |
|  | The system design shall accommodate a Bulgarian user interface. |  |  |
|  | The system design shall accommodate Chinese manuals only at launch |  |  |
|  | The system design shall accommodate a Croatian user interface. |  |  |
|  | The system design shall accommodate a Czech user interface. |  |  |
|  | The system design shall accommodate a Danish user interface. |  |  |
|  | The system design shall accommodate a Dutch user interface. |  |  |
|  | The system design shall accommodate a Finnish user interface. |  |  |
|  | The system design shall accommodate a French user interface. |  |  |
|  | The system design shall accommodate a German user interface. |  |  |
|  | The system design shall accommodate a Greek user interface. |  |  |
|  | The system design shall accommodate a Hungarian user interface. |  |  |
|  | The system design shall accommodate a Italian user interface. |  |  |
|  | The system design shall accommodate a Japanese user interface. |  |  |
|  | The system design shall accommodate a Korean - Manuals only at launch |  |  |
|  | The system design shall accommodate a Norwegian user interface. |  |  |
|  | The system design shall accommodate a Polish user interface. |  |  |
|  | The system design shall accommodate a Portuguese (Brazilian) user interface. |  |  |
|  | The system design shall accommodate a Romanian user interface. |  |  |
|  | The system design shall accommodate a Russian user interface. |  |  |
|  | The system design shall accommodate a Serbian user interface. |  |  |
|  | The system design shall accommodate a Slovakian user interface. |  |  |
|  | The system design shall accommodate a Slovene user interface. |  |  |
|  | The system design shall accommodate a Spanish (EU) user interface. |  |  |
|  | The system design shall accommodate a Swedish user interface. |  |  |
|  | The system design shall accommodate a Turkish user interface. |  |  |

## Resource Requirements [to be moved to the SRD]

-

|  |  |  |  |
| --- | --- | --- | --- |
|  | Hardware |  |  |
|  | The enterprise services must run on RedHat Enterprise. |  |  |
|  | (VM). |  |  |
|  |  |  |  |
|  | The data server shall store at least 2 TB of current log files. |  |  |
|  |  |  |  |
|  | The data server shall support data backups. |  |  |
|  | The data server shall support a minimum of two (2) years data archive. |  |  |

## Verification Requirements [ to be moved to the SRD ]

- specifies tests to be done during development, test data, test documentation to be delivered.

|  |  |  |  |
| --- | --- | --- | --- |
|  | Verification Requirements |  |  |
|  | All activities(messages) between VTS and Agent shall be logged called system logs |  |  |
|  | All activities(messages) between VTS and Ventilator should be logged, called app logs |  |  |
|  | All logs, including system logs and app logs, shall be stored locally. Agent shall transfer these logs to server when the network is available. |  |  |
|  | The system log and app log shall contain full information of the activity(message), while the BLOB part can be stored as a separated file and referenced in the log file |  |  |
|  | There shall be a MiM "man-in-the-middle" between VTS and Agent, responsible for reproducing the communication for both VTS and Agent. |  |  |
|  | MiM shall work as a bi-direction mock object where the data source is from the logs of previous communication. |  |  |
|  | MiM shall play back the logs and send the corresponding content to the other side. |  |  |
|  | When MiM is talking with Agent, it shall take the VTS system logs and BLOB files as input and provide the right response to the Agent so that it looks like the Agent is talking to the VTS. |  |  |
|  | For testing purpose, logs shall be modifiable via script language, like Lua, to simulate the different cases. |  |  |
|  | The log format shall include:   * Sender id/Module id * Session id(GUID)/Device id * User id * Action id * Date/time * Level * Message type (string, json, …) * Message |  |  |
|  | VTS shall log all communication activities with Vent. |  |  |
|  | VTS shall log all communication activities with Agent. |  |  |
|  | VTS shall interact with Agent without requiring the Ventilator. |  |  |
|  | Agent shall log all communication activities with VTS. |  |  |
|  | Agent shall interact with Server. |  |  |
|  | Server shall log all communication activities with Agent. |  |  |
|  | Server shall log all communication activities with Database. |  |  |
|  | Log server shall collect and store logs from VTS, Agent, app server and database. |  |  |
|  | Logs shall be queried and viewed via browser. |  |  |
|  | Queried logs shall be filtered, sorted and paged. |  |  |
|  | Queried logs shall be exported into CSV file or Excel file. |  |  |
|  | Logs shall be tracked by session, user and device. |  |  |
|  | Log server shall monitor the system status by analyzing the logs. |  |  |

## Documentation Requirements [to be moved to the SRD]

|  |  |  |  |
| --- | --- | --- | --- |
|  | Control system documentation, distribution, access, and use. |  |  |
|  | Project documentation shall be kept in GitHub for Netspective. |  |  |
|  | Project documentation shall be kept in SharePoint for Covidien. |  |  |
|  | Documentation shall include User Needs, System Requirements Document, Software Requirement Document, and System Architecture. |  |  |

## Quality Requirements [move to SRD]

|  |  |  |  |
| --- | --- | --- | --- |
|  | Quality Requirements |  |  |
|  | The system shall conform to the Covidien IS quality control process. |  |  |
|  | The system shall be validated to ensure accuracy, reliability, consistent intended performance, and the ability to discern invalid or altered records. |  |  |
|  | The ability to generate accurate and complete copies of records in both human readable and electronic form is required. |  |  |
|  | Records must be protected to enable accurate and ready retrieval throughout the records retention period. |  |  |
|  | Control system documentation, distribution, access, and use. [move to SRD] |  |  |
|  | Provide revision and change control procedures to maintain an audit trail that documents time-sequenced development and modification of systems documentation. |  |  |
|  | The system shall maintain the uniqueness of identification codes and passwords. |  |  |
|  | The system shall ensure that identification codes and passwords are periodically checked, recalled, or revised. |  |  |
|  | The system shall follow loss management procedures to electronically de-authorize lost or compromised passwords |  |  |
|  | The system shall use transaction safeguards to prevent unauthorized use. |  |  |
|  | The system shall detect attempts at unauthorized use. |  |  |
|  | The system shall report attempts at unauthorized use. |  |  |
|  | Documents shall be approved in Agile. |  |  |
|  | The system handoffs between executable shall use design by contract methodology. |  |  |

## Safety Requirements

|  |  |  |  |
| --- | --- | --- | --- |
|  | Safety Requirements |  |  |
|  | The system shall safe guard PHI information at all times. |  |  |
|  | The system shall encrypt PHI in transient. |  |  |
|  | The system shall encrypt PHI in storage. |  |  |
|  | The system shall encrypt PII in transient. |  |  |
|  | The system shall encrypt PII in storage. |  |  |
|  | The system shall abide by the HIPPA security instruction. |  |  |

## Reliability Requirements

|  |  |  |  |
| --- | --- | --- | --- |
|  | Reliability Requirements |  |  |
|  | The cloud host solution shall maintain 99.9% system uptime across the solution on an annual basis  [This is verified via the cloud hosting solution. And goes into the SLA.] |  |  |
|  | The data shall be backed up at all times. |  |  |
|  | The system shall have a 100% data recovery strategy.  [this informs the architecture and SRD] |  |  |
|  | Performance and Scalability Requirements |  |  |
|  | Web pages shall return to the client in 2 seconds on average with a standard deviation of less than 1 second within North America and EMEA. |  |  |
|  | The system shall upload 40 MB log files from the laptop agent to the server within 3 minutes with a standard deviation of 30 seconds. |  |  |
|  | The system shall download 10 MB software files to the laptop agent from the server within 1 minute with a standard deviation of 20 seconds. |  |  |

## Maintainability Requirements [to be moved ot the SRD]

|  |  |  |  |
| --- | --- | --- | --- |
|  | Maintainability |  |  |
|  | The system shall have 70% unit test coverage. |  |  |
|  | The system shall use pattern based designs. |  |  |
|  | The source code shall be documented. |  |  |
|  | The system shall have an E/R diagram for the database. |  |  |
|  | The system shall have a systems architecture document capturing the overall system design. |  |  |
|  | The system shall use static code analysis to catch and prevent coding errors. |  |  |

## Schedule A [ move to SRD]

Future releases shall have these requirements. They are captured here to inform design but are not part of Release 1 of the system. They are captured here to inform the system design.

The laptop agent shall be designed to running on the following operating systems:

Windows XP, Windows 7, iOS, and Embedded Linux

A single instance of an agent shall be able to communicate with and update software on several devices simultaneously.

The system shall operate correctly through the network infrastructure of any Covidien customer including firewalls and proxy servers without modifications to the customer network infrastructure.

## Schedule B

The agent shall run on the following operating systems:

Windows XP both 32/64 bit platforms

Windows 7 both 32/64 bit platforms

## Schedule C

The following are the devices that are configured to work with the device.

980 Series Ventilator