**Medtronic Emerging Markets**

**Research & Development**

**System Requirements Specification**

**Gateway Remote Service Platform**

**R0030891 Rev S**

|  |  |  |
| --- | --- | --- |
| Issue Date: 2/1/2017 | | Page 1 of 103 |
|  | | |
|  | | |
| Revision History: | | |
| Revision | SDA | Description |
| A | W0020843 | Initial Release – Requirements were reviewed by Core Team. |
| Rev B-G | N/A | Removed revision history for RevB – G for better readability of document. Refer to Rev G for revision history for Rev A – G. |
| H | W0039488 | 1. Modified Requirements: SRD- 427 2. New requirements: SRD-479, 481, 482, 483, 484, 485 |
| J | W0039488 | 1. Removed SRD-320, 450, 451, 452 as these requirements were determined to be out of scope for Phase 2.0 release by the CCB. |
| K | W0041195 | 1. Added SRD 535, 536, 537, 538 2. Updated business rule in 7.2.1.1 |
| L | RC000252 | 1. Deleted Requirements: SRD 108, 176, 219, 221, 222, 317, 319, 461 2. Added Requirements: SRD 063, 159, 214, 297, 405, 406, 496, 497, 499, 500, 501, 502, 503, 504, 506, 507, 508, 509, 510, 511, 513, 514, 515, 516, 517, 518, 519, 520, 521, 523, 528, 529, 530, 531, 533, 534, 539, 540, 541, 542, 549, 551, 552, 553, 554, 555, 556, 557, 558, 559, 560, 561, 564, 565, 566, 567, 568, 569, 570, 571, 573, 576, 577, 578, 579, 580, 581, 582, 583, 584, 585, 586, 588, 589, 590, 591, 592, 593, 594, 595, 596, 597, 598, 599, 606, 607, 608, 609, 610, 611, 615, 618, 619, 620, 621, 622, 623, 624, 625, 626, 627, 628, 629, 633, 634, 635, 636, 637, 638, 639, 640, 642, 643, 644, 645, 646, 647, 648, 649, 650, 651, 652, 653, 654, 655, 658, 659, 661, 662, 663 3. Revised Requirements: SRD 066, 129, 141, 142, 143, 153, 157, 159, 182, 205, 211, 218, 277, 278, 279, 357, 358, 393, 409, 418, 425, 466, 467, 478 |
| M | RC007382 | 1. Deleted Requirements: SRD 162, 163, 510, 518, 581, 584, 606, 652 2. Deferred Requirements: SRD 129 (Partial), 219 (Partial), 397, 398, 497, 551, 552, 553, 554, 555, 556, 557, 558, 559, 560, 561, 564, 565, 566, 567, 568, 569, 573 (Partial), 607, 608, 609, 633, 634, 635, 640, 646 (Partial), 658, 659, 3. Revised/Clarified Requirements: SRD 153, 159, 170, 214, 218, 303, 499, 508, 511, 513, 515, 523, 531, 573, 578, 592, 628, 638, 636, 637, 645, 661 4. New Requirements: SRD-664 |
| N | * RC012084 | 1. Deleted Requirement: SRD-92 2. Modified Clarified/Modified: SRD- 87, 114, 117, 192, 374, 424, 441 |
| P | * RC015387 | * 1. Deleted Requirement: SRD-629   2. “obsolete”Modified Requirement: SRD-218   3. Added Requirement: SRD-667 |
| Q | * RC029002 | * 1. Added Requirements :SRD- 668, 669   2. Updated Requirements: SRD-418, 425 |
| R | * RC049313 | * 1. Added Requirements: SRD-900, 901, 902, 903, 904   2. Updated Requirements: SRD 280, 281, 413, 528, 623 |
| S | * RC064500 | Added Requirements : SRD- 544, 552, 553, 554, 555, 556, 557, 558, 559, 560, 561, 564, 565, 566, 634, 635, 658, 660, 669, 670, 671, 672, 673, 674, 676, 677, 678, 679, 681, 682, 683, 685, 687, 690, 692, 702, 704, 706, 707, 708, 709, 710, 713, 714, 715, 716, 721, 722, 724, 726, 728, 731, 733, 736, 737, 738, 739, 740, 741, 744, 745, 746, 747, 748, 749, 753, 754, 756, 763, 764, 767, 769, 770, 771, 774, 792, 795, 798, 800, 802, 803, 804, 805, 806, 807, 808, 809, 810, 811, 812, 813, 814, 815, 817, 818, 819, 820, 821, 987, 988, 989, 990, 991, 992, 993, 994, 995, 996, 997, 998, 999, 1000, 1001, 1002, 1003, 1004, 1005, 1006, 1007, 1008, 1009, 1010, 1011, 1012, 1013, 1014, 1015, 1016, 1017, 1019, 1020, 1021, 1022, 1023, 1026, 1027, 1028, 1029, 1030, 1031, 1032, 1033, 1034, 1035, 1036, 1037, 1038, 9973, 9974, 9975, 9976, 9977, 9978, 9979, 1024, 1025  Updated Requirements: SRD- 49, 55, 62, 109, 129, 130, 133, 138, 161, 164, 196, 198, 214, 218, 297, 298, 330, 339, 342, 342, 344, 344, 345, 377, 382, 404, 410, 418, 424, 447, 449, 449, 456, 478, 478, 478, 496, 499, 502, 503, 507, 508, 509, 513, 515, 516, 517, 530, 571, 590, 598, 610, 611, 623, 627, 628, 636, 637, 642, 644  Deleted Requirements: SRD-427,428,429, 430, 502, 504, 506, 511, 519  Updated business rules section. |
| Author: Refer to Agile for approvals | | |
| Author: Refer to Agile for approvals | | |
| Ashwini Pandey / MITG R&D | | |
| Mirror Wang/ InsigmaUS [Manual Approval] | | |
|  | | |
| **Approvals:** Refer to Agile for approvals | | |
| Maureen Richard / HI&M, R&D | | |
| Paul Ourada / HI&M, R&D | | |
| Cliff Schorr / MITG, Quality | | |
| George Becker/ SI Service [Inform] | | |
| William Atkinson / HI&M , R&D | | |
| Scott Licursi/ Corporate IS[Inform] | | |
| Nidhi Khanna / SI R&D [Inform] | | |

**Table of Contents**

[1.1 Purpose 5](#_Toc472687169)

[1.2 Scope 5](#_Toc472687170)

[1.3 Structure of Document 5](#_Toc472687171)

[1.4 Definitions, Acronyms, and Abbreviations 5](#_Toc472687172)

[1.5 References 7](#_Toc472687173)

[2 Overall Description 7](#_Toc472687174)

[2.1 Perspective 7](#_Toc472687175)

[2.2 Related Projects 8](#_Toc472687176)

[2.3 System Environment 8](#_Toc472687177)

[3 Requirements 9](#_Toc472687178)

[3.1 Functional Requirements 9](#_Toc472687179)

[3.1.1 User Login 9](#_Toc472687180)

[3.1.2 User Self Registration 13](#_Toc472687181)

[3.1.3 Users 15](#_Toc472687182)

[3.1.4 Roles and Access Policies 17](#_Toc472687183)

[3.1.5 User Training Related Requirements 21](#_Toc472687184)

[3.1.6 Security Requirements 21](#_Toc472687185)

[3.1.7 Gateway Agent General Requirements 24](#_Toc472687186)

[3.1.8 Data Upload/Download Requirement 24](#_Toc472687187)

[3.1.9 Gateway Agent-Cache Auto Download Requirements 26](#_Toc472687188)

[3.1.10 Proxy Log-in Requirements 27](#_Toc472687189)

[3.1.11 Gateway Agent-Business Rules Requirements 27](#_Toc472687190)

[3.1.12 Device Identification 29](#_Toc472687191)

[3.1.13 Device Warranty Management Requirements 31](#_Toc472687192)

[3.1.14 Device Prep Step Requirements (Gateway 1930) 31](#_Toc472687193)

[3.1.15 Device Software Upgrade Related Requirements 32](#_Toc472687194)

[3.1.16 Device Log Handling 37](#_Toc472687195)

[3.1.17 Document Handling 38](#_Toc472687196)

[3.1.18 Regulatory and Trade Embargo Requirements 41](#_Toc472687197)

[3.1.19 Device Configuration Management 42](#_Toc472687198)

[3.1.20 Orion Specific Configuration Management Requirements 43](#_Toc472687199)

[3.1.21 Named Configuration 43](#_Toc472687200)

[3.1.22 Serial Number Reprogram 50](#_Toc472687201)

[3.1.23 Feature Licensing 50](#_Toc472687202)

[3.1.24 System Activity Tracking 58](#_Toc472687203)

[3.1.25 Gateway Agent Maintenance 60](#_Toc472687204)

[3.1.26 Client Application Software Related Requirements 61](#_Toc472687205)

[3.1.27 Alerts 61](#_Toc472687206)

[3.1.28 Reporting 65](#_Toc472687207)

[3.1.29 Part 11 Compliance and Related Requirements 79](#_Toc472687208)

[3.1.30 Gateway Agent Installer Requirements 81](#_Toc472687209)

[3.1.31 Recommended Requirements for Client Application Installer 82](#_Toc472687210)

[3.1.32 Common Client related Requirements 82](#_Toc472687211)

[3.1.33 Trade Embargo 84](#_Toc472687212)

[3.1.34 Device Hardware 84](#_Toc472687213)

[**3.1.35** **Gateway Log -Viewer Requirements** 86](#_Toc472687214)

[3.1.36 UI Validation 86](#_Toc472687215)

[3.2 Operational Requirements 87](#_Toc472687216)

[3.2.1 Operating Location 87](#_Toc472687217)

[3.2.2 Geography / Language 87](#_Toc472687218)

[3.3 Reliability Requirements 87](#_Toc472687219)

[3.3.1 Reliability Requirements 88](#_Toc472687220)

[3.3.2 Performance and Scalability Benchmarks (Gateway 1601) 88](#_Toc472687221)

[4 Schedule B 88](#_Toc472687222)

[5 Schedule C 89](#_Toc472687223)

[6 Schedule D 89](#_Toc472687224)

[7 Schedule E 89](#_Toc472687225)

[8 Business Rules 90](#_Toc472687226)

[8.1 Agent Rules 90](#_Toc472687227)

[8.1.1 Server Status Check 90](#_Toc472687228)

[8.1.2 Password Reset 90](#_Toc472687229)

[8.2 Common Rules 90](#_Toc472687230)

[8.2.1 Device Operations 90](#_Toc472687231)

[8.2.2 Configuration Validation 93](#_Toc472687232)

[8.3 Server Rules 94](#_Toc472687233)

[8.3.1 User Registration 94](#_Toc472687234)

[8.3.2 Device Customer Name and Country 95](#_Toc472687235)

[8.3.3 Named Configuration 95](#_Toc472687236)

[9 Appendix 95](#_Toc472687237)

[9.1 Future/Deferred Requirements 95](#_Toc472687238)

[9.2 Roles and Entitlements Matrix 100](#_Toc472687239)

[9.3 Access rights and Operation 101](#_Toc472687240)

## Purpose

*ID* : SRD-282

This System Requirements Specification (SRS) contains the set of system requirements for the Medtronic Gateway. This document provides sufficient guidance to the development team to allow them to develop the software. It also provides requirements against which the test team can develop test protocols. . While hardware will be specified, the focus is on software development.

## Scope

*ID* : SRD-283

The requirements contained within this document are for the Gateway Agent and the server software only. The Client Application requirements are contained in another SRS provided by the GBU for the specific product which uses this system.

## Structure of Document

*ID* : SRD-289

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

## Definitions, Acronyms, and Abbreviations

*ID* : SRD-284 :

**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. Note: 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, post-conditions 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.

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

**Gateway Agent** - The application software that manages communication between the server and the Client Application. Currently, the gateway agent is designed to run on Windows PC running specific OS detailed in Schedule B.

**Client Application** - The application software that manages communication between the Gateway Agent and the edge medical device.

**Business Rules File** – A set of rules external to the software which control the behavior of the system. Such a rules file may be used either by the Agent or the Client Application.

**Disconnected Mode**: Disconnected Mode is the update of software on the edge device when the intermediary device (for example, a laptop) is not connected to the server

**Edge Device:** The medical device that interacts with the Gateway server through the intermediaries-Client Application and Gateway Agent.

**Class of Trade (CoT)**: A set of products that are similar, such as ventilation (PB840, PB 980, etc.) is considered a Class of Trade. Other examples are Compression, Sealing and Ablation, etc.

**User Personal Data:**  User Personal Data consists of Passwords and the notifications to which the user subscribes.

**Entitled Customer**: Entitled customer refers to the fact that the customer is licensed to use a device feature such as particular software.

**Laptop/PC/Desktop/Computer:** The device that hosts the Gateway Agent and Client Application. The names laptop/PC/Desktop//Computer mean the same for the purpose of this document.

**Access Policy:** A group of access permissions assigned to a role

**Device Warranty**: Initial warranty that comes with the new device.

**Service Contract**: Service contract extends the device warranty for a specific term.

**Feature:** Feature is an optional extension to the basic functionality which is separately licensable.

**Feature Catalog:** Feature catalog contains the set of features available for a particular device type and version.

**Alerts:**  Alerts deliver system event information to the end user.

Alerts are of three types-

Technical Alerts- these involve non-business errors in the technology of the system (such as “server is down”) and require a follow up action from the technical staff.

Business Alerts- these are pre-defined error handlers in workflow of business use cases (such as “upgrade failed”) and require follow-up action from the applicable business administrators.

Informational Alerts- these for informational purposes only (such as “device changed country”) and don’t require any further action from the recipient

**Configuration:** A configuration is the grouping of configuration items of a particular set of HW/SW/FW and given a name.

## References

*ID* : SRD-292

GS10003599 Medtronic Corporate Part 11 Compliance Procedure

# Overall Description

## Perspective

*ID* : SRD-285 :

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

It will be used in the field by both certified client personal like hospital-based Biomedical-Technicians and by the Medtronic Customer Support Engineer (CSE). It will provide functionality for software updates to the edge device; manage the catalog of software; provide a mechanism to acquire the edge device 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 Medtronic Service Managers and Sales staff it will provide service management reports. For quality and customer complaint analyst, it will provide a device history record for the software upgrades.

It will be important to isolate the field service technician’s access to the system based on the division they support.

## Related Projects

*ID* : SRD-286 :

|  |
| --- |
| Project |
| Viking -developing the  PB980 Series Ventilator |
| PB980 ESS update |
| Enterprise One – complete redeployment of existing back end infrastructure |
| Signia Stapler Integration (VLEX 3.2) |
| SCD700 Robin Project |
| VLLS10 Integration with VLEX 3.0 |
| VLFT10 Integration (VLEX 3.1) |
| Emprint Procedure Planning Application |

## System Environment

*ID* : SRD-287 :

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 Medtronic 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 intermediary devices including laptops/desktops running, windows 7, windows 8 and windows 10~~iOS, and handheld devices running Android O/S.~~

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

# Requirements

## Functional Requirements

### User Login

*ID* : SRD-37

The systems web interface shall start with a login screen for both the customer and internal employees.

Note: This is the web interface to the backend server.

*ID* : SRD-38

The system shall support user authentication via the web interface.

*ID* : SRD-39

The system shall prompt with user-name and password credentials.

*ID* : SRD-668

The system shall use the following password construction rule:

a. Contain at least 8 characters, no maximum

b. Must use at least one upper case letter

c. Must use at least one lower case letter

d. Must use at least one numerical character

e. Must not contain the special characters & < > / ' "

f. Must contain at least 1 special character (e.g. $)

*ID* : SRD-46

System shall support username and password authentication.

*ID* : SRD-47

The system shall support user authorization.

*ID* : SRD-48

The system shall support role based authorization.

*ID* : SRD-49

The system shall support the following roles:

Application Support

Field Service Technician

Service Center Technician

Sales Rep

R & D

QA

Service manager

Biomed

User Administrator

Class of Trade Administrator

Marketing

Quality & Reliability  
Development Eng/Manager  
Technical Support  
Technical Service Engineer  
Release Validation Manager  
Manufacturing  
Distributor

*ID* : SRD-478

By default, the system shall support the following role-based user permissions:

Devices: Yes/No – entitled to view devices

Reports: Yes/No – entitled to view reports

User Management: View/Edit/No – entitled to access the user management functionality

HW Catalog: View/Edit/No – entitled to define hardware items

SW Catalog: View/Edit/No – entitled to define, upload and manage software items

Document Catalog: View/Edit/No – entitled to upload and manage documents

Configuration Management: View/Edit/No – entitled to create and manage named hardware/software/system configurations

Customer and Facility Management: View/No- entitled to view or edit customer account name/number, facility name/address and the association with customer and facilities (HIGH

Feature Catalog: View/ Edit/ No - entitled to define, and edit features in the Feature Catalog, and to manage feature entitlements.  
~~Trade Embargo: View/ Edit/ No - entitled to add/ modify/ delete trade embargo~~  
Alert: View/ Edit / No - entitled to view alert and manage alert subscriptions

Entitle to install SW: Yes/No – entitle to install Software

Install Latest Version SW Only: Yes/No – permission to install latest Version SW Only

Access Limited Release SW: Yes/No – Access to Limited Release status SW

Entitle to install Feature License: Yes/No – Entitle to install Feature License

Access Limited Release Feature License: Yes/No – Access to Limited Release status Feature License

*ID* : SRD-50

The system shall move to the ‘home’ screen if the user’s authentication and authorization test pass.

*ID* : SRD-51

The system shall return to the login screen if the user’s authentication and authorization tests fail.

*ID* : SRD-52

The system shall respond with a failed user login message.

Note: 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

*ID* : SRD-53

In the case of a failed login attempt, the system shall provide no more information than a message prompting the user to correctly enter his user name and password.

ID : SRD-298

Passwords shall be revised on a regular cycle as 90 days by default. After password expires, the system shall hint user to change password online.

Note: Required for Part 11 Section 7.1.8.7

See Also: Part 11 Compliance and Related Requirements

*ID* : SRD-55

After three failed log-in attempts, the system shall notify the user to contact the help desk for a password reset.

Note: Reset password request link should be provided on login page.

*ID* : SRD-56

The system shall provide help desk contact information on the login page.

*ID* : SRD-58

The system shall log failed login attempts including time, username, and hostname/IP Address.

*ID* : SRD-446

The gateway agent shall provide a means for the Client Application to request the “Forgot Password” function which resets the user’s password**.** The function is available ~~only~~ in connected mode.

NOTE: See Section 8.1.2, Password Reset.

*ID* : SRD-469

The system shall allow a user to request new password while in disconnected mode and the request will be granted when the agent connects to the server at next opportunity.

NOTE: See Section 8.1.2, Password Reset.

*ID* : SRD-447

The gateway agent shall enable changing passwords from Client Application, only if connected to Gateway Server

NOTE: See Section 8.1.2, Password Reset.

NOTE: User can enter Client Application with old password when the password is changed through Server WebUI.

NOTE: Change password is not allowed in disconnected mode.

~~NOTE: this is not applicable for Common Client Case~~

*ID* : SRD-462

The system shall send notification email with link to change password upon completion of forgot password request.

*ID* : SRD-472

Gateway agent shall encrypt user credentials to allow disconnected log-in.

ID: SRD-670

The system shall allow user to log out.

ID: SRD-671

The system shall allow system admin user to add facility information to the system database with the following information:

• Facility Name

• Facility Address

ID: SRD-672

The system shall allow system admin user to associate multiple facilities to a customer name.

Note:, This will allow customer to associate with more than one facility when the customer may own or have business with more than one facilities.

ID: SRD-673

The system shall allow user with adequate privileges to view the complete list of customers and their associated facilities.

ID: SRD-674

The system shall allow system admin user to add new customer to the system database with below information:

• Customer Account Number

• Customer Name

• Customer Address

ID:SRD-800

After 3 failed login attempts, the user account will be locked.

SRD-803:

A user’s account shall be unlocked under one of the following conditions:

1. System Administrator unlocks the account after verification.
2. The user waits a pre-configured lockout period (in minute)
3. The user resets password.

*ID* : SRD-802

The system shall accept usernames that consist of more than one period (.).

Note: This is to accommodate usernames that have more than one period in the name such as firstname.middlename1.middlename2.lastname@email.com

### User Self Registration

*ID* : SRD-588 (CRITICAL)

The System shall provide a means for the prospective new user (self-registrant) to request log in credentials.

*ID* : SRD-589 (CRITICAL)

The system through Gateway Agent shall provide to the Client a link to the server webpage for new user self-registration.

*ID* : SRD-904

The System shall allow grouping by device type or CoT on self-registration page.

Note: Although Signia Stapling device is part of Stapling CoT, it should be listed on same page as Vessel Sealing devices.

*~~ID~~* ~~: SRD-590 (CRITICAL)~~

~~Self-registration will have only 3 different statuses (pending, completed, activate).  
Pending – User submitted new user registration form successfully, and system will notify approving manager via email about the request.  
Completed – Approving manager received the request and approved or denied  
Activate – User successfully set the password and can use GDMP  
System shall provide feedback to the registrant regarding status of the self-registration~~

*ID* : SRD-590 (CRITICAL)

Self-registration shall have 3 valid status: Pending, Completed, Active.  
Pending – User submitted new user registration form successfully, and system will notify approving manager via email about the request.  
Completed – Approving manager received the request and approved or denied  
Active – User successfully set the password and can use GDMP

ID-SRD-804

System shall provide feedback to the registrant regarding status of the self-registration

*ID* : SRD-591 (CRITICAL)

System shall automatically process the self-registration request.

*ID* : SRD-593 (CRITICAL)

System shall set registration request state to pending upon successful completion of new user registration form.

*ID* : SRD-594 (CRITICAL)

System shall use email notification to obtain authorization for pending registration from approving manager.

*ID* : SRD-595 (CRITICAL)

System shall set registration state to approved state upon receipt of authorization from approving manager.

*ID* : SRD-596 (CRITICAL)

System shall send an email to registrant with id and a link to a Gateway page where the user sets their password.

*ID* : SRD-597 (CRITICAL)

System shall send an email to the registrant, if the registration has been in process for 48 hours or greater.

*ID* : SRD-598 (CRITICAL)

System shall send an email to Approving Manager/Proxy ~~the Gateway Support~~, if the registration has been in process for 48 hours or greater.

ID: SRD-798

The system shall allow approving proxy to approve non-Metronic user registration and approving manager to approve Medtronic user registration.

ID: SRD-678

The system shall allow GDMP admin to set approving proxy per device type as provided by a GBU representative so as that the non-Medtronic user registration requests can be routed for approval to this approving proxy for the particular device type. If a new user selects more than one device type on their self-registration request, then use the last selected one as approving proxy.

ID: SRD-679

The system shall allow CoT Admin to check the status of registration approval progress of his CoT’s registration forms.

ID: SRD-681

The system shall allow Non-Medtronic registrant that knows his customer name to identify customer name in the registration form to auto-fill registration fields.

ID: SRD-682

The system shall provide directions so that a non- Medtronic registrant that does not know his ~~company~~ customer information can obtain the required customer name for getting registered.

ID: SRD-676

The system shall allow prospective Medtronic GDMP user to identify the person that will approve his userid request.

Note: This is so that the user can receive his account credentials quickly and efficiently.

ID: SRD-677

The system shall allow Medtronic approving manager or proxy to authorize who will have access to the GDMP system for particular CoT.

ID: SRD-1010

When a user requests self-registration for PB980, the system should allow the user to select trainer. And the trainer list should not contain gw\_admin and etl\_admin.

ID: SRD-1011

The system should maintain a list of default trainer ID per device type. And system admin can configure whether they want to use the trainer ID as the approving Manager/proxy. There should have an entry in WebUI for this configuration. If “Use as Approving Mgr/Use As Approving Proxy” is set as “Y”, then the approving proxy set in WebUI will not take effect.

ID: SRD-1012

The system should support self-registration for different device types: Valleylab LS10, Valleylab FT10, SCD700, PB980 and Emprint.

### Users

*ID*: SRD-59

The system shall allow the creation of new users.

*ID* : SRD-463The User Administrator role shall be able to add new users to the system.

*ID* : SRD-464

The User Administrator role shall be able to modify user accounts in the system.

*ID* : SRD-465

The User Administrator role shall be able to delete user accounts in the system.

*ID* : SRD-646 (CRITICAL)

The system shall support the following user types:

a. Medtronic Users

b. Non- Medtronic users who are associated with a single Medtronic customer.

c. Non- Medtronic users who are associated with multiple Medtronic customers.~~(DEFERRED)~~

*ID* : SRD-62

User Data shall include:

First Name

Last Name

Role/Title

Login Name/Email

Password

Is Medtronic Employee

Company Name

Country

Language

*ID* : SRD-63 (HIGH)

Customer data shall include:

Customer Account Number

Customer Name

Customer Address

*ID* : SRD-64

The system shall identify the customer hospital, distributor or third-party a user works for if they are not a Medtronic employee.

*ID* : SRD-66

The system shall allow the editing of user permissions based on role.

Note: 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.

*ID* : SRD-67

The system shall allow the disabling of user permissions based on role.

*ID* : SRD-68

The system shall allow the assignment of user permissions to a role.

*ID* : SRD-374

When adding new devices, the system shall associate devices to the user’s customer account if the user is associated with a customer account.

Note: Refer to business rule in 8.2.2

*ID* : SRD-410

The system shall join multiple concurrent log-ins by a single user from different machines into a single session.

).

*ID* : SRD-529 (Gateway 1403) (CRITICAL)

The Agent shall support different Clients connecting to it sequentially.

Note: For example, the agent will allow connection from SCDU, followed by ESS, etc.

*ID* : SRD-318

The system shall allow deactivating/re-activating a user.

### Roles and Access Policies

*ID* : SRD-70

The system shall allow the creation of new roles.

*ID* : SRD-9997

The system shall provide separate role schemes for MDT and non-MDT personnel.

NOTE: non-MDT roles include:

Biomed

Distributor

ThirdPartyService

*ID* : SRD-9996

The system shall provide only non-MDT roles for non-MDT personnel.

NOTE: For instance, the Self Registration Screen

*ID* : SRD-9995

The system shall provide only MDT roles for MDT personnel.

*ID* : SRD-9994

All UI screens which list both MDT and non-MDT roles shall keep them segregated in their respective group, and shall label the groups accordingly.

*ID* : SRD-9993

The system shall provide a Limited Access role, which shall have a non-modifiable default device access permission of Default Dock Device.

*ID* : SRD-71

The system shall assign the right to create new roles through the access policy.

*ID* : SRD-72

Role Data shall include

Role Name

Description

*ID* : SRD-73

The system shall allow the editing of roles based on access policy.

*ID* : SRD-74

The system shall allow the deletion of roles based on access policy.

*ID* : SRD-75

The system shall allow the assignment of access policies to roles.

*ID* : SRD-76

They system shall allow the review of users assigned to a role.

*ID* : SRD-77

They system shall allow the review of access policies assigned to a role.

*ID* : SRD-78

The system shall define device types. (PB 980, ForceTriad, etc.)

*ID* : SRD-79

The system shall provide the ability to customize role regimes by Class of Trade.

*ID* : SRD-466

The system shall require that a user’s profile contain a training record for each applicable device type before allowing the user to update software on that device type.

NOTE: See section 8.2.1.2User Device Update Permission and section 8.2.1.6, Update Device Software Allowed

*ID* : SRD-81

All system users, agents, or tasks shall run under an access policy.

*ID* : SRD-82

The system shall allow the creation of access policies.

*ID* : SRD-83

The system shall allow the editing of access policies.

*ID* : SRD-84

The system shall allow the deleting of access policies.

*ID* : SRD-85

The system shall log the use of access rights granted by the policies, except the viewing activity.

*ID* : SRD-86

The system shall use access policies to manage access to administration activities.

*ID* : SRD-9999

The system shall use access policies to manage access to devices.

*ID* : SRD-87

The system shall use access policies to control access to user workflow activities.

Note: Here user workflows are the screens and menu items that a role has access to through the web interface. They are created in development. If your role does not have access the menu item will be disabled.

*ID* : SRD-88

The access policies shall govern create rights across entities.

*ID* : SRD-89

The access policies shall govern read rights across entities.

*ID* : SRD-90

The access policies shall govern update rights across entities.

*ID* : SRD-91

The access policies shall govern delete rights across entities.

*ID* : SRD-685

The default permission of Feature Catalog for CoT Admin shall be "View & Edit" in Web UI.

Note: see GW-2076

*ID* : SRD-342

The system shall support the following types of device access privileges:

Entitle to install SW

Install Latest Version SW Only

Access Limited Release SW

Entitle to install Feature License

Access Limited Release Feature License

User’s device access privilege can be the combination of above permission.

NOTE: See Section 8.2.1.8, Device Update Software Selection, and Section 8.2.1.2, User Device Update Permission.

*ID* : SRD-9998

The device access permission which is assigned to a role is default in nature, and the system shall provide a means for a user with the appropriate permissions to modify an individual user’s device access rights.

*ID* : SRD-343

Device access permission will be associated with a user and role profiles.

*ID* : SRD-344

The system shall include in the UI a permission indicating “Entitle to Install SW”, “Install Latest Version SW Only”, “Access Limited Release SW”, “Entitle to install Feature License”, “Access Limited Release Feature License” device access rights in the user's system profile.

NOTE: See Section 8.2.1.2, User Device Update Permission. Section 8.2.1.7, Software Component Matching , and Section 8.2.1.8, Device Update Software Selection

*ID* : SRD-345

The system shall not download software nor feature licenses, which are associated with a particular device type, to users who do not have both a device training record for that device type and device access permission greater than Entitle to Install SW for that device type.

*ID* : SRD-445

The gateway agent shall provide to Client Application a user’s role (system access rights) in disconnected as well as connected mode, provided the user has connected at least once in connected mode from the same laptop

*ID:SRD-687*

The system shall allow System to be able to manage a file extension white list ~~per CoT.~~

Note: This file extension white list refers to files that are allowed to be uploaded including software package, document and business rule.

*ID : SRD-615 (Gateway 1377) (CRITICAL)*

The system shall support the following permissions to control a non- Medtronic user’s rights to view device information on the WebUI:

a. User can view all devices for any customer with whom he is associated. If user is associated with more than one customer, he must first select customer account name on the WebUI before he can view devices for that customer. (

b. User can view devices for any device he has serviced, regardless of the customer

c. User cannot access the “Reports’ section of the WebUI. (OBSOLETED)

### User Training Related Requirements

*ID* : SRD-338

The system shall include a mechanism to identify a user that can train others.

*ID* : SRD-339

The system shall maintain a training record for all users including:

Trainer Name

Date of Training

Trainee Name

Device Type

*ID* : SRD-340

The system shall provide a means to view a user's training record.

*ID* : SRD-341

The system shall provide a means to view a list of training records for a particular device type.

*ID* : SRD-683

The system shall provide a means for a user with the appropriate permissions to obsolete a user's training record.

Note: This is desirable in order to be able to clean up duplicate training records, which have found their way into the systems.see GW-2918

### Security Requirements

*ID* : SRD-97

The system shall operate through a secure port.

*ID* : SRD-115

The system shall provide secure communication channels for sending data.

*ID* : SRD-116

The system shall provide secure communication channels for receiving data.

*ID* : SRD-105

The system shall encrypt the software manifest.

*ID* : SRD-416

The gateway agent shall set a timer on each encrypted file in the cache and delete that file after the timer expires.

*ID* : SRD-417

The gateway agent shall restart the timer every time the encrypted file in the cache is accessed.

*ID* : SRD-106

The encrypted components of the package shall be decrypted prior to transferring it to Client Application.

*ID* : SRD-419

The gateway agent shall delete the decrypted software package from laptop immediately on receipt of installation response message from the client application.

*ID* : SRD-420

The gateway agent shall delete decrypted software package from laptop within 2 hours if no installation response message is received from client application and the software package is not accessed.

*ID* : SRD-421

The gateway agent shall delete all the decrypted software package from laptop upon user log-out.

*ID* : SRD-109

The gateway agent shall completely delete a package after pre-configured expiration time has elapsed.

*ID* : SRD-653 (Gateway-2003)

All Gateway DMP servers shall participate in the Corporate IS remote security monitoring infrastructure.

*ID* : SRD-792

Software packages should be stream encrypted when they land on the server.

Note：refer to GW-3409

*ID* : SRD-1013

All system certificates/tokens used in the system shall be revocable and re-issuable.

*ID* : SRD-1014

All system components using a certificate/token shall be capable of revoking and re-issuing the certificate/token.

*ID* : SRD-1015

All system components which serve or are clients which need to obtain an authentication certificate/token, shall share a temporary encryption key which is used until the normal runtime certificate/token is granted (server) or obtained (client).

*ID* : SRD-1016

All system components which share a temporary encryption key shall be capable of keeping the shared key private during and after the installation of the system component.

*ID* : SRD-1017

All system components which are clients that use a temporary shared encryption key shall cause the shared encryption key to be unusable upon obtaining the normal runtime certificate/token.

*ID* : SRD-1019

All system components which use mutual authentication certificates/tokens in the development environment shall not use the same certificates/tokens in the production environment.

*ID* : SRD-1020

Machine login credentials, such as Agent login and Limited Access User login, shall be kept private in the system where they are used.

*ID* : SRD-1021

Mutual authentication certificates/tokens shall be kept private in the system component where they are installed and used.

*ID* : SRD-1022

Mutual authentication certificates/tokens installed in the production environment shall not be installed in the development environment and vice versa.

*ID* : SRD-1023

Below system components shall mutually authenticate themselves to each other.

WebUIApp Server

AgentApp Server

*ID* : SRD-1024

The current clients will not being impacted with the existing authentication and communication approach with Agent

### Gateway Agent General Requirements

*ID* : SRD-93

The system shall provide a Gateway agent.

*ID* : SRD-442

The gateway agent shall respond to the Client Application request for server connection status.

Note: See Section 8.1.1, Server Status Check.

*ID* : SRD-94

The gateway agent shall run on the operating systems defined in schedule B.

Note: We are using schedule B to allow the documented list of operating systems to grow over time.

*ID* : SRD-98

The gateway agent shall provide information to client application through message exchange.

*ID* : SRD-444

The gateway agent shall disconnect from Server when requested by Client Application.

*ID* : SRD-663

The gateway agent shall respond to a request from Client Application with network time (GMT) in connected mode.

### Data Upload/Download Requirement

*ID* : SRD-474

For all files presented to the Agent for delivery to the Server, the system shall deliver a bit accurate copy of such files to the Server and verify that it has done so.

*ID* : SRD-477

For all files uploaded to the Server with the intention to be delivered to the Agent or Client, the system shall deliver a bit accurate copy of such files to the respective Agent or Client, and verify that it has done so.

*ID* : SRD-399

During download of files from the server to the gateway agent, the gateway agent shall provide notification to client application of the time remaining until download is complete.

*ID* : SRD-400

When uploading files from the gateway agent to the server, the gateway agent shall provide notification to the client application of the time remaining until upload is complete.

*ID* : SRD-114

The system shall allow files to be transferred to the Windows personal computer from the server with or without any accompanying software update.

Note: Files in this case refer to documents, software packages. The business rules files are considered a type of software package.

*ID* : SRD-117

The system shall automatically compress binary files while transmitting between the agent and the server in either direction .

Note 1: Currently, device log files, SW packages and documents are sent as binary file.

Note 2: The messages between agent and server are sent as text data and these don't get compressed during transmission.

*ID* : SRD-118

The gateway agent shall cache its data during a download.

*ID* : SRD-119

The gateway agent shall cache its data during upload.

*ID* : SRD-121

The gateway agent shall be able to resume download to its download cache if communication is interrupted.

*ID* : SRD-124

The gateway agent shall provide status notification of errors to the client application.

*ID* : SRD-125

The gateway agent shall provide notifications to client application identifying problems and solutions as they occur in the process.

*ID* : SRD-191

The gateway agent shall store data collected locally on the laptop.

*ID* : SRD-192

The gateway agent shall upload cached data, such as log files and messages, to the server when a connection is made between the agent and the server.

*ID* : SRD-291

The gateway agent shall use a store and forward strategy for data management.

*ID* : SRD-362

The gateway agent shall send "time period remaining before cached software is removed" to the Client application in the Agent status message.

*ID* : SRD-363

The gateway agent shall send "data ready to send" to the Client application in the agent status message if there is cached data to upload.

*ID* : SRD-774

The system shall support all existing approach to client applications for downloading software packages and configurations.

*ID* : SRD-769

DMA shall support uploading of log files to DMP regardless of the size of the log file

Note: If the log file is larger than 10 MB , the files will be uploaded in chunks.

*ID* : SRD-756

The system shall support upload of the device log file to GDMP automatically from local cache whenever the connection between GDMP Agent and GDMP server becomes available.

### Gateway Agent-Cache Auto Download Requirements

*ID* : SRD-424

When a user logs in, the agent shall download all missing files from the server for the user’s Class of Trade where the user has download permission.

Note 1 : This requirement applies to devices that do not send Prep Step message.

Note 2 : For devices that send Prep-Step message, the system allows a user to select which device types to download prior to agent downloading the files.

~~Note 3: Archived and dirty expired files should not be downloaded.~~

Note 3: Archived ~~and expired~~ files are not downloaded.

Refer to 3.1.15 Device Prep Step Requirements.

*ID* : SRD-667

The Agent shall prioritize the downloading of Client data ahead of other download items such as packages or documents.

*ID* : SRD-418 (Gateway 1004)

The file cache deletion timeout period shall be 90 days by default.

*ID* : SRD-425(Gateway 1004)

The file cache deletion timeout period for SCD700 shall be 3700 days.

*ID* : SRD-669

The Agent shall clear the password cache at a configurable period time which defaults to 90 days.

ID : SRD-497(Gateway 1004) (HIGH)

The FILE cache deletion timeout period shall be configurable by device type.

Note: This requirement is distinct from SRD-669 which details agent PASSWORD cache behavior.

### Proxy Log-in Requirements

*ID* : SRD- 471

The Gateway Agent shall support communication with the Gateway server through a proxy.

Note: This is requirement for the Supporting systems of Gateway.

*ID* : SRD- 479

The Agent shall support proxy log-in credentials from multiple users.

NOTE: Use case where multiple users share the same computer and a proxy login is required.

Note: The proxy log-in expiry is determined by the user site requirements

*ID* : SRD- 481

The Agent shall cache all proxy log-in credentials in a secure method.

*ID* : SRD- 482

The Agent shall be able to select cached proxy credentials which match the logged in user.

*ID* : SRD- 483

The Agent shall use the last logged in user's proxy credentials when all users have logged out of the computer.

*ID* : SRD- 484

The Agent shall be able to designate one proxy login credential as a machine login.

*ID* : SRD- 485

If a proxy login credential has been designated as a machine login, the Agent shall only use that credential to login to the proxy server.

### Gateway Agent-Business Rules Requirements

*ID* : SRD-394

The system shall provide for Gateway Agent Business Rules.

*ID* : SRD-395

The system shall provide for Client Application Business Rules.

*ID* : SRD-364

The system shall have a means to identify “Business Rules” files for use by gateway agent during interactions with gateway agent.

*ID* : SRD-365

The system shall provide a means to name “Business Rules” files.

*ID* :

*ID* : SRD-367

The system shall version the Business Rules file(s).

*ID* : SRD-368

The system shall support a message requesting the Business Rule file(s) for operation.

*ID* : SRD-369

The message shall contain the version of all existing Business Rule files on the agent.

*ID*

*ID* :

*ID* : SRD-448

The system shall provide a means for a user to upload a Business Rules file to the server, and have the server download that file to the client application.

NOTE: This Business Rules file could be used for mapping regions to countries, or listing ISO country codes, or defining serial number rules, etc.

*ID* : SRD-449 (Gateway-1150)

The system shall use device-type specific business logic for applying the combination of software name, Comparison Order , and associated hardware to present software to the client for installation.

NOTE: The business logic should be based on the following behaviors:

1. For PB980 and SCD700, in order to match the running configuration of a docked device, the software item name should not change from one software version to another, only the part number and/or the revision number is allowed to change.

2. For PB980, every time the software revision is rolled, the same Agile software part number is retained, i.e. only the revision number changes. NOTE: The PB980 part number refers to the PB980 UI displayed language. This should be reflected in the SW Catalog for each unique part number.

3. For SCD700, Emprint, LS10, FT10, and Signia, every time the software revision is  rolled, a new Agile software part number is created, i.e. the revision number and the part number changes

PB980 and SCD700 (match on name and associated hardware)

1. A user with permission to install all production versions can get all software packages which have same software name, and are associated with the same hardware as the docked device, and are not excluded by Country Exclusion..

2. A user with permission to install only the latest version can only get the software package~~s~~ which has the highest Comparison Order,  the same software name and is associated with the same hardware as the docked device, and is not excluded by Country Exclusion.

Emprint, LS10, FT10, Signia (match on hardware)

1.  A user with permission to install all production versions can get all software packages which are part of a system configuration that matches the hardware in the running configuration of the docked device, and is not excluded by Country Exclusion.

2. A user with permission to install only the latest software version can get only the software package which has the highest Comparison Order and is part of a system configuration that matches the hardware in the running configuration of the docked device, and is not excluded by Country Exclusion.

NOTE: For a Medtronic user, the default permission setting is to install all production versions. However this can be changed on an individual user basis.

For a non-Medtronic user, the default permission setting is to install only the latest production version. However this can be changed on an individual user basis.

*ID* : SRD-393

The gateway agent shall use business rules logic for device software selection in disconnected mode.

*ID* : SRD-396

The gateway agent shall provide the updated Business Rule(s) Files to the Client application

### Device Identification

*ID* : SRD-126

The system shall accept device identification.

*ID* : SRD-99

The gateway agent shall collect the device information through a message exchange with client application.

*ID* : SRD-127

The system shall enumerate devices by device type.

*ID* : SRD-128

The device types shall include those identified on schedule C.

*ID* : SRD-129 (Gateway-1685) (CRITICAL)

Device identifying information shall include:

Device Type

Device serial number

Device hardware

Device hardware version

Device hardware feature(s), if available

Device software

Device software version

Device feature (s), if available

*ID* : SRD-130

The system shall maintain a map between the device type, serial number and the customer.

Note 1: Serial numbers are not guaranteed to be unique across CoT so it’s important to qualify them with Device Type.

*ID* : SRD-140

The system shall be capable of automatically grouping devices according to a device type for viewing at the server.

*ID* : SRD-141

The system shall recognize a new device through device discovery.

*ID* : SRD-142

The system shall add new devices to the device records.

*ID* : SRD-143

The system shall categorize any new device added to the system by device type.

*ID* : SRD-144

The system shall support a multidimensional lookup to determine the current software for a device.

*ID* : SRD-149

The dimensions of the lookup shall include:

Country

Regulatory Approval

Entitlement

Device type

Device hardware

Device hardware version

Device hardware options [plural ], if available

Device software

Device software version

Device option software [plural ], if available

Device option software version [plural ], if available

*ID* : SRD-133

Device identifying information shall be exchanged in industry standard format for an example as XML.

*ID* : SRD-539 (Gateway 1597) (CRITICAL)

The Agent shall accept a message from the Client specifying device region for a specific device.

*ID* : SRD-540 (Gateway 1597) (CRITICAL)

The System shall record device region associated with a specific device, if provided by the Client.

*ID* : SRD-541 (Gateway 1597) (CRITICAL)

The System shall include device region in device history reports, if included in the device record.

### Device Warranty Management Requirements

*ID* : SRD-405 (High)

The system shall store the device maintenance expiration date, if available for a device.

*ID* : SRD-406 (High)

The system shall display the device maintenance expiration date, if available for a device.

### Device Prep Step Requirements (Gateway 1930)

*ID* : SRD-599 (CRITICAL)

Gateway Agent shall accept a list of device types from the client to limit the packages the Agent will download.

NOTE: This is for prep step.

*ID* : SRD-618 (CRITICAL)

If there is no active user session or all active user sessions have completed their package downloads, then Agent shall restart the download for any pending files.

*ID* : SRD-619 (CRITICAL)

When a user logs into the Client, the Agent shall suspend any package download activity unrelated to devices managed by the Client and for which the user has device permission.

*ID* : SRD-620 (CRITICAL)

The Agent shall report remaining download time by device type.

*ID* : SRD-621 (CRITICAL)

The Agent shall provide a means for the Client to identify itself via the Client’s GUID.

*ID* : SRD-622 (CRITICAL)

Upon receiving a Prep Step message from the Client, the Agent shall suspend downloading activity for all devices not specified in the Prep Step message..

*ID* : SRD-651 (CRITICAL)

Upon receiving a Prep Step message from the Client, as appropriate, the Agent shall start, continue or resume, downloading activity for all devices specified in the Prep Step message.

*ID* : SRD-623 (CRITICAL)

Packages which are downloaded by the Agent shall be cached according to CoT and device type.

NOTE: Cache

VENTILATION

PB980

VESSEL\_SEALING

VLLS10

VLFT10

ABLATION

Emprint Planning Software

COMPRESSION

SCD700

**STAPLING**

**Signia(TM) Stapler**

*ID* : SRD-624 (CRITICAL)

For each CoT, the Agent shall report the cumulative size on disk for all packages per device type per CoT.

*ID* : SRD-625 (CRITICAL)

The Agent shall read in an Agent-specific business rule file for associating CoT and Device Type.

*ID* : SRD-626 (CRITICAL)

The Agent shall check the Server for new versions of the CoT/Device Business Rule File and download it as appropriate.

### Device Software Upgrade Related Requirements

*ID* : SRD-101

The gateway agent shall manage the download of software from the server.

*ID* : SRD-102

The system shall notify the client application of completed software download via message exchange.

*ID* : SRD-103

The gateway agent shall cache the software package locally.

*ID* : SRD-104

The gateway agent shall check the package cache before downloading software packages to avoid duplication.

*ID* : SRD-356

The gateway agent shall identify all device-type software versions in its cache that are available for installation on edge devices.

*ID* : SRD-357

Upon connecting to the server, the gateway agent shall send a message to the server requesting all software versions for a specific device type that are available on the server.

*ID* : SRD-358

The "software request" message sent by the gateway agent upon connection to the server shall retrieve a list of all the software versions for a specific device type the server currently has available.

*ID* : SRD-359

The system shall determine which device type software is missing from the gateway agent's software list.

*ID* : SRD-360

The gateway agent shall determine the software needed based on the difference between software in its cache and the available software listed by the server.

*ID* : SRD-414

The gateway agent shall download all missing software based on the users’ authorized device type(s).

*ID* : SRD-361

The gateway agent shall download all missing software based on the missing software message from the server.

*ID* : SRD-158

The system shall support software package status.

*ID* : SRD-159

The software package status shall include:

Limited Release

In Production

Archived

*ID* : SRD-160

The agent shall present a list of all available software packages to the client application.

*ID* : SRD-161

The software package at the agent shall have an expiration time. (default 14 days， SCD700 is 3700 days)

*ID* : SRD-174

The device software installation shall be done by the client application.

*ID* : SRD-177

The system shall confirm successful updates of device software~~.~~

*ID* : SRD-178

The system shall prevent download of any package with ‘Limited Release’ status by users with insufficient privileges.

*ID* : SRD-179

The system shall provide a user interface to allow administrative users to upload software packages to the system.

*ID* : SRD-180

The system shall default to setting the status of new software packages to ‘Limited Release’.

*ID* : SRD-181

The system shall allow the administrator to set the software package status of a software package.

*ID* : SRD-530 (Gateway 1503) (CRITICAL)

The system shall provide a means by which a user with appropriate privileges is able to set the release order precedence of the Software packages.   
  
NOTE: The appropriate permissions are defined in SRD-478, use SW Catalog permission for this req.

*ID* : SRD-531 (Gateway 1503) (CRITICAL)

The system shall use the pre specified release order precedence to provide latest software to the client  
NOTE: This should operate in both connected and disconnected mode

*ID* : SRD-662 (Gateway 2224) (CRITICAL)

The system shall inform the Client application of the pre-specified order precedence of the downloaded software.

*ID* : SRD-661

The system shall allow devices that have a running configuration which corresponds to an archivednamed system configuration to upgrade to newer named system configuration.

*ID* : SRD-706

Software package contains subtypes including:

* Firmware
* BootCode
* Software Bundle
* Business Rule
* Software

*ID* : SRD-707

When a user archives a software/hardware package which is contained within named configurations, they should get a popup telling them that by archiving the software/hardware all configurations containing the software/hardware will also be archived and let user select whether to continue ~~or not~~.

Note: see GW-2928, GW-2934

*ID* : SRD-708

The system shall automatically create software ~~components~~ items which do not exist in the SW Catalog when the system discovers them in a device's running configuration. And these software ~~components~~ items shall be assigned with ~~Software~~ software bundle as software subtype by default.

Note: See GW-3051

*ID* : SRD-709

The system shall allow user to search software items by software name, or device type, or software type per CoT under Software Catalog.

*ID* : SRD-710

The system shall allow CoT Admin ~~administrator user~~ to associate the documents with software, in order to provide instructions or information to the end users.

*ID* : SRD-713

The system shall allow user to view the named system or software configurations that are associated with particular software.

Note: This requirement applies to Named Configurations devices.

*ID* : SRD-714

The system shall allow CoT Admin administrator user to clone existing software configuration(s) in order to create new software configuration(s).

*ID* : SRD-715

The system shall allow user to see the clone map of a software configuration, such as parent, siblings, and children.

*ID* : SRD-716

The system shall allow CoT Admin ~~administrator User~~ to add one or more country exclusions and associate it with a software item. If a software configuration or system configuration contains a software item that has country exclusion, then that configuration inherits the country exclusion from the item.

*ID* : SRD-1007

The system shall allow administrator user to transit status of software item as:

Unknown->Limited Release, In Production.

Limited Release -> In Production, Archived

In Production -> Archived, Limited Release

Archived -> Limited Release, In Production

ID: SRD-1028

User with appropriate permission can edit existing SW item based on below rules:

| **Entity** | **Status** | **Fields Which Can be Edited** | **Fields Which Cannot be Edited** |
| --- | --- | --- | --- |
| **Software Item** | Unknown | Comparison Order | Name |
|  |  | Description | Part Number |
|  |  | Software Type | Revision |
|  |  | Status | Device Type |
|  |  | Language |  |
|  |  | Allowed to upload package file |  |
|  |  | Country Exclusions |  |
|  |  | Associated Documents |  |
|  |  | Associated HW Items |  |
|  |  |  |  |
|  | Limited Release | All fields can be edited unless formerly In Production. If formerly In Production, then only fields that can be edited In Production can be edited | |
|  |  |  |  |
|  | In Production | Comparison Order | Name |
|  |  | Description | Part Number |
|  |  | Revision | Device Type |
|  |  | Software Type | Cannot delete file |
|  |  | Language |  |
|  |  | Allowed to upload package file |  |
|  |  | Country Exclusions |  |
|  |  | Associated Documents |  |
|  |  | Associated HW Items |  |
|  |  |  |  |
|  | Archived | Description | Name |
|  |  | Status | Part Number |
|  |  |  | Revision |
|  |  |  | Comparison Order |
|  |  |  | Device Type |
|  |  |  | Software Type |
|  |  |  | Language |
|  |  |  | Cannot delete or add files |
|  |  |  | Country Exclusions |
|  |  |  | Associated Documents |
|  |  |  | Associated Hardware |

### Device Log Handling

*ID* : SRD-100

The gateway agent shall accept logs if the client application provides them.

*ID* : SRD-164

If a device type provides log files, then the system shall accept log files from the device before updating the software

*ID* : SRD-165

If a device type provides log files, then the system shall store the device logs on the server.

*ID* : SRD-168

If a device type provides log files, then the system shall associate the logs for each device with that particular device serial number.

*ID* : SRD-173

If a device type provides log files, then the system shall allow the retrieval of all logs from the device

*ID* : SRD-169

The system shall capture service type with uploaded service information.

*ID* : SRD-170

The service type enumeration shall include:

Log Retrieval, if applicable for the device type (Log upload from the device)

Upgrade – Pass/Fail/Not-Attempted (Receipt of acknowledgement message from the Client Application/ Receipt of failed software update message from the Client Application/ User logs out without installing software after extraction, resulting in Not Attempted message)

Device Discovery (Device record created in database as a result of device connecting to the Client Application/Agent)

Device Registration (Device record created in database as a result of receiving the S/N from Medtronic Enterprise Database)

Device Connection (Device docked and sends a pre-defined message)

Configuration Update (New component detected in Device Information message)

Device Country Update (device country changed by Client)

Customer Information Changed (Customer name and/or address was changed in the device record).

*ID* : SRD-193

The system shall store the service records for each device on the server.

*ID* : SRD-194

The system shall default to reverse chronological order for the display of device service information.

*ID* : SRD-195

The system shall provide a user Interface to review service records.

*ID* : SRD-542 (Gateway 1645) (HIGH)

For all service events, the system shall include in all relevant screens and reports, the timestamp at which the event occurred, as well as the timestamp at which the server was notified of the event having occurred.   
  
NOTE: Service events include software upgrades, log file uploads, device discoveries, device configuration uploads, etc

*ID* : SRD-120

The gateway agent shall keep cached log files for 24 hours after receipt of a successful upload of the log files.

Note: This is a Disaster Recovery (DR) provision to help protect the system from data loss.

*ID* : SRD-150

The system shall provide a user interface to users to view device information on the server. The device information includes device logs and service records. (Gateway 1151 update)

*ID* : SRD-467

The system shall control access to view device records through the Web UI based on role, device access permissions, CoT, and user type.

*ID* : SRD-468

The system shall allow a user with appropriate permissions to view device records  through the Web UI that belong to the Classes of Trade with which the user is associated.

*ID* : SRD-721

The system shall allow a user to download a decrypted log file to his computer through the log-viewer.

### Document Handling

*ID* : SRD-152

The system shall allow the upload of documents for distribution by CoT Admin users..

*ID* : SRD-153 (CRITICAL)

The system shall allow the option of associating a document with a SW or HW or Featurecatalog item.

*ID* : SRD-154

The system shall allow the independent download of documents based on role and access policy.

*ID* : SRD-156

The system shall classify uploaded documents by document type

*ID* : SRD-157

The document type enumeration shall include:

Release Notes

User Guides

Service Manual

Other

*ID* : SRD-382

The UI shall support a PDF Viewer that only supports viewing of PDF documents.

NOTE: Do not allow other functions such as printing, saving,etc**.**

*ID* : SRD-736

The system shall allow CoT Admin administrator user to edit an existing document item based on below rules:

| **Entity** | **Status** | **Fields Which Can be Edited** | **Fields Which Cannot be Edited** |
| --- | --- | --- | --- |
| **Document Item** | Unknown - NA |  |  |
|  |  |  |  |
|  | Limited Release | All fields can be edited. | |
|  |  |  |  |
|  | In Production | Description | Name |
|  |  | Document Type | Part Number |
|  |  | Revision | Device |
|  |  | Status | Cannot delete file |
|  |  | Language |  |
|  |  | Accessible |  |
|  |  | Allowed to upload file |  |
|  |  | Associated Hardware Items |  |
|  |  | Associated Software Items |  |
|  |  | Associated Feature Items |  |
|  |  |  |  |
|  | Archived | Description | Name |
|  |  | Status | Part Number |
|  |  |  | Revision |
|  |  |  | Device Type |
|  |  |  | Document Type |
|  |  |  | Language |
|  |  |  | Accessible |
|  |  |  | Cannot delete or add files |
|  |  |  | Associated Hardware |
|  |  |  | Associated Software |
|  |  |  | Associated Features |

*ID* : SRD-737

The system shall allow CoTadmin to archive existing documents.

*ID* : SRD-738

The system shall allow administrator user to transit status of document as:

Limited Release -> In Production, Archived

In Production -> Archived, Limited Release

Archived -> Limited Release, In Production

*ID* : SRD-739

The system shall allow user to search documents by document name, or device type.

*ID* : SRD-740

The system shall allow a CoT Admin user to clone existing document items in order to easily create new document item

*ID* : SRD-741

The system shall allow user to see the clone map of document, such as parent, siblings, and children.

*ID* : SRD-1002

The system shall allow CoT admin to choose whether the document can be seen by non-covidien user when he adds a document.

### Regulatory and Trade Embargo Requirements

*ID* : SRD-166

If a device type provides log files, then the system shall retain the log files for a minimum of seven (7) years.

*ID* : SRD-331

The system shall not provide software to devices in countries that are denied regulatory approval.

NOTE: Refer to Section 8.2.1.4, Device Regulatory Permission.

*ID* : SRD-332

The system shall provide a means to track countries where regulatory approval has not been gained.

*ID* : SRD-334

The system shall associate a country with the user.

*ID* : SRD-335

The UI shall allow the selection of a country as part of the user profile screen.

*ID* : SRD-336

The gateway agent shall provide the country associated with the user to client applications for use as the default country for installation.

Note: Default will be provided when there is no country information in device info message.

*ID* : SRD-337

If a client provides a country code to the gateway agent, the system shall use this as the device’s country for software installation.

*ID* : SRD-473

If a client does not provide a country code to the gateway agent, the system shall use the country associated with the user as the device’s country for software installation.

*ID* : SRD-454

The Gateway Agent shall provide a means for the Client Application to send user-entered customer information to be stored on the server.

Note: This does not replace the data obtained from public schema.

Note: This address is entered as free form text and does not follow any particular rules. This should be able to be pulled into a report.

### Device Configuration Management

*ID* : SRD-456

The system shall allow configuration management, including hardware, software, feature, and system configuration through the web UI.

*ID* : SRD-196

The system shall verify that device information sent from the gateway agent matches server database configuration records for the device.

Note: The comparison data comes from configurations that are created by the CoT Admin on the server.

*ID* : SRD-138

The system shall determine most current software for the device based on the device’s running configuration information.

Note: Criteria for Update: Configuration and Country of Device. (Warranty status is not a criteria for eligibility for update of Surgical Solutions devices).

*ID* : SRD-197

The system shall flag devices that have configurations that differ from the server database records.

*ID* : SRD-198

The system shall report configuration discrepancies.

Note: Differences between what is actually found in the field versus what was expected to be on the device. The intent of this requirement is for the system to create an exception every time a device docks with a configuration that has been changed from the last time it docked, except when the configuration was changed by the GDMP (i.e. performing a software update on a device).

*ID* : SRD-220

The system shall provide a UI to display discrepancy lists.

*ID* : SRD-458

The gateway agent shall respond to a request from the client asking if a device configuration is valid.

NOTE: Refer to Section 8.2.2, Configuration Validation.

*ID* : SRD-404

When a conflict exists between a device’s configuration on the server and the device’s running configuration as reported by the device, the system shall use the configuration reported by the device

*ID* : SRD-496 (Gateway 664) (CRITICAL)

The system shall store all configuration items reported by the device which are defined in the HW/SW/Featurecatalogs.

ID: SRD- 642 (HIGH)

If a configuration item sent to the server from the agent is not found in the HW/SW/Feature catalog, then the system shall report the state of the configuration item as “Unknown”

*ID* : SRD-610 (Gateway 1665) (CRITICAL)

The system shall provide a means for the client to report the docked device's running configuration.

*ID* : SRD-611 (Gateway 1665) (CRITICAL)

Reported running device configurations shall consist of one or more software components, and one or more hardware components.   
  
NOTE: Optionally, device location may be specified.  
  
~~NOTE: For v3.0, all device components may be reported as a single named configuration.~~   
NOTE: For v3.0, activated features may also be reported.

### Orion Specific Configuration Management Requirements

*ID* : SRD-654 (Gateway 2004) (CRITICAL)

The system shall provide an interface to the Client to send a serial number for a device hardware component to the system.

*ID* : SRD-655 (Gateway 2004) (CRITICAL)

The system shall store the serial number for all hardware components in the device record.

*ID : SRD-658 (Gateway 2012)*

The system shall provide a view of the VLFT10 hardware component serial numbers in the device configuration history.

### Named Configuration

***Named Configuration Requirements- Server/Web UI***

*ID* : SRD-297 (HIGH)

The system shall allow a user with Configuration Admin permission to create/edit/archive named configurations.

*ID* : SRD-499 (Gateway 1054) (HIGH)

Only users who have Configuration Administration permission shall be permitted to add /modify/archive named configurations.

*ID* : SRD-500 (Gateway 1054) (HIGH)

The system shall support named hardware configurations.

*ID* : SRD-501 (Gateway 1054) (HIGH)

The system shall support named software configurations.

*ID* : SRD-503 (Gateway 1054) (HIGH)

A named system configuration shall be composed of any combination of the following:

- a named hardware configuration,

- a named software configuration,

- a named feature configuration

-

ID: SRD-795

System configuration with "In Production" status shouldn't contain software configuration in 'Limited Release' status.

.

*~~ID~~* ~~: SRD-504 (Gateway 1054) (HIGH)~~

~~A software configuration item uploaded to the Software Catalog must be associated with one or more compatible~~ **~~hardware~~** ~~configurations.~~

~~NOTE: Currently a software configuration item is associated only with a compatible hardware configuration item.~~

*ID* : SRD-507 (Gateway 1054) (HIGH)

A named hardware configuration shall be composed of one or more hardware items.

*ID* : SRD-508 (Gateway 1054) (HIGH)

Each hardware item within a named hardware configuration shall be treated by the system as “enforceable”.

NOTE: ”Enforceable means the hardware items contained in the running hardware configuration must be checked to determine if a particular named configuration is compatible with the running HW configuration.

NOTE: All hardware items listed in a hardware configuration are enforceable by default.

*ID* : SRD-509 (Gateway 1054) (HIGH)

A named software configuration shall be composed of one or more software configuration items.

*ID* : SRD-513 (Gateway 1054) (HIGH)

System shall not present to the Client those Named System Configurations which have constituent components with either archive status.

*ID* : SRD-514 (Gateway 1240) (HIGH)

A device configuration shall be considered valid if it matches a valid named system configuration on the server.

*ID* : SRD-523 (Gateway 1240) (HIGH)

The gateway agent shall respond to a request from the client asking for a list of all valid named system configurations for a specific instance of a device type.

*ID* : SRD-515 (Gateway 1054) (HIGH)

When the user adds a new software item, system shall allow user to associate this software item with ~~existing hardware configuration (for 3.0 product line) or~~ existing hardware item (for Catalog Configuration Devices)

*ID* : SRD-516 (Gateway 1054) (HIGH)

When searching for a matching hardware configuration and multiple matching configurations are found, the system shall select the most constrained matching hardware configuration.

Note:

HW configurations can contain one or more HW item. If a device matches three HW configurations:

A

A, B

A, B, C

Then A, B, C will be selected, because it is the most constrained – i. e. it has the most components, and that limits, or constrains, the number of HW variations it can match versus the other two configurations.

*ID* : SRD-517 (Gateway 1054) (HIGH)

The system shall allow a user to associate one or more documents with a hardware, software, or feature item.

*ID* : SRD-520 (Gateway 1054) (HIGH)

System shall allow user (with appropriate permissions) to associate a software configuration with a system configuration.

Note: A s/w configuration is contained within a s/w package.

Note: The s/w and system configuration are created by GBU (CoT Admin)

*ID* : SRD-521 (Gateway 1054) (Low- High)

The Gateway Agent shall provide a list comprising of all Named System Configurations and its subcomponents, recursively down to individual configuration items, for the device type which is currently docked to the Client.

*ID* : SRD-627 (Gateway 1054) (HIGH)

The system shall return appropriate software list based on the device running configuration sent by the Client.

.

NOTE: For v2.0, the first software component is used for comparison to hardware components to verify device configuration as valid and to determine available software.

*ID* : SRD-628 (Gateway 1054) (HIGH)

The system shall allow a user with appropriate permissions to set a named configuration to one of the following states through the WebUI:

* 1. In Production
  2. Archived
  3. Limited Release

*ID* : SRD-644 (Gateway 1054) (CRITICAL)

If a device docks with a running hardware configuration that satisfies the hardware items in a named system configuration, then the software package from the named system configuration will be delivered to the Client.

NOTE: Any hardware item in the device running hardware configuration which is not found in a hardware configuration in a named configuration, that hardware item is treated as a “don’t care” and has no impact on the hardware configuration match.

*~~ID~~* ~~: SRD-742~~

~~Need add the rules for download software packages by matching Named System Configuration.~~

*~~ID~~* ~~: SRD-743~~

~~Add New Configuration page shall default to whatever type of configuration was selected in previous page.~~

~~Note: refer to GW-2841~~

*ID* : SRD-744

The system shall provide appropriate candidate list of warning-configurations for different warning types. These are:

1. HW incompatible with HW: Only show warning hardware configuration in the candidate list

2. SW incompatible with SW: Only show “warning sw configuration’ in the candidate list

3. Upgrade-Forbidden System Configurations: Only show “valid sw-config” and “valid hw-

config’ in the candidate list

4. HW incompatible with SW: Only show “valid sw-config” and “valid hw-config”as candidate list

* 1. Feature incompatible with Feature: Only show warning Feature configurations as candidate list
  2. HW incompatible with Feature: Only show HW and Feature configurations as candidate list.
  3. SW incompatible with Feature: Only show SW and Feature configurations as candidate list
  4. HW/SW incompatible with Feature: show HW, SW and Feature configurations as candidate list.

*ID* : SRD-745

The system shall allow CoT Admin administrator user to view a country exclusion that may be associated with software items in the software configuration.

*ID* : SRD-746

The system shall allow user to search configurations by name, or device type, or configuration type.

*ID* : SRD-747

The system shall allow user to view a named hardware/software/feature/system configuration.

*ID* : SRD-748

User with appropriate permission can edit named hardware configuration based on below rules:

| **Entity** | **Status** | **Fields Which Can be Edited** | **Fields Which Cannot be Edited** |
| --- | --- | --- | --- |
| **Hardware Configuration** | Unknown - NA |  |  |
|  |  |  |  |
|  | Limited Release | All fields can be edited unless formerly In Production. If formerly In Production, then only fields that can be edited In Production can be edited | |
|  |  |  |  |
|  | In Production | Description | Name |
|  |  | Status | Device Type |
|  |  | ??? | Associated Hardware |
|  |  |  | Is Warning Config |
|  |  |  | Warning Config type |
|  |  |  |  |
|  | Archived | Description | Name |
|  |  | Status | Device Type |
|  |  |  | Is Warning Config |
|  |  |  | Associated Hardware |

.

ID: SRD-1029

User with appropriate permission can edit named software configuration based on below rules:

| **Entity** | **Status** | **Fields Which Can be Edited** | **Fields Which Cannot be Edited** |
| --- | --- | --- | --- |
| **Software Configuration** | Unknown - NA |  |  |
|  |  |  |  |
|  | Limited Release | All fields can be edited unless formerly In Production. If formerly In Production, then only fields that can be edited In Production can be edited | |
|  |  |  |  |
|  | In Production | Description | Name |
|  |  | Status | Device Type |
|  |  | ??? | Associated Software |
|  |  |  | Is Warning Config |
|  |  |  | Warning Config type |
|  |  |  |  |
|  | Archived | Description | Name |
|  |  | Status | Device Type |
|  |  |  | Is Warning Config |
|  |  |  | Associated Software |

ID: SRD-1030:

User with appropriate permission can edit named system configuration based on below rules:

| **Entity** | **Status** | **Fields Which Can be Edited** | **Fields Which Cannot be Edited** |
| --- | --- | --- | --- |
| **System Configuration** | Unknown - NA |  |  |
|  |  |  |  |
|  | Limited Release | All fields can be edited unless formerly In Production. If formerly In Production, then only fields that can be edited In Production can be edited | |
|  |  |  |  |
|  | In Production | Description | Name |
|  |  | Status | Device Type |
|  |  | ??? | Associated HW Configs |
|  |  |  | Associated SW Configs |
|  |  |  | Associated Feature Configs |
|  |  |  | Is Warning Config |
|  |  |  | Warning Config type |
|  |  |  |  |
|  | Archived | Description | Name |
|  |  | Status | Device Type |
|  |  |  | Is Warning Config |
|  |  |  | Associated HW Configs |
|  |  |  | Associated SW Configs |
|  |  |  | Associated Feature Configs |

*ID* : SRD-1006

The system shall allow administrator user to transit status of named configuration as:

Limited Release -> In Production, Archived

In Production -> Archived, Limited Release

Archived -> Limited Release, In Production

*ID* : SRD-1009

When the status of item changes form In Production to Limited Release, system shall provide a warning that all related in-production named configurations will be changed to Limited Release, and let user to determine whether continue to proceed.

### Serial Number Reprogram

*ID* : SRD-549 (CRITICAL)

The Gateway Agent shall accept notification from Client that the serial number has been programmed on the device.

NOTE: This workflow can be implemented in both connected and disconnected modes.

*ID* : SRD-647 (CRITICAL)

The system shall store serial number reprogramming information in the associated device record.

*ID* : SRD-648 (CRITICAL)

The system shall provide a serial number reprogrammed notification to those users who are subscribed.

*ID* : SRD-649 (CRITICAL)

The system shall record serial number reprogramming user activity into the user audit log.

*ID* : SRD-650 (CRITICAL)

The system shall display serial number reprogramming user activity in the user activity report.

### Feature Licensing

ID : SRD-557 (CRITICAL)

The System shall provide a view of the feature entitlement properties which are associated with a device as part of the device record view.

ID : SRD-544(Gateway 1659) (CRITICAL)

The System shall provide a means to associate a single unique device feature with one or more device configurations.

NOTE: Feature associations shall only be implemented with the Named Configurations functionality of the System.

ID : SRD-558 (CRITICAL)

The System shall provide a Feature Catalog, which contains Feature Items.

ID : SRD-988 (CRITICAL )

Feature Items shall contain the following information:

Feature Name

Feature SKU

Feature Description

Country Exclusion List

NOTE: Feature Items will perform a similar function as HW/SW Items, and will identify individual features just as HW/SW Feature Items identify HW/SW components of the system.

ID : SRD-559 (CRITICAL)

The System shall provide a means for a user with appropriate permissions to create, edit, clone and archive feature items in the Feature Catalog.

ID : SRD-987 (CRITICAL)

The System shall provide a Feature type of Named Configuration – i.e. a Named Feature Configuration.

ID : SRD-566 (CRITICAL)

The System shall provide a means to create, edit, clone and archive Named Feature Configurations.

ID : SRD-560 (CRITICAL)

The System shall provide a means for a user with appropriate permissions to associate Feature Items in the Feature Catalog with Named Feature Configurations.

ID : SRD-561 (CRITICAL)

The System shall provide a means for a user with appropriate permissions to associate a Feature Item in the Feature Catalog with one or more countries for which the feature should not be deployed.

ID : SRD-999 (CRITICAL)

The System shall provide a means for a user with appropriate permissions to associate a Named Feature Configuration with a Named System Configuration

ID : SRD-998 (CRITICAL)

The System shall provide a means to accept feature entitlement sales record data from the corporate enterprise repository.

ID : SRD-997 (CRITICAL)

The System shall interpret feature entitlement sales records and for each sales record, and for each entitlement sale, shall entitle each referenced device instance (serial number) according to the entitlement license terms in the record.

ID : SRD-554 (CRITICAL)

The System shall store feature entitlement properties in the device record for permanent storage (This will be separate from last known device configuration).

ID : SRD-996 (CRITICAL)

The System shall provide a UI that enables a user with appropriate permissions to modify a device’s feature entitlements and save them for later deployment.

ID : SRD-552 (CRITICAL)

The System shall provide a list of last known actually enabled features to the Client which are associated with a connected device.

ID : SRD-553 (CRITICAL)

The System shall accept a list from the Client of currently enabled features for a device connected to the Client.

ID : SRD-555 (CRITICAL)

The System shall record device feature enabled status received from the Client in the device running configuration.

ID : SRD-556 (CRITICAL)

On docking, the System shall provide to the Client a list of Feature Entitlements, and their properties, together with the last known device configuration.

ID : SRD-995 (CRITICAL)

The Feature Entitlement functionality of the System shall accommodate the addition of new devices which use existing Feature Entitlement functionality by simply adding the device and its Class of Trade to the System.

NOTE: System restart may be required, and is acceptable.

NOTE: Addition of the new device’s HW/SW/Feature items to the various catalogs and Named Configurations is required of the CoT/device customer to make the device fully functional in the new System.

ID : SRD-994 (CRITICAL)

The System shall implement a pluggable interface in its Feature Entitlement function to accommodate onboarding new devices which have Feature Entitlement requirements which are not met by the existing System.

ID : SRD-993 (CRITICAL)

The System shall provide the following Feature Entitlement extension points (abstractions) as part of the pluggable interface.

• Feature Entitlement Workflow

o Where Feature Entitlement sales data are received from

o Where Feature Entitlement change management data is delivered

• Licensing Mechanism

o How the device is told what features are to be enabled/disabled (activation key, license file, where to get them, means of generating them)

• License Metadata

o How the license terms are specified

• License application rules

o How the license terms are interpreted

• Feature Entitlement Views

o Device configuration

o Feature catalogs and named configurations

• Feature Entitlement Alerting

• Feature Entitlement Reporting

ID : SRD-992 (CRITICAL)

The System shall provide a Device Feature Entitlement Report View which is filterable by

• Country(s)/All

• Customer(s)/All

• Device Type

• Feature Type(s)/All

• Entitled/Not Entitled/Both

o Entitled

 Entitled Date Range/All

 Enabled/Disabled/Both

o Not Entitled

 No sub-filters

ID : SRD-991 (CRITICAL)

The System Device Feature Entitlement Report View shall display the following information.

• Filters

o Countries filtered

o Customers filtered

o Device Type

o Feature Types filtered

o Entitled filters

o Enabled filter

• Report Data Columns/Content

o Country

o Customer

o Device Serial Number

o Filtered Features List (one per line)

*  Entitlement ID
*  Entitlement State (Entitled/Not Entitled)
*  Entitlement Term
*  Device Feature Enabled Status

ID : SRD-990 (CRITICAL)

The System Device Feature Entitlement Report View shall have an option to print (TBD: save???) the report.

ID : SRD-989 (CRITICAL)

The System Device Feature Entitlement Report View shall print the following information.

• Title Page

o Device Feature Entitlement Report for <UserName>

o Countries filtered

o Customers filtered

o Device Type

o Feature Types filtered

o Entitled filters

o Enabled filter

• Page 2+ Header

o Countries filter

o Customers filter

o Device Type

o Feature Types filter

o Entitled filter

o Enabled filter

• Page 2+ Body

o Section Headings

 By Country

• By Customer

o Columns/Content

 Device Serial Number

 Filtered Features List (one per line)

• Entitlement ID

• Entitlement State (Entitled/Not Entitled)

• Entitlement Term

• Device Feature Enabled Status

ID: SRD-9974

If feature entitlement constraints are violated, GDMP should inform user when the device is next docked.

ID : SRD-692

The system shall enable user to review the features for a specific device with the following information:

- Feature name

- Feature description

- Feature license term

- Enabled Status: Enabled/disabled

- Entitlement Status: Entitled/ Not Entitled

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

ID : SRD-722

The system shall allow administrator user to import feature license for devices from ETL.

ID : SRD-9979

The System Shall provide a device-specific license in the form which is recognizable by the device..

ID : SRD-9978

The System shall be capable of creating feature licenses which are specific to a particular device instance.

ID : SRD-9977

The System shall be capable of creating feature licenses which contain features to be enabled on the device which match the device’s entitlement record.

ID : SRD-724

The system shall provide to the client a license intended for a specific device.

ID : SRD-564 (CRITICAL)

The System shall record device feature licensing operations in the device's and user's audit trail.\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

ID : SRD-565 (CRITICAL)

The System shall provide a means to notify users of device feature licensing operations \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

ID : SRD-9976 (CRITICAL)

The System shall provide a means for users to subscribe to one or more different device feature license operation notifications.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

ID : SRD-634 (CRITICAL)

If a feature sent to the server from the agent is not found in the feature catalog, then the system shall generate an alert for unknown feature.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

ID : SRD- 635 (CRITICAL)

If a device record is not entitled for a feature which is reported as activated, then the system shall generate an alert for unentitled feature.

ID: SRD-9975

The system should generate an alert when temporary entitlements expire according to their license term.

ID: SRD-9973

The system should provide different warning messages to client according to different warning configurations, and the warning message should be implemented in an <extended\_info> tag in message.

ID:SRD-1008

The system shall allow administrator user to transit status of feature item as:

Unknown  -> Limited Released, In Production

Limited Release -> In Production, Archived

In Production -> Archived, Limited Release

Archived -> Limited Release, In Production

ID: SRD-1031

User with appropriate permission can edit feature item based on below rule:

| **Entity** | **Status** | **Fields Which Can be Edited** | **Fields Which Cannot be Edited** |
| --- | --- | --- | --- |
| **Feature Item** | Unknown | Description | Name |
|  |  | Status | Device Type |
|  |  | SKU |  |
|  |  | Country Exclusions |  |
|  |  | Associated Documents |  |
|  |  |  |  |
|  | Limited Release | All fields can be edited unless formerly In Production. If formerly In Production, then only fields that can be edited In Production can be edited | |
|  |  |  |  |
|  | In Production | Description | Name |
|  |  | Status | Device Type |
|  |  | Country Exclusions | SKU |
|  |  | Associated Documents |  |
|  |  |  |  |
|  | Archived | Description | Name |
|  |  | Status | Device Type |
|  |  |  | SKU |
|  |  |  | Country Exclusions |
|  |  |  | Associated Documents |

ID: SRD-1032

User with appropriate permission can edit feature configuration based on below rule:

| **Entity** | **Status** | **Fields Which Can be Edited** | **Fields Which Cannot be Edited** |
| --- | --- | --- | --- |
| **Feature Configuration** | Unknown - NA |  |  |
|  |  |  |  |
|  | Limited Release | All fields can be edited unless formerly In Production. If formerly In Production, then only fields that can be edited In Production can be edited | |
|  |  |  |  |
|  | In Production | Description | Name |
|  |  | Status | Device Type |
|  |  | ??? | Associated Features |
|  |  |  | Is Warning Config |
|  |  |  | Warning Config type |
|  |  |  |  |
|  | Archived | Description | Name |
|  |  | Status | Device Type |
|  |  |  | Is Warning Config |
|  |  |  | Warning Config type |
|  |  |  | Associated Features |

ID: SRD-1033

User with appropriate permission can edit feature entitlement based on below rule:

| **Entity** | **Status** | **Fields Which Can be Edited** | **Fields Which Cannot be Edited** |
| --- | --- | --- | --- |
| **Feature Entitlement** | Unknown | Term | Name |
|  |  | Count | Device Type |
|  |  | License File | Serial Number |
|  |  | License Key |  |
|  |  |  |  |
|  | Limited Release | All fields can be edited unless formerly In Production. If formerly In Production, then only fields that can be edited In Production can be edited | |
|  |  |  |  |
|  | In Production | Status | Name |
|  |  |  | Device Type |
|  |  |  | Device Serial Number |
|  |  |  | Term |
|  |  |  | Start Date |
|  |  |  | End Date |
|  |  |  | License Type |
|  |  |  | License Key |
|  |  |  |  |
|  | Archived | Status | Name |
|  |  |  | Device Type |
|  |  |  | Device Serial Number |
|  |  |  | Term |
|  |  |  | Start Date |
|  |  |  | End Date |
|  |  |  | License Type |
|  |  |  | License Key |

ID : SRD-1035

The System shall provide a means for a user with appropriate permissions to clone feature entitlement.

ID: SRD-1036

The feature entitlement should have status: Unknown, Limited Release, In Production and archived. And feature entitlement status can be transit from one to another.

ID: SRD-1037

When the status of a Feature is changed, the corresponding Feature Entitlement will be changed accordingly by the system automatically.  
Exception: When a Feature Entitlement is in "Archived" state, the system shall only allow manual change to come out of the "Archived" status.

ID: SRD-1038

When either a Feature or a Feature Entitlement is discovered when a device is docked (i.e not already defined in the Feature catalog), it shall be added to the appropriate page and the Status set to Unknown. Any information about the Feature Entitlement that is provided by the device should be entered in the Feature Entitlement page. Any missing information shall be filled in by the CoT Admin.

### System Activity Tracking

*ID* : SRD-199

The system shall maintain an audit trail of system activity.

*ID* : SRD-200

The system shall keep activity logs that track logins.

*ID* : SRD-201

The system shall keep activity logs tracking software upgrades.

*ID* : SRD-202

The system shall keep activity logs tracking user activity through the gateway agent that runs on a Windows PC.

*ID* : SRD-203

The system shall enumerate user Action Type which will include:

Log Retrieval, if applicable for the device type (Log upload from the device)

Upgrade - Pass/Fail /Not-Attempted (Receipt of acknowledgement message from the Client Application/ Receipt of failed software update message from the Client Application/ User logs out without installing software after extraction, resulting in Not Attempted message)

Device Discovery (Device record created in database as a result of device connecting to the Client Application/Agent)

Device Registration (Device record created in database as a result of receiving S/N from Medtronic Enterprise Database )

Device Connection (Device docked and sends a pre-defined message)

Configuration Update (New component detected in Device Information message)

*ID* : SRD-204

The system shall include the following in non-software update audit data:

Date and time

User identity

Device type

Device serial number

Action type

*ID* : SRD-205

The system shall capture and store each software update that was performed. Information to be included in this record will include at a minimum:

Type of device updated

Serial number of device updated

Date/time of upgrade

Name of person performing the upgrade

Name of the software package

Configuration of device prior to the update (hardware and software versions)

Configuration of device following the update (hardware and software versions)

Success or failure status of the update

### Gateway Agent Maintenance

*ID* : SRD-377

The system shall maintain latest version of agent software.

*ID* : SRD-378

The system shall support a message whose contents are the current revision number for the agent software.

*ID* : SRD-379

The system shall check for updates to the agent software when agent connects to the server.

*ID* : SRD-380

The agent will download new version of itself if available.

*ID* : SRD-381

The system shall install new versions of the agent software if if user’s machine is idle

*ID* : SRD-753

The system shall allow the user to sign on to the GDMP via the Agent, when the server connection is available. When the server connection is not available, the Agent will sign on the user using the local cache.

*ID* : SRD-754

The system shall automatically sync user credentials ~~support sync user sign on criteria~~ as well as roles and permissions from GDMP server when agent is connected with server.

*ID* : SRD-763

Agent should enforce the device serial number formatting.

*ID* : SRD-764

GDMP agent shall record current version of agent in the registry of machine during installation process.

*ID* : SRD-767

All interactions between DMA and DMP shall be independent of user sessions.

Note: The session between Client App and DMA shall be maintained due to backwards capability with legacy clients.

*ID* : SRD-770

Agent shall delete notifications if they have been delivered to client or server

By default it's 24 hours later.

*ID* : SRD-771

Client application shall be able to get agent status such as GDMP server is available, GDMP server is connected from agent

### Client Application Software Related Requirements

*ID* : SRD-326

The system shall maintain a list of client application software and their versions.

*ID* : SRD-327

The system shall support a message whose contents are the current revision numbers for the client application software.

*ID* : SRD-328

The system shall check for updates to the client application software when the agent connects to the server.

*ID* : SRD-329

The agent will download new version of the client application software if available.

*ID* : SRD-330

Client application shall choose to install upgrade or not per its configuration.

*ID* : SRD-749

System shall allow user to download an Agent Installer from GDMP web after successful login.

### Alerts

*ID* : SRD-182

The system shall provide a user interface to allow users to subscribe and unsubscribe to alerts per device type.

*ID* : SRD-218 (CRITICAL)

The following events result in generation of *informational alert* event:

New device registration

Device Update – NOTE: Device docked and its configuration updated on server

Device SW Upgrade

Feature enablement

A device's configuration has changed (discrepancy report regarding HW/SW/Feature)

Device docked with unknown component

Serial Number changed (realigned)

*ID* : SRD-573 (CRITICAL)

The following alerts result in the generation of *business alert* event:

* (FUTURE REQ) Invalid Configuration Alert - An invalid device configuration was detected.
  + Invalid configuration
  + Not all Components Found
  + No Components Found
* Upgrade Failed Alert - A software upgrade package has failed or installation was incomplete.
* The country sent by the Client is different from the Device record in server.
* Attempt to update software without upgrade privileges
* A software update is started but not completed within a configurable time limit, while in the connected mode
* Alert when a non- Medtronic user attempts to upgrade SW on a device which is assigned to an account number which is not the user's account number. (RMS only)

*ID* : SRD-645 (CRITICAL)

A Medtronic user can subscribe to alerts for operations on all devices for a particular device type.

*ID* : SRD-638 (CRITICAL)

A non- Medtronic user with appropriate permissions can subscribe to alerts related to a particular device type

*ID* : SRD-636 (CRITICAL)

A user with appropriate privileges may generate a General Notification for the following events:

* System upgrade notice

 general notification to users associating with Device Type

*ID* : SRD-211

The system shall use the email to notify end users of alerts.

*ID* : SRD-215

The system shall provide a means to filter alerts based on alert event type, device type and CoT.

*ID* : SRD-216

The system shall classify alerts according to alert event type.

*ID* : SRD-217

The alert event type text shall be in the subject line of the email.

*ID* : SRD-637 (Gateway-1377) (CRITICAL)

The system shall support the following alert notification permissions, which can be applied to any role:

* 1. Subscribe to alert notifications for devices serviced by user (across one or more selectable device types)
     1. Subscribe to informational alerts
     2. Subscribe to business alerts
  2. Subscribe to alert notifications for all devices of a specific device type by Country or groups of countries
     1. Subscribe to informational alerts
     2. Subscribe to business alerts
  3. Subscribe to alert notifications for all devices associated with the same customer account numbers with which the user is associated (across one or more selectable device types)
     1. Subscribe to informational alerts
     2. Subscribe to business alerts

NOTE: Only the Site Admin creates/Sends/subscribes/unsubscribes Technical alerts. CoT admin can review the tech alert list and history.

*ID* : SRD-214 (Gateway 799) (CRITICAL)

The system shall enable System administrator to manually create **custom** email content of general notification and send it on command to all users of a specific device type.

*ID* : SRD-576 (CRITICAL)

The system shall provide the ability to configure how the alert is sent.

Note: For v3.0, only email will be supported.

*ID* : SRD-577 (CRITICAL)

The system shall track the state of an alert.

*ID* : SRD-578 (CRITICAL)

The **states of alert** shall include:

* Pending
* Sent
* Duplicate
* Acknowledged
* Resolved
* Closed

*ID* : SRD-579 (CRITICAL)

The system shall allow the collection of user comments on all alert state changes which are made by user.

*ID* : SRD-580 (CRITICAL)

The system shall provide a means for a user with appropriate privileges to view an alert state.

*ID* : SRD-582 (CRITICAL)

The system shall allow a user with appropriate privileges to transition an Alert from Sent to Acknowledged.

*ID* : SRD-583 (CRITICAL)

The system shall allow a user with appropriate privileges to transition an Alert from Acknowledged to Resolved.

*ID* : SRD-643 (CRITICAL)

The system shall allow a user with appropriate privileges to transition an Alert from Resolved to Closed.

*ID* : SRD-585 (Gateway 1377) (CRITICAL)

The system shall allow a user to subscribe/unsubscribe their individual alerts.

*ID* : SRD-586 (CRITICAL)

The system shall provide an interface to view all alerts.

*ID* : SRD-731

System shall allow Medtronic security user to send informational notification automatically when users change their status so that they can verify changes are authorized and properly made by themselves or manager.

*ID* : SRD-733

System shall be able to send business alerts when activated by a business rule so that the notified users can take appropriate action.

*ID* : SRD-1005 (CRITICAL)

When a user subscribe alert event, he can choose which device scope to subscribe including “Mine” and “All”. For a MDT user, if he selects “Mine”, they he should receive alerts only for cases where he performed the event causing the alert. If he selects “All”, then he should receive alerts for any user performing the event causing the alert. For a non-MDT user, if choose Mine, then user can only view alert triggered from my devices; If choose All, then user can view All alert from devices with the same customer.

ID: SRD-1025

If user gets the same Alert on the same Device within 24 hours, it will be treated as Duplicated. User will not receive notification email for duplicated alert.

The duplicate alert is per Device per Event Code per Alert Recipient. So the user who actually generated the alert does not matter, just the person who the alert is sent to. Sometimes this is the same person, but not always, depending on whether the person subscribed to "Mine" vs "All" alerts.

ID: SRD-1034

Cot Admin/Site Admin can enable or disable global alert subscription per device type per event per role. Only after admin enable an Alert for a role, individual user of the role can subscribe for the alert.

ID: SRD-1027

Individual user can receive alert notification mail only after subscribe the alert for himself.

### Reporting

#### General requirement on Reports

*SRD-805*

*All items in filter drop down lists shall be displayed in alphabetical order.*

*SRD-806*

*All filter drop down lists shall be searchable by entering at least the first 3 characters of the item name.*

*SRD-807*

*All items in the filter drop down lists shall be displayed when the user types in 3 space characters.*

*SRD-808*

*The system shall allow the user to sort a displayed report based on any column.*

*SRD-809*

*The system shall provide tooltips on each entry of reports.*

*SRD-810*

*The system shall allow user to download reports as files of PDF, CSV, XLS format, or print online. The content of downloaded or printed reports shall be the same as the reports displayed on Web UI.*

*SRD-811*

*The system shall allow user to search for these filters of User name, Customer name and Device serial number with partial keyword.*

*SRD-812*

*The system shall allow user to type a date of MM/DD/YYYY format for those date type filters.*

SRD-813

For all reports in which Configuration Names are displayed, the system shall allow the user to select the Configuration Name to view the items within the configuration.

NOTE: The affected reports include: Named Configuration Report, Device Current Configuration Report, Device Historical Configuration Report, and Where Used Report.

*ID* : SRD-639 (CRITICAL)

The system shall control access to reports based on roles, permissions CoT, user type

#### Software Update Report

*ID*: SRD-238

Software Update Report: The system shall provide a report listing all software update service events.

Mandatory search filters:

* Device Type

Optional search filters:

* User Name, who performing the update
* Customer Name
* Country
* From Date, starting date of the date range
* End Date, end date of the date range
* Software Upgrade Status, software update result status

The header of the report shall display the following filter values:

* CoT
* Device Type
* Customer Name
* Country
* From Date, starting date of the date range
* End Date, end date of the date range
* Software Upgrade Status, software update result status

The body of the report shall display the following fields:

* Customer name
* Device serial number
* Software Update status (Pass/Fail/Download Only)
* # of Attempts, number of attempts
* Previous Software Version
* Current Software Version
* Date and Time of Software Update
* User performing the update
* Country

NOTE: The reported software version should be the version number of the package only. The report should not contain version numbers of individual software items within the package.

#### Software Audit Report

*ID*: SRD-814

Software Audit Report: The system shall provide an entry for both Software Audit by Device Type Report and Software Audit by CoT Report.

Mandatory search filters:

* Search Type, with options: Software Audit by Device Type Report(default search type) and Software Audit by CoT Report

*ID* : SRD-533 (HIGH)

Software Audit by Device Type Report: The system shall provide a report that shows the number of devices of a specified device type at each software version by customer by Country.

Mandatory search filters:

* Search Type with option setting as “Software Audit by Device Type Report”
* Device Type

Optional search filters:

* None

The header of the report shall display the following filter values:

* CoT
* Device Type
* Total # of Devices, Total number of devices in the world of this device type

This body of the report shall display the following fields:

* Country
* Customer Name
* Software Version
* # of Devices, Number of devices of the specified device type at the reported software version for the reported customer
* % Country, Number of devices of the specified device type at the reported software version for the reported customer as a percentage of total number of devices of the specified device type at the reported software version in the entire country
* % Overall, Number of devices of this device type at the reported software version for the reported customer as a percentage of total number of devices of the specified device type at the reported software version in all countries

NOTE: The reported software version should be the version number of the software package only. The report should not contain version numbers of individual software items within the package.

Note: Refer to Gateway 1513 for example of report layout.

NOTE: Refer to GW-3043 and 3044.

*ID* : SRD-534 (HIGH)

Software Audit by CoT Report: The system shall provide a report that shows the number of devices at each reported software version by customer for all device types in the selected CoT.

Mandatory search filters:

* Search Type with option setting as “Software Audit by CoT Report”

Optional search filters:

* None

The header of the report shall display the following filter values:

* CoT
* Total # of Devices, Total number of devices in the world of all device types within the selected CoT

This body of the report shall display the following fields:

* Device Type
* Country
* Customer Name
* Software Version
* # of Devices, Number of devices of a reported device type at the reported software version for the reported customer
* % Device Type, Number of devices of a reported device type at the reported software version for the reported customer as a percentage of total number of devices of the reported device type at the reported software version in the entire country
* % Overall, Number of devices of a reported device type at the reported software version for the reported customer as a percentage of total number of devices of the reported device type at the reported software version in the world.

NOTE: The reported software version should be the version number of the software package only. The report should not contain version numbers of individual software items within the package.

Note: Refer to Gateway 1513 for example of report layout.

#### Software Versions Report

*ID* : SRD-570 (GW\_RSS\_RQ\_55) (HIGH)

Software Versions Report: The system shall generate and display SW Versions by serial number Report.

NOTE: This report is about current software version of the device, not its history

Mandatory search filters:

* Device Type

Optional search filters:

* Country
* Customer Name
* Device Serial Number
* Software package name and version (only packages belonging to the selected device type should be listed in the drop down. And the filter shall be partially searchable. )
* Start Date, the starting date of the date range for Last date docked
* End Date, the ending date of the date range for Last date docked

The header of the report shall display the following filter values:

* CoT
* Device Type
* Country
* Customer Name
* Software package name and version
* Last date docked

This body of the report shall display the following fields:

* Country
* Customer Name
* Customer Address
* Device Serial Number
* Software package name and version
* Last date docked

NOTE: The reported software version should be the version number of the software package only. The report should not contain version numbers of individual software items in the package.

Refer to GW-3041.

#### Device Historical Configuration Report

*ID* : SRD-571 (GW\_RSS\_RQ\_142) (HIGH)

Device Historical Configuration Report: The system shall generate and display report of device historical configuration information.

Note: This report provides historical device configuration information data for a device serial number.

Mandatory search filters:

* Device Type
* Device Serial Number.

Optional search filters:

* None

The header of the report shall display the following filter values:

* CoT
* Device Type
* Device Serial number
* Current Customer Name
* Last date that device was docked

The body of the report shall display the following fields:

* Hardware Items : it can be expanded and show all sub-components
* Software Items : it can be expanded and show all sub-components
* Features Items: it can be expanded and show all sub-components
* Country Code, Country code in which configuration was reported
* Date configuration reported

#### Named Configurations Report

*ID* : SRD-660 (GW\_RSS\_RQ\_61) (HIGH) (Must Have)

Named Configurations Report: The system shall generate a report of all named configurations by device type.

Mandatory search filters:

* Device Type

Optional search filters:

* None

The header of the report shall display the following filter values:

* CoT
* Device Type

The body of this report shall include the following fields:

* Configuration Type (System, Hardware, Software, Feature)
* Configuration Name
* Warning Configuration Type (None, Incompatible Software, Incompatible Hardware, etc.)
* Hardware, software, or feature items in the configuration to include name, version, part number
* Configuration Status (Limited Release, In Production, Archived)

SRD-815

Named Configurations Report: The system shall export the Named Configurations Report as a file and not display the report on the Web UI.

#### Device Country Change Report

*ID* : SRD-664 (HIGH)

Device Country Change Report: The system shall generate and display a Device Country Change Report.

NOTE: This report shows the history of all changes made to a device’s country setting.

Mandatory search filters:

* Device Type

Optional search filters:

* User Name, User who changed the device country assignment
* From Date, starting date of Date range
* End Date, end date of Date range

The header of the report shall display the following filter values:

* CoT
* Device type
* User Name, User who changed the device country assignment
* From Date, starting date of Date range
* End Date, end date of Date range

The body of the report shall display the following fields:

* Device Serial Number
* Customer Name
* User Name, User id of user who changed the country code
* Date country code was changed
* Previous country (i.e. “changed from” country), shall display full county name and ISO country code
* Current country (i.e. “changed to” country) shall display full county name and ISO country code

NOTE: The full name of the country should be displayed and not just the country code.

#### Report Categories

*ID : SRD-640 (CRITICAL)*

Reports shall be organized by categories. Viewing of one or more report categories shall be assigned to each role and user type.

Report categories are:

a. Administrative Report Category

NOTE: Currently contains Audit Report, Training Report, User Activity Report

b. Alert Report Category

NOTE: Currently contains, Component Discrepancy Report

c. Device Report Category

NOTE: Currently contains Device Configuration Report, Service Records Report, Software Versions Report, Device Historical Information Report, Software Audit Report, Device Country Change Report, Named Configuration Report, Software Update Report, Device Feature Entitlement Report, Clone Report, Configuration Where used Report.

#### Audit Trail Report

*ID : SRD-1000 (CRITICAL)*

Audit Trail Report: The system shall provide a report of all activities performed on the system for a specific CoT.

Mandatory search filters:

* None

Optional search filters:

* User Name, User’s name
* Email Address, User’s email address
* Customer name
* Activity TypeFrom Date, starting date of Date range
* End Date, end date of Date range

The header of the report shall display the following filter values:

* CoT
* User Name
* Email Address, User’s email address
* Customer name
* Activity Type
* From Date, starting date of Date range
* End Date, end date of Date range

The body of the report shall display the following fields:

* User Name
* Customer Name
* Activity, User performing the activity
* Host Name, IP address from the computer where activity was performed
* Device Type, Device type on which activity was performed (where appropriate)
* Device Serial Number, Device serial number on which the activity was performed (where appropriate)
* Date & Time, Date and time at which activity was performed

#### Training Report

*ID* : SRD-726

Training Report: The system shall generate a report of all user training performed as a pre-requisite for granting software update permission to a user.

Mandatory search filters:

* Device Type

Optional search filters:

* Trainer, Trainer’s user id
* Trainee, Trainee’ user id
* Customer Name
* Status, status of training
* From Date, starting date of Date range
* End Date, end date of Date range

The header of the report shall display the following filter values:

* CoT
* Device Type
* Trainer, Trainer’s user id
* Trainee, Trainee’ user id
* Customer Name
* Status, Status of training
* From Date, starting date of Date range
* End Date, end date of Date range

The body of the report shall display the following fields:

* Customer Name
* User Name, User who was trained
* Date of Training, Date training was recorded
* User Name, User who performed the training
* Status, status of training

#### Component Discrepancy Report

*ID : SRD-1001*

Component Discrepancy Report: The system shall generate a report of all devices which reported a different hardware, software, or feature component than what was expected by the system.

Mandatory search filters:

* Device Type

Optional search filters:

* Customer Name
* Country
* Device Serial Number

The header of the report shall display the following filter values:

* CoT
* Device Type
* Device Serial Number
* Customer Name
* Country

The body of the report shall display the following fields:

* Device Serial Number
* Customer Name
* Component Name
* Component type (hardware, software, feature)
* Expected Part Number
* Actual Part Number
* Expected Version
* Actual Version

SRD-816

Component Discrepancy Report: The Component Discrepancy Report shall list only discrepancies that were created outside of the use of this system

NOTE: For example, using this system to update software should not result in a discrepancy reported for the changed software item.

#### Device Current Configuration Report

*ID* : SRD-728

Device Current Configuration Report: The system shall generate a report of the current configuration of all devices of a specific device type.

Mandatory search filters:

* Device Type

Optional search filters:

* Device Serial number
* Customer name
* Country
* Hardware Items
* Software Items
* Feature Items

The header of the report shall display the following filter values:

* CoT
* Device type

The body of this report shall include the following fields:

* Device serial number
* Customer name
* Hardware Items : it can be expanded and show all sub-components
* Software Items : it can be expanded and show all sub-components
* Features Items : it can be expanded and show all sub-components
* Country Code
* Date, Date configuration reported

#### Service Records Report

SRD-817

Service Records Report: The system shall generate a report of all service events performed to devices.

Mandatory search filters:

* Device Type

Optional search filters:

* Service Type, Service event type
* Country
* Customer Name
* Device Serial Number
* From Date, starting date of Date range
* End Date, end date of Date range

The header of the report shall display the following filter values:

* CoT
* Device Type
* Service Type, Service event type
* Country
* Customer Name
* Device Serial Number
* From Date, starting date of Date range
* End Date, end date of Date range

The content of this report shall display the following fields:

* Device Serial Number
* Customer Name
* User Name, User who performed the service event
* Date & Time, Date and time service event performed
* Service Type, Service event type
* Data
* Previous
* Current

SRD-818

Service Records Report: The service event types listed in the Service Records Report shall be limited to the service event types defined in SRD-170.

SRD-819

Service Records Report: The Service Records Report shall contain the following fields which are customized based on the service event type:

* Data
* Previous
* Current

Log Retrieval service event:

“Data” field contains name of the log retrieved

“Previous” field contains N/A

“Current” field contains N/A

Software Update service event:

“Data” field contains name of the software package installed

“Previous” field contains previous package software version

“Current” field contains current package software version

Device Discovery service event:

“Data” field contains N/A

“Previous” field contains N/A

“Current” field contains N/A

Device Registration service event:

“Data” field contains N/A

“Previous” field contains N/A

“Current” field contains N/A

Device Connection service event:

“Data” field contains N/A

“Previous” field contains N/A

“Current” field contains N/A

Configuration Update service event:

“Data” field contains name of new/changed component

“Previous” field contains previous version of changed component

“Current” field contains current version of changed component

Customer Information Changed service event:

“Data” field contains N/A

“Previous” field contains previous customer information

“Current” field contains current customer information

#### Clone Report

SRD-820

Clone Report: The system shall generate a report of a specified cloned entity and its relationships to other cloned entities. Relationships are parent, siblings, and children entities.

Mandatory search filters:

* Device Type
* Clone Name, the field can be searchable partially
* Clone Entity Type (hardware/software/feature item, or hardware/software/feature/system configuration)
* Clone Entity Status

Optional search filters:

* Clone Entity Status (Limited Release, In Production, Archived)

The header of the report shall display the following filter values:

* CoT
* Device Type
* Clone Name
* Clone Entity Type
* Clone Entity Status

The content of this report shall display the following parts with fields:

* *Specified clone*
  + *Clone name, Clone entity type, Clone entity status*
* *Parent~~s~~ of specified clone*
  + *Clone name, Clone entity type, Clone entity status*
* *Siblings of specified clone*
  + *Clone name, Clone entity type, Clone entity status*
* *Children of specified clone*
  + *Clone name, Clone entity type, Clone entity status*

NOTE: Cloned entity types are hardware/software/feature item or hardware/software/feature/system configuration.

NOTE: The report should be displayed in a tree-like structure format for each clone entity in rows, where any node in the tree can be expanded to show its relationships.

#### Configuration Where Used Report

SRD-821

Configuration Where Used Report: The system shall generate a report showing where a selected entity is used. Entities include hardware/software/feature items and hardware/software/feature configurations.

Mandatory search filters:

* Device Type
* Entity Name
* Entity Type (hardware/software/feature items and hardware/software/feature configurations.

Optional search filters:

* Entity Status (Limited Release, In Production, Archived)

The header of the report shall display the following filter values:

* CoT
* Device Type
* Entity Name
* Entity Type
* Entity Status

The body of this report shall display the following fields:

* Configurations Where Used (lists each configuration that contains specified entity including its type and status)
  + Entity Name
  + Entity Type
  + Entity Status

NOTE: The contents of the Configurations Where Used field are a list of every configuration in which the specified entity is contained. For example, if the specified entity is a software item, then the Where Used field would list each software and system configuration that contains the specified software item. If the specified entity is a hardware configuration, then the Where Used field would list each system configuration that contains the specified hardware configuration.

#### User Activity Report

SRD-1003

User Activity Report: The system shall provide a report listing all activities performed by a user.

Mandatory search filters:

* None

Optional search filters:

* User name
* User role
* Medtronic Employee (Yes/No)
* Customer Name
* Customer Account

The header of the report shall display the following filter values:

* User name
* User role
* Medtronic Employee (Yes/No)
* Customer Name
* Customer Account

The body of the report shall display the following fields:

* User name
* Activity performed
* Host name (IP address from which activity was performed)
* Device Type (where applicable for device related activities)
* Device Serial Number (where applicable for device related activities)
* Date & Time (that activity was performed)

SRD-1004

The system shall allow only users with User Management permissions or System Admin permissions to run the User Activity Report.

### Part 11 Compliance and Related Requirements

*ID* : SRD-134

The system shall be 21CFR Part 11 compliant to the extent that each upgrade record is considered an electronic record.

*ID* : SRD-135

The system shall not delete records or data rows that are part of the audit trail.

*ID* : SRD-136

The system shall mark data records as inactive when asked to delete them.

*ID* : SRD-299

Service records shall be time-stamped with network time on the server

Note: Required for Part 11 Section 7.1.8.1

*ID* : SRD-183

The system must have secure, computer generated, time stamped audit trails to independently record the date and time of operator entries and actions.

*ID* : SRD-184

Record changes shall append to previously recorded information

*ID* : SRD-185

Audit trails must be retained for as long as the underlying records as required for the records.

*ID* : SRD-186

Access to modify the system or records must be limited to authorized roles.

*ID* : SRD-300

The system shall allow selectable portions of the audit trail to be extracted into a transportable electronic format

Note: Required for Part 11 Section 6.5.13

*ID* : SRD-301

The system shall allow selectable portion of the audit trail to be printed

Note: Required for Part 11 Section 6.5.12

*ID* : SRD-302

The system shall allow selectable portions of the audit trail to be viewed

Note: Required for Part 11 Section 6.5.12

*ID* : SRD-303

Users shall be able to archive software packages on the server

Note: Required for Part 11 Section 6.5.8

*ID* : SRD-304

Users shall not be able to delete software packages from the server

Note: Required for Part 11 Section 6.5.8

*ID* : SRD-305

Users shall not be able to modify or delete service records

Note: Required for Part 11 Section 6.5.8

*ID* : SRD-306

When data is changed or deleted, all previous values shall still be electronically available

Note: Required for Part 11 Section 6.5.8

*ID* : SRD-307

The system shall protect the system date and time from unauthorized change

Note: Required for Part 11 Section 6.5.7

*ID* : SRD-308

Users shall not be able to disable the audit trail function

Note: Required for Part 11 Section 6.5.4

*ID* : SRD-309

The audit trail must be read-only

Note: Required for Part 11 Section 6.5.3

*ID* : SRD-310

The system shall protect records against intentional or accidental modification or deletion

Note: Required for Part 11 Section 6.4.1

*ID* : SRD-311

The system shall check for the expected device type connected before allowing software updates

Note: Required for Part 11

*ID* : SRD-312

The system shall be capable of generating all the service records electronically in a format that can be put on a portable medium or transferred electronically

Note: Required for Part 11 Section 6.2.3

*ID* : SRD-313

The system shall allow a user to print the entire contents of service records

Note: Required for Part 11 Section 6.2.2

*ID* : SRD-314

The system shall allow a user to view the entire contents of service records

Note: Required for Part 11 Section 6.2.1

### Gateway Agent Installer Requirements

*ID* : SRD-432

The system shall provide an installation tool to install the Gateway Agent and its dependent packages.

ID: SRD-796

Note:. Implement new strategy for warning user if disk space will be exceeded during system operation.

*ID* : SRD-433

The installation tool shall be a single executable program.

*ID* : SRD-434

The installation tool shall run on 32/64 bits Windows XP SP3/Windows 7 Operating Systems.

*ID* : SRD-435

The installation tool shall provide a UI to guide the installation of the Gateway Agent.

*ID* : SRD-441

The Agent installation tool shall ensure availability of at least ~~25~~ 9 GB disk space before installing the Gateway Agent.

ID SRD: 797

Agent installer shall display an error message and stop installing ~~if~~ ~~admin privilege does not exist~~ if user doesn’t have windows admin privilege to do the installation.

### Recommended Requirements for Client Application Installer

Note: These are not Gateway system requirements.

*ID* : SRD-437

The system shall provide an installation tool to install the Client Application and its dependent packages.

*ID* : SRD-438

The installation tool shall be a single executable program.

*ID* : SRD-439

The installation tool shall run on 32/64 bits Windows XP SP3/Windows 7 Operating Systems.

*ID* : SRD-440

The installation tool shall provide a UI to guide the installation of the Client Application.

### Common Client related Requirements

*ID* : SRD-691

The system shall return all devices of a specific facility via agent.

*ID* : SRD-718

System shall have ability to configure the following attributes to device level:

* Enable/disable features through command or license file

Currently Common Client UI does have a button to apply feature license file on a device.

*ID* : SRD-719

The system shall provide a way to let client get timestamp of last uploaded log file for a given device

*ID* : SRD-720

The system shall make it configurable to the given device type for allowing delete log file or not after each time log file is retrieved.

Log file is deleted from device after Common Client pull the log file out of it.

*ID* : SRD-730

The system shall have user activity status report

Search criteria: user name, user email, time

Results:

HEADER: refer to SRD-223, SRD-225

BODY: User ID, Customer Name, Customer Account number, Activity, Host IP, Device Type, Serial Number, Day & Time

*ID* : SRD-735

The system shall allow client to upload/download user activities to/from the Server..

*ID* : SRD-750

When downloading to Agent, the system shall provide download completion percentage of the completion.

*ID* : SRD-751

GDMP Agent shall allow multiple users to sign on concurrently.

*ID* : SRD-755

The system shall support decoding binary format device log files retrieved from device.

*ID* : SRD-757

The system shall allow user to search Device log file by criteria via web UI (time duration, device type).

*ID* : SRD-758

The system shall make the duration to locally cache device log file configurable

Note:

Expired log files shall be removed from local cache unless it is not yet uploaded to GDMP.

*ID* : SRD-761

The system shall enable a user to view the complete feature list of a given device along with and enabled feature list.

*ID* : SRD-762

The system shall support distribute files (configuration, Software/Hardware package, feature licensing) in streaming approach to downstream client applications.

*ID* : SRD-765

Agent shall cache user activities from Common Client. The period of how long user activities cached in Agent shall be configurable.

*ID* : SRD-790

All files transferred between Agent and Common Client shall be in memory or over the network, no decrypted file is allowed during the transfer process.

### Trade Embargo

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

ID : SRD-397

The system shall provide a means to track countries where trade embargo prohibits devices to be installed or sold.

NOTE: Refer to Section 7.2.1.5, Device Embargo Permission.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

ID : SRD-398

The system shall only provide software to countries where no trade embargo exists.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

### Device Hardware

ID : SRD-694

Hardware shall not be deleted (archived) if there is a software associated with it.

ID : SRD-695

System shall allow CoT Admin user to associate documents with hardware in order to provide instructions or information to the end users.

ID : SRD-698

System shall allow user to view the named system/hardware/software/feature configurations that are associated with selected hardware..

Note: This is applicable for device types that support named configurations.

ID : SRD-699

System shall allow user to clone existing hardware item in order to create new hardware item.

ID : SRD-700

System shall allow user to see the clone map of hardware items , such as parent, siblings, and children.

ID : SRD-701

System shall allow CoT Admin user to be able to create hardware item with information including: hardware name, device type, Part#, Revision, Description, Hardware Type and Status.

ID : SRD-702

System shall allow CoT Admin user to be able to edit an existing hardware item based on below rule.

| **Entity** | **Status** | **Fields Which Can be Edited** | **Fields Which Cannot be Edited** |
| --- | --- | --- | --- |
| **Hardware Item** | Unknown | Description | Name |
|  |  | Hardware Type | Part Number |
|  |  | Status | Revision |
|  |  | Associated Documents | Device Type |
|  |  |  |  |
|  | Limited Release | All fields can be edited unless formerly In Production. If formerly In Production, then only fields that can be edited In Production can be edited | |
|  |  |  |  |
|  | In Production | Description | Name |
|  |  | Hardware Type | Part Number |
|  |  | Revision | Device Type |
|  |  | Status |  |
|  |  | Associated Documents |  |
|  |  |  |  |
|  | Archived | Description | Name |
|  |  | Status | Part Number |
|  |  |  | Revision |
|  |  |  | Device Type |
|  |  |  | Hardware Type |
|  |  |  | Associated Documents |

ID : SRD-703

System shall allow CoT Admin user to be able to track status of hardware as in ”Limited Release”, “In Production” or “Archived”.

ID : SRD-704

System shall allow administrator user to transit status of hardware as below:

Unknown  -> Limited Released, In Production  
Limited Release -> In Production, Archived  
In Production -> Archived, Limited Release  
Archived -> Limited Release , In Production

ID : SRD-705

System shall allow user to search hardware by hardware name, or device type, or hardware type.

* + 1. **Gateway Log -Viewer Requirements**

*ID* :  SRD- 900 (SSRD46)

The Gateway Log Viewer shall provide a link for users to view and download device logs in device log viewer page.

ID: SRD-901

The Gateway Log Viewer shall provide a means for users to filter the Log Viewer list by log type.

ID: SRD-902

The Gateway Log Viewer shall provide a means for users to filter the Log Viewer list to display the logs for a particular service date

ID: SRD-903

The Gateway Log Viewer shall provide a means to disable download and/or view for specified log types in the Log Viewer list by CoT as detailed below.

**Vessel Sealing**

**Valley Lab FT10 –** RFData, RFID, Debug (disable download or view on UI)

**Stapling**

**Signia –** Device Onewire, EventLog (disable view on UI, Allow download from link)

*ID* : SRD-1026

FT10 SW Discrepancy Shouldn't Compare Part Numbers

### UI Validation

ID : SRD-793

Data input on UI shall be validated. The field should include:

1. User Name: no special character is allowed
2. Email: follow email format
3. Role name: only alphabet, number ,‘\_’,’&’, ‘/’and blank are allowed
4. Date: MM/DD/YYYY
5. Account Number: only Number
6. Serial Number: Number + Alphabet
7. File Name: No special character is allowed
8. Hardware/Software Name: No special character is allowed
9. Part Number: Number+Alphabet+’-’
10. Revision number: Number+Alphabet+’.’+’\_’+’-’

Note: refer to GW-3145

## Operational Requirements

### Operating Location

*ID* : SRD-239

The system shall operate in environments where network connectivity may be compromised.

Note: This is the source of the disconnected operational modes for the gateway agent and the store and forward strategy.

*ID* : SRD-240

The system shall operate - across the globe where connectivity to world-wide-web is available.

Note: This is the other reason for a store and forward strategy, to provide robustness in uncertain environments.

*ID* : SRD-241

The system shall operate in Medtronic office spaces across the globe.

### Geography / Language

*ID* : SRD-244

The system shall provide an English user interface.

## Reliability Requirements

### Reliability Requirements

*ID* : SRD-275

The cloud host solution shall have a 99.9% system uptime SLA.

*ID* : SRD-271

The data shall be backed up at all times.

*ID* : SRD-272

The system shall have a 100% data recovery strategy.

Note: This informs the architecture and SRD

### Performance and Scalability Benchmarks (Gateway 1601)

(Note- 1: these assume availability of internet connection with minimum 2 Mbps throughput

Note- 2: These are benchmark guidelines that the system will aim to attain. The system may or may not be able to meet these benchmarks. The testing for these benchmarks will be done through out the product life cycle and may or may not be done as part of formal system testing)

*ID* : SRD-277

Web pages should return to the client in 2 seconds on average with a standard deviation of less than 1 second within North America and EMEA except for running reports.

Note: Due to nature of report queries, a set time limit cannot be established for running reports, but typically the report should return in 3 minutes or less.

*ID* : SRD-278

The system should be able to upload 40 MB log files from the gateway agent to the server within 3 minutes with a standard deviation of 30 seconds.

*ID* : SRD-279

The system should be able to download 10 MB software files to the gateway agent from the server within 1 minute with a standard deviation of 20 seconds.

# Schedule B

*ID* : SRD-280

The agent shall run on the following operating systems:

Windows 7 both 32/64 bit platforms

Windows 8 64 bit platforms

Windows 10 64 bit platforms

# Schedule C

*ID* : SRD-281

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

PB980 Series Ventilator

SCD 700 Sequential Compression Device

Valleylab Ligasure 10 (VLLS10)

Valleylab ForceTriad 10 (VLFT10)

Emprint Procedure Planning Application

Signia Stapler

# Schedule D

*ID* : SRD-413

The pc/laptop hosting the Gateway Agent shall have the following minimum requirements:

-RAM: 4 GB or better

-Hard disk available space: 9 GB or better

-Processor: Intel i5, or better

-Ethernet and/or wireless port

-Additional RAM, hard disk space, ports as needed by Client Application requirements

*ID* : SRD-772

Agent shall be able to run under Java 8.

Note: refer to GW-3144

# Schedule E

*ID* : SRD-528

The system shall be compatible to work with following browsers:  
  
IE v 11 and later   
Safari OSX v 6.1 and later   
Mozilla Firefox v 10 and later

Chrome v33 and later

# Business Rules

SRD-476

This section contains clarifying text for the above requirements. Such text details the logic that implements the requirements.

## Agent Rules

### Server Status Check

Refer to SRD-442

Upon startup, Agent sets server availability status to not available.

Agent always returns server availability status immediately to Client.

There is no waiting for the check to complete.

IF server status NOT EQUAL TO available  
THEN

Set server availability check to every 5 seconds.

ELSE

Set server availability check to every 3 minutes.

Rationale is that if the server is not available, the reason is likely that there is no physical connection to the internet, and so there will be little impact on either customer or Medtronic equipment by checking frequently.

### Password Reset

Refer to SRD-447

1. The Agent will provide a message which the Client can send to the server.
   1. The server will email the user a link to the Forgot Password page on the server.
2. Change password is not allowed in disconnected mode.
3. In disconnected mode, user can enter Client Application with old password when the password is changed through Server WebUI.

## Common Rules

### Device Operations

#### Create Device and Logs Permission

Refer to SRD-409

Service can register user with these limited permissions.

IF (User Registered) THEN

User Upload Logs Permission = TRUE

User Create Device = TRUE

END

#### User Device Update Permission

Refer to SRD-344, 475

IF (User Training Record for Device) AND

(User Role Update Permission NOT EQUAL None)

THEN

User Device Update Permission = TRUE

ELSE

User Device Update Permission = FALSE

END

#### Device Warranty Permission

Requires Connected Mode?? Warranty data must be in device for disconnected mode???

Refer to SRD-450, SRD-451, SRD-452.

IF (CoT NOT EQUALS Ventilation) OR

((CoT EQUALS Ventilation) AND (Device warranty date is later than current date))

THEN

Device Warranty Permission = TRUE

ELSE

Device Warranty Permission = FALSE

END

#### Device Regulatory Permission

Refer to SRD-331, SRD-333.

IF (Device Country NOT IN Software Configuration Regulatory Exclusion List)

THEN

Device Regulatory Permission = TRUE

ELSE

Device Regulatory Permission = FALSE

END

#### Device Embargo Permission

Refer to SRD-397.

IF ((Device Country NOT IN Embargo Country List) OR

(Device Configuration CONTAINS Regulatory Exception) AND (Regulatory Exception EQUALS Device Country))

THEN

Device Embargo Permission = TRUE

ELSE

Device Regulatory Permission = FALSE

END

#### Update Device Software Allowed

IF (User Device Update Permission) AND

(Device Warranty Permission)

THEN

Update Device Software Allowed = TRUE

ELSE

Update Device Software Allowed = FALSE

END

#### Software Component Matching

Refer to SRD-449

The component name should not change from one software revision to another, only the part number and/or the revision number is allowed to change.

SwVersionMatch = FALSE

IF (Device EQUALS PB980)

THEN

FOR (All Sw in ConfigDb.SwCatalog[Device.Sw.Name])

IF (Sw.Version EQUALS Device.Sw.Version)

THEN

SwVersionMatch = TRUE

END

END

ELSEIF (Device EQUALS SCD700)OR(DEVICE EQUALS VLLS10) OR (Device EQUALS VLFT10) OR (Device EQUALS Emprint) OR (Device EQUALS Signia) NOTE: Add CoolTip, ForceTriad for v3.0

THEN

FOR (All Sw in ConfigDb.SwCatalog[Device.Sw.Name])

IF (Sw.Version EQUALS Device.Sw.Version) AND

(Sw.PartNumber EQUALS Device.Sw.PartNumber)

THEN

SwVersionMatch = TRUE

END

END

#### Device Update Software Selection

Refer to SRD-178, SRD-344, SRD-342

SELECT (All Software Applicable to Device Type)

WHERE (Update Device Software Allowed) AND

(Software Entitlement Permission) AND

(Device Regulatory Permission) AND

(Device Embargo Permission) AND

(

(

((Software Release NOT EQUAL Limited Release) AND

(User Install Permission EQUAL TO Entitle to Install SW)) OR

((User Install Permission EQUAL TO Entitle to Install SW + Install Latest Version SW Only) AND

(Software Version = Latest Release Version)) OR

((User Install Permission EQUAL TO Entitle to Install SW + Install Latest Version SW Only + Access Limited Release SW) AND

(Software Version = Latest Release Version)) OR

((Software Release EQUAL TO Limited Release) AND

(User Install Permission EQUAL TO Entitle to Install SW + Access Limited Release SW))

)

)

END

### Configuration Validation

Refer to SRD-458, SRD- 374

NOTE: For GDMP v2.1

devConfig = Retrieve device configuration from device or device record

IF (devConfig.HW INTERSECTS ConfigDB.HwCatalog[DeviceType]) AND

(devConfig.SW INTERSECTS ConfigDB.SwCatalog[DeviceType]) AND

(All ConfigDB(devConfig.SW) are associated with ConfigDB.HwCatalog(devConfig.HW))

THEN

ValidConfigurationStatus = TRUE

END

IF (devConfig.HW INTERSECTS ConfigDB.HwCatalog[DeviceType]) AND

(devConfig.SW INTERSECTS ConfigDB.SwCatalog[DeviceType]) AND

(Any ConfigDB(devConfig.SW) are not associated with ConfigDB.HwCatalog(devConfig.HW))

THEN

IF (DeviceType EQUALS VLLS10)

THEN

ValidConfigurationStatus = Invalid Configuration

ELSE

ValidConfigurationStatus = TRUE

END

END

IF (Any devConfig.HW NOT INTERSECTS ConfigDB.HwCatalog) OR

(Any devConfig.SW NOT INTERSECTS ConfigDB.SwCatalog)

THEN

IF (DeviceType EQUALS VLLS10)

THEN

ValidConfigurationStatus = Not all components found

ELSE

ValidConfigurationStatus = TRUE

END

END

IF (ALL devConfig.HW NOT INTERSECTS ConfigDB.HwCatalog) AND

(ALL devConfig.SW NOT INTERSECTS ConfigDB.SwCatalog)

THEN

ValidConfigurationStatus = No components found

END

**For GDMP 3.0 with named configuration**

If there isn’t warning message after matching configuration, then running configuration from device is valid. Logc of matching is described below (physical implementation can be different, but logic input and output should be the same):

* Compare running config collected from device and named system config pulled from server. For a named system config, if all HW items inside it appeared in running config, then put it in matched-config candidate list
* Sort the candidate list. By using the <comparison\_order> number. Higher order number will result in higher position in candidate list. (so SW item with highest comparison order will be the first matched config, which will be treated as “latest” by client)
* Compare running config and warning-configs, prepare warning string if there is any.
* Scan the candidate list. for each named system config in this list, if running config’s country matches any regulatory exclusion in it, then remove it from candidate list and prepare warning message.
* Generate response with matched-config list and warning info.
* Note: For hardware component match of Emerald, ForceTraid, CoolTip and Orion, hardware revision number should be ignored.

## Server Rules

### User Registration

#### Training Record

IF (CoT EQUALS Compression)

THEN

Training Documentation must be uploaded

END

### Device Customer Name and Country

Refer to SRD-336, SRD-337.

NOTE: New details for v3.0 are listed in Gateway-1368.

Device Exists in Database:   
1. If ETL is received for the device   
If current Customer name == “Unknown Customer”, then replace with ShipTo Customer data from ETL   
If current Customer name <> “Unknown Customer”, then ignore ETL

1. Always replace the device’s Country with the Country sent by the client, regardless of who docks the device.
2. If MDT user docks a device, then do not change device's Customer name.

4. . If non-MDT user of type “services a single Medtronic customer” docks a device, then replace device's Customer name with user's Customer name [Compression, Ablation, Vessel Sealing]

5. . If non-MDT user of type “services multiple Medtronic customers” docks a device, then do not replace device’s Customer name with user’s Customer name   [Compression, Vessel Sealing, Ablation].

5. If non-MDT user docks a device, then do not change device's Customer name  [Ventilation]

6

7

### Named Configuration

NOTE: v3.0 Business Rule

IF (Number of Required HW Items Changes) OR (Part Numbers of HW Items Changes)

THEN

A new Named Configuration must be created

END

# Appendix

## Future/Deferred Requirements

*ID : SRD-470*

*The system shall be capable of supporting user interfaces in languages besides English as deemed necessary.*

*ID : SRD-723 (Deferred)*

*The system shall allow user to config "Auto update" flag per device type.*

*With the flag, the system shall update feature license files to update to device automatically.*

*ID* : SRD-600 @F

The Gateway Agent shall upload logs to the server before attempting to download packages.

*ID* : SRD-601c@F

The Gateway Agent shall delete logs which have been uploaded to the server.

*ID* : SRD-602 @F

The Gateway Agent shall determine space requirements prior to downloading packages.

*ID* : SRD-603 @F

If there is insufficient space to download requested package, the Gateway Agent shall respond with an error.

*ID* : SRD-604 @F

If the Agent was unable to download packages requested by the Client, the Agent shall respond with an error indicating so.

*ID* : SRD-AAAA @F (Need further discussion)

A non-Medtronic user who subscribes to an email notification will only receive notifications on operations performed to devices associated with his customer account.

*ID* : SRD-9478

By default, the system shall support the following role-based user permissions:

Warranty Expiration Date: View/Edit – entitled to view or modify device warranty expiration dates. (LOW)

NOTE: v3.0 permissions changes

Machine Log-in: Yes/No- Log in credentials never expire (LOW)

*ID* : SRD-546 (Gateway 1694) (LOW)

The system shall provide a means for a user with User Admin permissions to designate a user credential as being a machine login.

*ID* : SRD-547 (Gateway 1694) (LOW)

The system shall not check the expiry date of user login credentials which are designated as a machine login.

*ID* : SRD-526 (Gateway 1242) (LOW)

The system shall notify by email that the user's password is expiring in 5 days prior to the expiry date.

*ID* : SRD-613 (Gateway 1377) (LOW)(Deferred)

The system shall support the following non-Covidien user roles:

* 1. Hospital employee (ex: biomed)
  2. Medtronic contractor
  3. Hospital contractor
  4. DME
  5. DME contractor
  6. Distributor
  7. Distributor extensions
  8. Limited access user (can be either Medtronic or non- Medtronic user)

NOTE: 1. DME has the same permissions as a hospital employee/biomed

1. DME Contractor has same permissions as hospital contractor
2. Distributor has the same permissions as a hospital employee/biomed and a hospital contractor

*ID* : SRD-614 (Gateway-1377) (LOW)

The system shall support allowing one or more customer account numbers associated with a non- Medtronic user

*ID* : SRD-525 (Gateway 1215) (LOW)

The system shall use the selected Class of Trade to determine which device types can be accessed on Web UI pages.

*ID* : SRD-524 (Gateway 1079) (LOW)

The system shall provide a means to store on the server a user’s training record attachment which is the proof of training.

*ID* : SRD-535 (LOW)

The system shall allow users without training certification on a specific device type to be able to upload device configurations from a connected device of that device type.

*ID* : SRD-536 (LOW)

The system shall allow users without training certification on a specific device type to be able to create a new device of that device type in the database by connecting it.

*ID* : SRD-537 (LOW)

The system shall allow users without training certification on a specific device type to be able to set a country code in a device of that device type using clients that support this capability.

*ID* : SRD-538 (LOW)

The system shall not allow users without training certification on a specific device type to perform a software update on a device of that device type.

*ID* : SRD-545 (Gateway 1676) (LOW)

The system shall provide a means for the *Client Application* (not a user) to obtain Client-specific data (packages, rules, documentation) during a non-authenticated session with the Agent.

Note: Non-authenticated session means the session before a user logs-in.

*ID* : SRD-616 (Gateway 1377) (LOW)

In the case where a docked device already exists in the database, the association of a device to a customer account made when a non- Medtronic user docks a device shall be dependent on role. These rules shall be configurable per CoT.

Defaults are:

* 1. Biomed: Docked device is assigned to customer account associated with user’s profile
  2. Medtronic contractor: Docked device’s customer account is not changed unless user enters customer account number through client
  3. Hospital contractor: Docked device’s customer account is not changed unless user enters customer account number through client
  4. DME: Docked device’s customer account is not changed unless user enters customer account number through client
  5. DME contractor: Docked device’s customer account is not changed unless user enters customer account number through client
  6. Distributor: Docked device’s customer account is not changed unless user enters customer account number through client
  7. Distributor extensions: Docked device’s customer account is not changed unless user enters customer account number through client

NOTE: These default rules assume that all non- Medtronic users except Biomeds have multiple customer accounts and that they will not be expected to enter an account number through the client.

*ID* : SRD-617 (Gateway 1377) (LOW)

In the case where a docked device does not already exist in the database, the system shall implement the following rules when a device is docked by a non- Medtronic user. These rules shall be configurable per CoT.

* 1. If the user is associated with a single customer account, then the newly created device will be associated with the customer from the user’s profile.
  2. If the user provides a customer account through the client, then the newly created device will be associated with the customer provided through the client.
  3. Otherwise, the newly created device will be associated with Unknown customer.

*~~ID~~* ~~: SRD-493 (LOW)~~

~~The system shall allow a user with appropriate permissions to add and modify customer account name and/or number stored on the server.~~

*~~ID~~* ~~: SRD-494 (LOW)~~

~~The CoT admin is allowed by default to modify customer account name and/or number on the server.~~

*ID* : SRD-490 (Gateway 997) (LOW)

The system shall allow a user with appropriate permissions to modify device warranty expiration dates.

*ID* : SRD-491(Gateway 997)(LOW)

The CoT admin is allowed by default to change device warranty expiration dates..

*ID* : SRD-450 (Gateway-873) *( THIS WAS REMOVED FROM REV K (REGRESSION) AND PUT BACK IN L (3.0))(LOW)*

The system shall have the capability to prevent software from being installed on devices not under warranty or service contract by non- Medtronic users.

*ID* : SRD-451 (Gateway-873) *( THIS WAS REMOVED FROM REV K (REGRESSION) AND PUT BACK IN L (3.0))(LOW)*

The capability to prevent delivery of software to the client by the gateway agent for devices not under warranty or service contract shall be determined according to pre-configured business rules for a device type.

NOTE: Refer to 7.2.1.3, Device Warranty Permission.

Compression / Vessel Sealing CoT allows devices to be updated regardless of warranty coverage.

*ID* : SRD-452 (Gateway-873) *( THIS WAS REMOVED FROM REV K (REGRESSION) AND PUT BACK IN L (3.0))(LOW)*

The Gateway Server shall provide a user interface to allow a Medtronic user with sufficient role privileges to exclude software package from the no warranty/no installation behavior.

NOTE: To be used in the event of recall, one time software update, etc.

NOTE: Refer to 7.2.1.3, Device Warranty Permission.

*ID* : SRD-453 (Gateway-873) (LOW)

The Gateway Server shall provide an interface to allow a Medtronic user with sufficient role privileges to exempt a specific device from the no warranty/service contract exclusion.

*ID* : SRD-320 ( THIS WAS REMOVED FROM REV K (REGRESSION) AND PUT BACK IN L (3.0)) (LOW)

The system shall have capability to prevent a non- Medtronic user from accessing documents for devices that are not under warranty or service contract.

*ID* : SRD-460 (LOW)

The system shall provide a means by which the Client Application may request all known valid device configurations based on:

Device Type

*ID* : SRD-522 (Gateway 1054) (LOW)

The system shall return appropriate software list based on the device configuration sent by the Client.

Note: Typically, this will include updated software and current version software for roll-back, depending on user privileges.

*ID* : SRD-630 (Gateway 1054) (LOW)

The system shall automatically assign versions to named configurations.

*ID* : SRD-631 (Gateway 1054) (LOW)

When the user edits a named configuration through the WebUI, the system shall automatically increment its version number.

*ID* : SRD-632 (Gateway 1054) (LOW)

The system shall display only the latest version of a named configuration in the WebUI.

*ID* : SRD-574 (LOW)

The system shall provide an alert creation, update and delete interface.

*~~ID~~* ~~: SRD-575 (LOW)~~ (DUPLICATE OF 214)

~~The system shall provide the ability to define content of messages associated with an alert.~~

*ID* : SRD-641

The system shall limit a non- Medtronic user to the following criteria when running reports:

1. The report will include information for a single Customer account, which is selected by the user. The Customer account list will be limited to customers associated with the user.

NOTE: Report includes all devices from all CoT(s) associated with the customer, regardless of which user performed the service.

1. The report will include information for every device that the user has serviced, regardless of Customer account. (DEFER)
2. This limitation applies only to Non- Medtronic users

NOTE: Report includes all devices for which the user was the last person to service.

*ID* : SRD-528

The system shall be compatible to work with following browsers:  
  
  
iOS v 7.0 and later (LOW)  
  
Google Chrome v 33 and later (LOW)

**Requirements Deferred from GW v3.0**

(3.1.21) Orion Specific Configuration Management Requirements

(3.1.22) Named Configuration

*ID* : SRD-633 (Gateway 1054) (HIGH)

The system shall allow a user to clone an existing named configuration and rename it to create a new named configuration.

* + 1. **Feature Licensing**

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

ID : SRD-551 (CRITICAL)

The system shall provide a list of licensed features to the client for a connected device in online mode. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

ID : SRD-552 (CRITICAL)

The system shall provide a list of last known actually enabled features to the client for a connected device in online mode. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

ID : SRD- 659 (CRITICAL)

The system shall provide notification to the Client regarding whether the docked device has the SW required to enable the feature.

*~~ID~~* ~~: SRD-629 (Gateway 1054)(HIGH)~~

~~If a configuration sent to the server from the agent is not found in the database, then the system shall report the state of the configuration as “Unknown”.~~

(3.1.29) Reporting

*ID* : SRD-568 (GW\_RSS\_RQ\_51) (HIGH)

The system shall generate and display a report of alert events by device serial number.

Mandatory search fields are “Date Range”, and/or “Serial Number”, and/or “Reason for Alert” code (must supply at least one of these).

This report shall include the following fields:

• Device S/N

• Reason for Alert Code

• Date

*ID* : SRD-569 (GW\_RSS\_RQ\_58) (HIGH)

The System shall generate and display a report of users against the device serial number which they have worked on.

Mandatory search fields shall be of following type: (Device Type) AND (Username OR Country)

This report shall include the following fields:

* User login User ID
* User name
* User type
* Device Type
* Device Serial Number
* System configuration
* User assigned country
* Device Region

*ID* : SRD-609 (GW\_RSS\_RQ\_67) (HIGH)

The system shall generate and display SW Catalog Report by Device Type.

This report shall include the following fields:

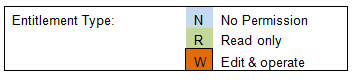
* Device Type
* Software Name and Version
* Software Part Number
* Status
* Country(ies) Excluded

(3.1.6) Limited User Access Related Requirement

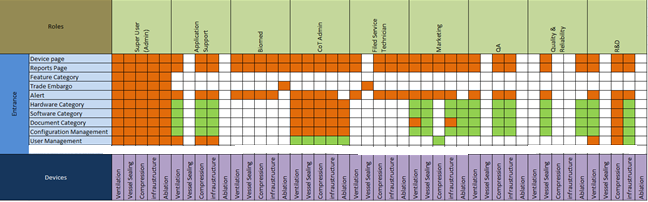
*ID* : SRD-401

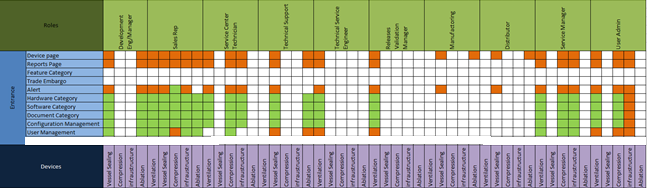
The user shall view the Service Manual in the PDF Viewer only if they are associated with a customer account which has a device under warranty

## Roles and Entitlements Matrix



Note: The following Matrix only shows default permission of WebUI Category per role per CoT.





## Access rights and Operation

Device Access Type: Entitle to install SW

Access Latest Version SW

Access In Production SW

Access Limited Release SW

Entitle to install Feature License

Access In Production Feature License

Access Limited Release Feature License

