**Medtronic Emerging Markets**

**Research & Development**

**System** **Requirements** Traceability Matrix

**Device Management Platform v4.0**

|  |  |  |  |
| --- | --- | --- | --- |
| Issue Date: Refer to Agile | | | Page 1 of 146 |
|  | | | |
| Revision History: | | | |
| Revision | SDA | Description | |
| A | RC086302 | Initial Release for Gateway v4.0 | |
|  |  |  | |
|  |  | | |
| Author(s): Refer to Agile for approvals | | | |
| *Mirror Wang* – InsigmaUS QA [Manual Approval] | | | |
|  | | | |
| **Approvals:** Refer to Agile for approvals | | | |
| *Paul Ourada – System Architect* | | | |
| *Maureen Richard – Product Owner* | | | |
| *Ashwini Pandey – MI Program Manager* | | | |
| *Cliff Schorr – QA, PMR* | | | |

**RE00062808 Rev A**

Table of Contents

[1 Overview 3](#_Toc458775886)

[1.1 Scope 3](#_Toc458775887)

[1.2 Responsibilities 3](#_Toc458775888)

[1.3 Reference 3](#_Toc458775889)

[2 Requirements Traceability Matrix 4](#_Toc458775890)

[2.1 Description of Matrix Fields 4](#_Toc458775891)

[2.2 Requirements Traceability Matrix 5](#_Toc458775892)

# Overview

This document is the System Requirements Traceability Matrix document for Gateway v 4.0.

## Scope

The requirements traceability matrix is used to trace project life cycle testing activities and working efforts to the project requirements. The matrix establishes a thread that traces between requirements and all test procedures.

## Responsibilities

The requirements traceability matrix will be maintained by the InsigmaUS Testing Team.

## Reference

1. R0030891 System Requirements Specification (SRS), Rev S
2. RE00062907\_Revision\_A\_System\_Install\_Qual\_(IQ)\_Gateway\_4 0
3. R0036601 Data Backup Strategy & Procedure Gateway
4. R0042328 Report Cloud System Security Setup Gateway
5. RE00062810\_Revision A\_System\_Verification\_Plan\_Gateway\_4\_0
6. R0054299\_B\_PLAN\_PROC Verification Connection\_Tool\_v4.0
7. RE00003668\_A\_Redline\_ B\_PROC End\_to\_End\_Test Emerald Orion Gateway v4.0
8. R0037808\_D\_Redline\_E\_PROC\_End-End\_Test\_System\_SCD700\_Gateway\_v4.0R0035793, Database Validation Test Plan and Procedure Gateway; Rev B
9. R0020235\_D\_ Redline\_E\_System\_End\_to\_End\_Test\_Proc\_PB980 Gateway 4.0 RE00055296\_A\_Redline\_B\_PROC End\_to\_End\_Test Signia Gateway v4.0; Rev A
10. RE00068285\_B\_System\_Test\_Procedure\_Gateway\_v4.0
11. \*GDMP SysOps Guide
12. RE00031461\_A\_Redline\_B\_PROC\_End to End\_Test\_Emprint Procedure Planning Application\_Gateway\_v4.0 Application\_Gateway
13. RE00026733\_B\_System\_Verification\_Procedure\_CC\_v1.0

**\* This document is available on the GDMP SysOps PulseConnect site in the Server Support Category**

Note: Unless specified with a version number, all documents will be referenced by their latest approved version in Agile.

# Requirements Traceability Matrix

## Description of Matrix Fields

This matrix show traceability of test procedures to the requirements. The requirements traceability matrix contain the following fields:

* **Requirements** - A unique identification number containing the System Requirements Specification (SRS) number of the requirement.
* **Requirement Description** - Detail description of System Requirements Specification (SRS) items.
* **Test Procedure** – Test Procedure list which covers requirement accordingly which includes test procedures
  + **\*Note:** 
    - **Script test procedures listed in [12] System\_Test\_Procedures**
* **Notes** – Comments related with specific trace activities.

**Note**:

* Security and Performance are not in the testing scope, as it is non-functional requirement.
* Common Client is also not in the scope of this test, it will be covered in Common Client project integration test phase.
* Some of Feature License cases will be tested together with CC in Common Client project integration test phase.

## Requirements Traceability Matrix

| **Requirements** | **Requirement Description** | **Test Procedure** | **Notes** |
| --- | --- | --- | --- |
| **3.1.1       User Login** | | | |
| 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. | TC\_UserMgt\_008.1  TC\_UserMgt\_008.2  TC\_UserMgt\_008.3  TC\_UserMgt\_008.4 |  |
| SRD-38 | The system shall support user authentication via the web interface. | TC\_UserMgt\_008.1  TC\_UserMgt\_008.2  TC\_UserMgt\_008.3  TC\_UserMgt\_008.4 |  |
| SRD-39 | The system shall prompt with user-name and password credentials. | TC\_UserMgt\_008.1  TC\_UserMgt\_008.2  TC\_UserMgt\_008.3  TC\_UserMgt\_008.4 |  |
| 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 & < > / ' " | TC\_UserMgt\_006.1  TC\_UserMgt\_006.2 |  |
| SRD-46 | System shall support username and password authentication. | TC\_UserMgt\_008.1  TC\_UserMgt\_008.2  TC\_UserMgt\_008.3  TC\_UserMgt\_008.4 |  |
| SRD-47 | The system shall support user authorization. | TC\_UserMgt\_008.1  TC\_UserMgt\_008.2  TC\_UserMgt\_008.3  TC\_UserMgt\_008.4  TC\_UserMgt\_009.1  TC\_UserMgt\_009.2  TC\_UserMgt\_009.3  TC\_UserMgt\_009.4 |  |
| SRD-48 | The system shall support role based authorization. | TC\_UserMgt\_008.1  TC\_UserMgt\_008.2  TC\_UserMgt\_008.3  TC\_UserMgt\_008.4 |  |
| 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 | TC\_RolePermission\_001.1  TC\_RolePermission\_001.2  TC\_RolePermission\_001.3  TC\_RolePermission\_001.4  TC\_RolePermission\_001.5 |  |
| 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. 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 | TC\_RolePermission\_001.1  TC\_RolePermission\_001.2  TC\_RolePermission\_001.3  TC\_RolePermission\_001.4  TC\_RolePermission\_001.5 |  |
| SRD-50 | The system shall move to the ‘home’ screen if the user’s authentication and authorization test pass. | TC\_UserMgt\_008.1  TC\_UserMgt\_008.2 | |  | | --- | |  | |  | |
| SRD-51 | The system shall return to the login screen if the user’s authentication and authorization tests fail. | TC\_UserMgt\_008.3  TC\_UserMgt\_008.4 |  |
| SRD-52 | The system shall respond with a failed user login message. | TC\_UserMgt\_008.3  TC\_UserMgt\_008.4  TC\_UserMgt\_009.3  TC\_UserMgt\_009.4 |  |
| 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. | TC\_UserMgt\_008.3  TC\_UserMgt\_008.4  TC\_UserMgt\_009.3  TC\_UserMgt\_009.4 |  |
| 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 | TC\_UserMgt\_007.1  TC\_UserMgt\_007.2  TC\_UserMgt\_007.3  TC\_UserMgt\_007.4  TC\_UserMgt\_007.5  TC\_UserMgt\_006.1  TC\_UserMgt\_006.2 |  |
| 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. | TC\_UserMgt\_008.5 |  |
| SRD-56 | The system shall provide help desk contact information on the login page. | TC\_UserMgt\_008.5 |  |
| SRD-58 | The system shall log failed login attempts including time, username, and hostname/IP Address. | TC\_UserMgt\_008.3  TC\_UserMgt\_008.4  TC\_UserMgt\_009.3  TC\_UserMgt\_009.4  TC\_UserMgt\_009.9  TC\_UserMgt\_009.10 |  |
| 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. | TC\_UserMgt\_005.2  TC\_UserMgt\_005.3 |  |
| 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. | TC\_UserMgt\_005.3 |  |
| 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. | TC\_UserMgt\_005.2  TC\_UserMgt\_005.3 |  |
| SRD-462 | The system shall send notification email with link to change password upon completion of forgot password request. | TC\_UserMgt\_005.1  TC\_UserMgt\_005.2  TC\_UserMgt\_005.3 |  |
| SRD-472 | Gateway agent shall encrypt user credentials to allow disconnected log-in. | TC\_UserMgt\_009.7  TC\_UserMgt\_009.8 |  |
| SRD-670 | The system shall allow user to log out. | TC\_UserMgt\_008.7  TC\_UserMgt\_008.8  TC\_UserMgt\_009.1  TC\_UserMgt\_009.2 |  |
| SRD-671 | The system shall allow admin user to add facility information to the system database with the following information:  • Facility Name  • Facility Address  Facility Country | TC\_UserMgt\_010.1  TC\_UserMgt\_010.5 |  |
| SRD-672 | The system shall allow 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. | TC\_UserMgt\_010.2  TC\_UserMgt\_010.3 |  |
| SRD-673 | The system shall allow user with adequate privileges to view the complete list of customers and their associated facilities. | TC\_UserMgt\_010.4 |  |
| SRD-674 | The system shall allow admin user to add new customer to the system database with below information:  • Customer Account Number  • Customer Name  • Customer Address | TC\_UserMgt\_010.2  TC\_UserMgt\_010.3 |  |
| SRD-800 | After 3 failed login attempts, the user account will be locked. | TC\_UserMgt\_008.5  TC\_UserMgt\_009.5  TC\_UserMgt\_009.11 |  |
| SRD-803 | A user’s account shall be unlocked under one of the following conditions:   1. System Administrator or CoT Admin unlocks the account after verification. 2. The user waits a pre-configured lockout period (in minute) 3. The user resets password. | TC\_UserMgt\_008.6  TC\_UserMgt\_009.6  TC\_UserMgt\_009.12  TC\_UserMgt\_004.3  TC\_UserMgt\_005.5 |  |
| 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 | TC\_UserMgt\_001.3  TC\_UserMgt\_011.3 |  |
| **3.1.2       User Self Registration** | | | |
| SRD-588 | The System shall provide a means for the prospective new user (self-registrant) to request log in credentials. | TC\_UserMgt\_013.1  TC\_UserMgt\_020.1 TC\_UserMgt\_020.2  TC\_UserMgt\_013.5  TC\_UserMgt\_014.4  TC\_UserMgt\_011.8  TC\_UserMgt\_012.4 |  |
| SRD-589 | The system through Gateway Agent shall provide to the Client a link to the server webpage for new user self-registration. | TC\_UserMgt\_020.1  TC\_UserMgt\_020.2 |  |
| 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. | TC\_UserMgt\_011.7  TC\_UserMgt\_012.8 |  |
| 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 | TC\_UserMgt\_013.1  TC\_UserMgt\_013.2  TC\_UserMgt\_014.1  TC\_UserMgt\_014.2 |  |
| SRD-804 | System shall provide feedback to the registrant regarding status of the self-registration. | TC\_UserMgt\_013.1  TC\_UserMgt\_013.2  TC\_UserMgt\_014.1  TC\_UserMgt\_014.2 |  |
| SRD-591 | System shall automatically process the self-registration request. | TC\_UserMgt\_011.1  TC\_UserMgt\_012.1  TC\_UserMgt\_013.1  TC\_UserMgt\_014.1 |  |
| SRD-593 | System shall set registration request state to pending upon successful completion of new user registration form. | TC\_UserMgt\_013.1  TC\_UserMgt\_014.1 |  |
| SRD-594 | System shall use email notification to obtain authorization for pending registration from approving manager. | TC\_UserMgt\_013.1  TC\_UserMgt\_013.2  TC\_UserMgt\_014.1  TC\_UserMgt\_014.2 |  |
| SRD-595 | System shall set registration state to approved state upon receipt of authorization from approving manager. | TC\_UserMgt\_013.1  TC\_UserMgt\_014.1 |  |
| SRD-596 | System shall send an email to registrant with id and a link to a Gateway page where the user sets their password. | TC\_UserMgt\_013.1  TC\_UserMgt\_014.1 |  |
| SRD-597 | System shall send an email to the registrant, if the registration has been in process for 48 hours or greater. | TC\_UserMgt\_013.4 |  |
| SRD-598 | System shall send an email to Approving Manager/Proxy ~~the Gateway Support~~, if the registration has been in process for 48 hours or greater. | TC\_UserMgt\_013.4 |  |
| SRD-798 | The system shall allow approving proxy to approve non-Metronic user registration and approving manager to approve Medtronic user registration. | TC\_UserMgt\_014.1  TC\_UserMgt\_014.2  TC\_UserMgt\_014.3  TC\_UserMgt\_013.1  TC\_UserMgt\_013.2  TC\_UserMgt\_013.3 |  |
| 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. | TC\_UserMgt\_015.1 |  |
| SRD-679 | The system shall allow CoT Admin to check the status of registration approval progress of his CoT’s registration forms. | TC\_UserMgt\_017.1  TC\_UserMgt\_017.2  TC\_UserMgt\_017.3  TC\_UserMgt\_017.4 |  |
| 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. | TC\_UserMgt\_012.1  TC\_UserMgt\_012.2  TC\_UserMgt\_012.3  TC\_UserMgt\_012.4  TC\_UserMgt\_012.5  TC\_UserMgt\_012.6  TC\_UserMgt\_012.7  TC\_UserMgt\_012.8 |  |
| SRD-682 | The system shall provide directions so that a non- Medtronic registrant that does not know his customer information can obtain the required customer name for getting registered. | TC\_UserMgt\_012.1 |  |
| 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. | TC\_UserMgt\_011.1  TC\_UserMgt\_011.2  TC\_UserMgt\_011.3  TC\_UserMgt\_011.4  TC\_UserMgt\_011.5  TC\_UserMgt\_011.6  TC\_UserMgt\_011.7 |  |
| SRD-677 | The system shall allow Medtronic approving manager or proxy to authorize who will have access to the GDMP system for particular CoT. | TC\_UserMgt\_013.1  TC\_UserMgt\_013.2  TC\_UserMgt\_013.3  TC\_UserMgt\_014.1  TC\_UserMgt\_014.2  TC\_UserMgt\_014.3 |  |
| 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. | TC\_UserMgt\_011.4  TC\_UserMgt\_012.5 |  |
| 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. | TC\_UserMgt\_016.1  TC\_UserMgt\_016.2  TC\_UserMgt\_016.3 |  |
| SRD-1012 | The system should support self-registration for different device types: Valleylab LS10, Valleylab FT10, SCD700, PB980 and Emprint. | TC\_UserMgt\_011.1  TC\_UserMgt\_011.4  TC\_UserMgt\_011.5  TC\_UserMgt\_011.6  TC\_UserMgt\_011.7  TC\_UserMgt\_012.1  TC\_UserMgt\_012.5  TC\_UserMgt\_012.6  TC\_UserMgt\_012.7  TC\_UserMgt\_012.8  TC\_UserMgt\_011.8  TC\_UserMgt\_012.4 |  |
| **3.1.3 Users** | | | |
| SRD-59 | The system shall allow the creation of new users. | TC\_UserMgt\_001.1  TC\_UserMgt\_001.2  TC\_UserMgt\_001.3  TC\_UserMgt\_001.4  TC\_UserMgt\_002.1  TC\_UserMgt\_002.2  TC\_UserMgt\_002.3 |  |
| SRD-463 | The User Administrator role shall be able to add new users to the system. | TC\_UserMgt\_001.1  TC\_UserMgt\_001.2  TC\_UserMgt\_001.3  TC\_UserMgt\_001.4  TC\_UserMgt\_002.1  TC\_UserMgt\_002.2  TC\_UserMgt\_002.3  TC\_UserMgt\_003.1  TC\_UserMgt\_003.2  TC\_UserMgt\_003.3 |  |
| SRD-464 | The User Administrator role shall be able to modify user accounts in the system. | TC\_UserMgt\_004.1 |  |
| SRD-465 | The User Administrator role shall be able to delete user accounts in the system. | TC\_UserMgt\_004.2 |  |
| SRD-646 (CRITICAL) | The system shall support the following user types:  a. MentronicUsers b. Non- Medtronic users who are associated with a single Medtronic customer. c. Non- Medtronic users who are associated with multiple Medtronic customers. | TC\_UserMgt\_001.1  TC\_UserMgt\_002.1  TC\_UserMgt\_002.2 |  |
| SRD-62 | User Data shall include:  First Name Last Name Role/Title Login Name/Email Password Is Medtronic Employee Company Name Country  Language | TC\_UserMgt\_001.1  TC\_UserMgt\_002.1  TC\_UserMgt\_011.1  TC\_UserMgt\_012.1 |  |
| SRD-63 (HIGH) | Customer data shall include:  Customer Account Number Customer Name Customer Address | TC\_UserMgt\_010.2  TC\_UserMgt\_010.3  TC\_UserMgt\_010.4 |  |
| SRD-64 | The system shall identify the customer hospital, distributor or third-party a user works for if they are not a Medtronic employee. | TC\_UserMgt\_002.1  TC\_UserMgt\_002.2  TC\_UserMgt\_002.3 |  |
| 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. | TC\_RolePermission\_003.1  TC\_RolePermission\_003.2  TC\_RolePermission\_008.1 |  |
| SRD-67 | The system shall allow the disabling of user permissions based on role. | TC\_RolePermission\_003.1  TC\_RolePermission\_003.2 |  |
| SRD-68 | The system shall allow the assignment of user permissions to a role. | TC\_RolePermission\_003.1  TC\_RolePermission\_003.2 |  |
| 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 | TC\_Agent\_001.2  TC\_Agent\_001.4  TC\_Agent\_001.6  TC\_Agent\_001.8  TC\_Agent\_001.10  TC\_Agent\_001.12  TC\_Agent\_002.2  TC\_Agent\_002.4  TC\_Agent\_002.6  TC\_Agent\_002.8  TC\_Agent\_002.10  TC\_Agent\_002.12 |  |
| SRD-410 | The system shall join multiple concurrent log-ins by a single user from different machines into a single session. | TC\_UserMgt\_018.1 |  |
| 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. | TC\_UserMgt\_018.2 |  |
| SRD-318 | The system shall allow deactivating/re-activating a user. | TC\_UserMgt\_004.4  TC\_UserMgt\_004.5 |  |
| **3.1.4     Roles and Access Policies** | | | |
| SRD-70 | The system shall allow the creation of new roles. | TC\_RolePermission\_002.1  TC\_RolePermission\_002.2 |  |
| SRD-9997 | The system shall provide separate role schemes for MDT and non-MDT personnel.  NOTE: non-MDT roles include:  Biomed  Distributor  ThirdPartyService | TC\_RolePermission\_004.1  TC\_RolePermission\_004.2  TC\_RolePermission\_004.3 |  |
| SRD-9996 | The system shall provide only non-MDT roles for non-MDT personnel.  NOTE: For instance, the Self Registration Screen | TC\_RolePermission\_004.1  TC\_RolePermission\_004.2  TC\_RolePermission\_004.3 |  |
| SRD-9995 | The system shall provide only MDT roles for MDT personnel. | TC\_RolePermission\_004.2  TC\_RolePermission\_004.3 |  |
| 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. | TC\_RolePermission\_004.1  TC\_RolePermission\_004.2  TC\_RolePermission\_004.3 |  |
| SRD-9993 | The system shall provide a Limited Access role, which shall have a non-modifiable default device access permission of Default Dock Device. | TC\_RolePermission\_005.1  TC\_RolePermission\_005.2 |  |
| SRD-71 | The system shall assign the right to create new roles through the access policy. | TC\_RolePermission\_002.1  TC\_RolePermission\_002.2 |  |
| SRD-72 | Role Data shall include  Role Name Description | TC\_RolePermission\_002.1  TC\_RolePermission\_002.2 |  |
| SRD-73 | The system shall allow the editing of roles based on access policy. | TC\_RolePermission\_002.3 |  |
| SRD-74 | The system shall allow the deletion of roles based on access policy. | TC\_RolePermission\_002.4  TC\_RolePermission\_002.5 |  |
| SRD-75 | The system shall allow the assignment of access policies to roles. | TC\_RolePermission\_002.1  TC\_RolePermission\_002.2  TC\_RolePermission\_002.3  TC\_RolePermission\_003.1  TC\_RolePermission\_003.2 |  |
| SRD-76 | They system shall allow the review of users assigned to a role. | TC\_UserMgt\_019.1  TC\_UserMgt\_019.2 |  |
| SRD-77 | They system shall allow the review of access policies assigned to a role. | TC\_RolePermission\_001.1  TC\_RolePermission\_001.2  TC\_RolePermission\_001.3  TC\_RolePermission\_001.4  TC\_RolePermission\_001.5 |  |
| SRD-78 | The system shall define device types. (PB 980, ForceTriad, etc.) | TC\_UserMgt\_021.1  TC\_UserMgt\_021.2  Appendix B CoT and Device Type |  |
| SRD-79 | The system shall provide the ability to customize role regimes by Class of Trade. | TC\_RolePermission\_001.1  TC\_RolePermission\_001.2  TC\_RolePermission\_001.3  TC\_RolePermission\_001.4  TC\_RolePermission\_001.5 |  |
| 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 | TC\_Agent\_003.1  TC\_Agent\_004.1  TC\_Agent\_005.1  TC\_Agent\_006.1  TC\_Agent\_007.1  TC\_Agent\_008.1  TC\_Agent\_020.1  TC\_Agent\_020.2 |  |
| SRD-81 | All system users, agents, or tasks shall run under an access policy. | TC\_RolePermission\_006.1  TC\_RolePermission\_006.4  TC\_UserMgt\_008.1  TC\_UserMgt\_008.2  TC\_UserMgt\_009.1  TC\_UserMgt\_009.2  TC\_Agent\_003.1  TC\_Agent\_003.2  TC\_Agent\_004.2  TC\_Agent\_004.2  TC\_Agent\_005.1  TC\_Agent\_005.2  TC\_Agent\_006.1  TC\_Agent\_006.2  TC\_Agent\_007.1  TC\_Agent\_007.2  TC\_Agent\_008.1  TC\_Agent\_008.2 |  |
| SRD-82 | The system shall allow the creation of access policies. | TC\_RolePermission\_002.1  TC\_RolePermission\_002.2 |  |
| SRD-83 | The system shall allow the editing of access policies. | TC\_RolePermission\_002.3 |  |
| SRD-84 | The system shall allow the deleting of access policies. | TC\_RolePermission\_002.4  TC\_RolePermission\_002.5 |  |
| SRD-85 | The system shall log the use of access rights granted by the policies, except the viewing activity. | TC\_UserMgt\_008.1  TC\_UserMgt\_008.2  TC\_UserMgt\_008.3  TC\_UserMgt\_008.4  TC\_UserMgt\_009.1  TC\_UserMgt\_009.2 |  |
| SRD-86 | The system shall use access policies to manage access to administration activities. | TC\_UserMgt\_008.1  TC\_UserMgt\_008.2  TC\_UserMgt\_008.3  TC\_UserMgt\_008.4 |  |
| SRD-9999 | The system shall use access policies to manage access to devices. | TC\_UserMgt\_009.1  TC\_UserMgt\_009.2  TC\_UserMgt\_009.3  TC\_UserMgt\_009.4  TC\_RolePermission\_003.2 |  |
| 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. | TC\_UserMgt\_008.1  TC\_UserMgt\_008.2  TC\_RolePermission\_003.1 |  |
| SRD-88 | The access policies shall govern create rights across entities. | TC\_RolePermission\_001.1  TC\_RolePermission\_001.2  TC\_RolePermission\_001.3  TC\_RolePermission\_001.4  TC\_RolePermission\_001.5 |  |
| SRD-89 | The access policies shall govern read rights across entities. | TC\_RolePermission\_001.1  TC\_RolePermission\_001.2  TC\_RolePermission\_001.3  TC\_RolePermission\_001.4  TC\_RolePermission\_001.5 |  |
| SRD-90 | The access policies shall govern update rights across entities. | TC\_RolePermission\_001.1  TC\_RolePermission\_001.2  TC\_RolePermission\_001.3  TC\_RolePermission\_001.4  TC\_RolePermission\_001.5 |  |
| SRD-91 | The access policies shall govern delete rights across entities. | TC\_RolePermission\_001.1  TC\_RolePermission\_001.2  TC\_RolePermission\_001.3  TC\_RolePermission\_001.4  TC\_RolePermission\_001.5 |  |
| SRD-685 | The default permission of Feature Catalog for CoT Admin shall be "View & Edit" in Web UI. | TC\_RolePermission\_001.1  TC\_RolePermission\_001.2  TC\_RolePermission\_001.3  TC\_RolePermission\_001.4  TC\_RolePermission\_001.5 |  |
| 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. | TC\_RolePermission\_003.2  TC\_RolePermission\_008.1 |  |
| 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. | TC\_RolePermission\_008.1 |  |
| SRD-343 | Device access permission will be associated with a user and role profiles. | TC\_RolePermission\_003.2  TC\_RolePermission\_008.1 |  |
| 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 7.2.1.2, User Device Update Permission. Section 7.2.1.7, Software Component Matching , and Section 7.2.1.8, Device Update Software Selection | TC\_RolePermission\_003.2  TC\_RolePermission\_008.1  TC\_Agent\_003.1  TC\_Agent\_003.2  TC\_Agent\_004.1  TC\_Agent\_004.2  TC\_Agent\_005.1  TC\_Agent\_005.2  TC\_Agent\_006.1  TC\_Agent\_006.2  TC\_Agent\_007.1  TC\_Agent\_007.2  TC\_Agent\_008.1  TC\_Agent\_008.2 |  |
| 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. | TC\_RolePermission\_006.1  TC\_RolePermission\_006.4 |  |
| 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 | TC\_UserMgt\_009.1  TC\_UserMgt\_009.2  TC\_UserMgt\_009.3  TC\_UserMgt\_009.4 |  |
| SRD-687 | The system shall allow System Administrator to be able to manage a file extension white list ~~.~~  Note: This file extension white list refers to files that are allowed to be uploaded including software package, document and business rule. | TC\_RolePermission\_007.1  TC\_RolePermission\_007.2 |  |
| SRD-615 | 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) | TC\_RolePermission\_009.1  TC\_RolePermission\_009.2 |  |
| **3.1.5 User Training Related Requirements** | | | |
| SRD-338 | The system shall include a mechanism to identify a user that can train others. | TC\_UserMgt\_001.4 |  |
| SRD-339 | The system shall maintain a training record for all users including: Trainer Name Date of Training  Trainee Name Device Type | TC\_Report\_009.1  TC\_Report\_009.2  TC\_Report\_009.4  TC\_Report\_009.3 |  |
| SRD-340 | The system shall provide a means to view a user's training record. | TC\_UserMgt\_019.3 |  |
| SRD-341 | The system shall provide a means to view a list of training records for a particular device type. | TC\_Report\_009.1  TC\_Report\_009.2  TC\_Report\_009.4  TC\_Report\_009.3 |  |
| 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 | TC\_UserMgt\_004.6 |  |
| **3.1.6       Security Requirements** | | | |
| SRD-97 | The system shall operate through a secure port. | TC\_Security\_009.1 | Security test will be conducted by MDT Cyber Security Test Team on an ongoing basis. |
| SRD-115 | The system shall provide secure communication channels for sending data. | TC\_Security\_009.1  TC\_Security\_001.1  TC\_Security\_001.2  TC\_Security\_001.3 | Security test will be conducted by MDT Cyber Security Test Team on an ongoing basis. |
| SRD-116 | The system shall provide secure communication channels for receiving data. | TC\_Security\_009.1  TC\_Security\_001.1  TC\_Security\_001.2  TC\_Security\_001.3 | Security test will be conducted by MDT Cyber Security Test Team on an ongoing basis. |
| SRD-105 | The system shall encrypt the software manifest. | TC\_Security\_009.1 |  |
| SRD-416 | The gateway agent shall set a timer on each encrypted file in the cache and delete that file after the timer expires. | TC\_Security\_003.1  TC\_Security\_004.1  TC\_Security\_004.1 |  |
| SRD-417 | The gateway agent shall restart the timer every time the encrypted file in the cache is accessed. | TC\_Security\_003.1  TC\_Security\_004.1  TC\_Security\_004.1 |  |
| SRD-106 | The encrypted components of the package shall be decrypted prior to transferring it to Client Application. | TC\_Security\_006.1  TC\_Security\_006.2  TC\_Security\_006.3  TC\_Security\_006.4 |  |
| SRD-419 | The gateway agent shall delete the decrypted software package from laptop immediately on receipt of installation response message from the client application. | TC\_Security\_004.1  TC\_Security\_004.2  TC\_Security\_004.3  TC\_Security\_004.4 |  |
| 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. | TC\_Security\_003.1  TC\_Security\_003.2  TC\_Security\_003.3  TC\_Security\_003.4  TC\_Security\_003.5  TC\_Security\_003.6 |  |
| SRD-421 | The gateway agent shall delete all the decrypted software package from laptop upon user log-out. | TC\_Security\_005.1  TC\_Security\_005.2  TC\_Security\_005.3  TC\_Security\_005.4 |  |
| SRD-109 | The gateway agent shall completely delete a package after pre-configured expiration time has elapsed. | TC\_Security\_002.1  TC\_Security\_002.2  TC\_Security\_002.3  TC\_Security\_002.4 |  |
| SRD-792 | Software packages should be stream encrypted when they land on the server.  Note：refer to GW-3409 | TC\_Security\_007.1  TC\_Security\_007.2 |  |
| 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). | TC\_Security\_010.1 | Besides TC\_Security\_010.1, agent UT will cover security test about certificate/token. |
| 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. | TC\_Security\_010.1 | Besides TC\_Security\_010.1, agent UT will cover security test about certificate/token. |
| 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. | TC\_Security\_010.1 | Besides TC\_Security\_010.1, agent UT will cover security test about certificate/token. |
| 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. | TC\_Security\_010.2  TC\_Security\_010.3 | Besides TC\_Security\_010.1, agent UT will cover security test about certificate/token. |
| SRD-1021 | Mutual authentication certificates/tokens shall be kept private in the system component where they are installed and used. | TC\_Security\_010.1 | Security test will be conducted by MDT Cyber Security Test Team on an ongoing basis. |
| SRD-1023 | Below system components shall authenticate themselves to each other.    AgentApp Server | TC\_Security\_010.1 | Besides TC\_Security\_010.1, agent UT will cover security test about certificate/token. |
| SRD-1024 | The current clients will not being impacted with the existing authentication and communication approach with Agent | TC\_Security\_010.1  TC\_Security\_010.2  TC\_Security\_010.3 |  |
| **3.1.7       Gateway Agent General Requirements** | | | |
| SRD-93 | The system shall provide a Gateway agent. | AgentUninstallTestProcedure  AgentReinstallTestProcedure | Refer to [2] |
| 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. | AgentReinstallTestProcedure |  |
| 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. | AgentUninstallTestProcedure  AgentReinstallTestProcedure | Refer to [2] |
| SRD-98 | The gateway agent shall provide information to client application through message exchange. | TS\_Agent\_001  TS\_Agent\_002  TS\_Agent\_003  TS\_Agent\_004  TS\_Agent\_005  TS\_Agent\_006  TS\_Agent\_007  TS\_Agent\_008 |  |
| SRD-444 | The gateway agent shall disconnect from Server when requested by Client Application. | TC\_Agent\_014.1  TC\_Agent\_014.2 |  |
| SRD-663 | The gateway agent shall respond to a request from Client Application with network time (GMT) in connected mode. | TC\_Agent\_010.3 |  |
| **3.1.8       Data Upload/Download Requirement** | | | |
| 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. | TC\_DeviceManage\_008.3  TC\_DeviceManage\_008.5  TC\_DeviceManage\_008.10  TC\_DeviceManage\_008.12  TC\_DeviceManage\_008.14 |  |
| 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. | TC\_RolePermission\_006.1  TC\_RolePermission\_006.2  TC\_RolePermission\_006.4 |  |
| 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. | TC\_DeviceManage\_001.1  TC\_DeviceManage\_001.2  TC\_DeviceManage\_001.3  TC\_DeviceManage\_001.4 |  |
| 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. | TC\_DeviceManage\_008.3  TC\_DeviceManage\_008.5  TC\_DeviceManage\_008.10  TC\_DeviceManage\_008.12  TC\_DeviceManage\_008.14 |  |
| 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. | TC\_DeviceManage\_001.1  TC\_DeviceManage\_001.2  TC\_RolePermission\_006.1  TC\_RolePermission\_006.2 |  |
| 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. | TC\_Agent\_011.1  TC\_Agent\_011.2  TC\_Agent\_011.3  TC\_Agent\_011.4 |  |
| SRD-118 | The gateway agent shall cache its data during a download. | TC\_DeviceManage\_001.1  TC\_DeviceManage\_001.2  TC\_DeviceManage\_001.3  TC\_DeviceManage\_001.6 |  |
| SRD-119 | The gateway agent shall cache its data during upload. | TC\_DeviceManage\_008.2 |  |
| SRD-121 | The gateway agent shall be able to resume download to its download cache if communication is interrupted. | TC\_DeviceManage\_001.3 |  |
| SRD-124 | The gateway agent shall provide status notification of errors to the client application. | TC\_UserMgt\_009.3  TC\_UserMgt\_009.4  TC\_Agent\_020.1  TC\_Agent\_020.2  TC\_Agent\_020.3  TC\_Agent\_020.4 |  |
| SRD-125 | The gateway agent shall provide notifications to client application identifying problems and solutions as they occur in the process. | TC\_UserMgt\_009.3  TC\_UserMgt\_009.4  TC\_Agent\_020.1  TC\_Agent\_020.2  TC\_Agent\_020.3  TC\_Agent\_020.4 |  |
| SRD-191 | The gateway agent shall store data collected locally on the laptop. | TC\_DeviceManage\_001.1  TC\_DeviceManage\_001.2  TC\_DeviceManage\_001.3  TC\_DeviceManage\_001.5 |  |
| 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. | TS\_Agent\_002  TC\_Agent\_003.3  TC\_Agent\_003.4  TC\_Agent\_004.3  TC\_Agent\_004.4  TC\_Agent\_005.3  TC\_Agent\_005.4  TC\_Agent\_006.3  TC\_Agent\_006.4  TC\_Agent\_007.3  TC\_Agent\_007.4  TC\_Agent\_008.3  TC\_Agent\_008.4  TC\_DeviceManage\_008.2 |  |
| SRD-291 | The gateway agent shall use a store and forward strategy for data management. | TS\_Agent\_002 TC\_DeviceManage\_008.2 |  |
| SRD-362 | The gateway agent shall send "time period remaining before cached software is removed" to the Client application in the Agent status message. | TC\_Security\_002.1  TC\_Security\_002.2  TC\_Security\_002.3  TC\_Security\_002.4 |  |
| 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. | TC\_Agent\_015.1  TC\_Agent\_015.2  TC\_Agent\_015.3 |  |
| SRD-774 | The system shall support all existing approach to client applications for downloading software packages and configurations. | TC\_DeviceManage\_001.1  TC\_DeviceManage\_001.2  TC\_DeviceManage\_001.3  TC\_DeviceManage\_001.4  TC\_DeviceManage\_001.5  TC\_DeviceManage\_019.1 |  |
| 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 then 10 MB, the files will be uploaded in chunks. | TC\_DeviceManage\_008.1  TC\_DeviceManage\_008.7  TC\_DeviceManage\_008.8 |  |
| 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. | TC\_DeviceManage\_008.2 |  |
| **3.1.9       Gateway Agent-Cache Auto Download Requirements** | | | |
| 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 files are not downloaded.  Refer to 3.1.15 Device Prep Step Requirements. | TC\_DeviceManage\_001.1  TC\_DeviceManage\_001.2  TC\_DeviceManage\_001.3  TC\_DeviceManage\_001.4  TC\_DeviceManage\_001.5 |  |
| SRD-667 | The Agent shall prioritize the downloading of Client data ahead of other download items such as packages or documents. | TC\_DeviceManage\_001.1 |  |
| SRD-418 (Gateway 1004) | The file cache deletion timeout period shall be 90 days by default. | TC\_Security\_002.2  TC\_Security\_002.4 |  |
| SRD-425(Gateway 1004) | The file cache deletion timeout period for SCD700 shall be 3700 days. | TC\_Security\_002.1  TC\_Security\_002.3 |  |
| SRD-669 | The Agent shall clear the password cache at a configurable period time which defaults to 90 days. | TC\_UserMgt\_007.1  TC\_UserMgt\_007.2  TC\_UserMgt\_007.3  TC\_UserMgt\_007.4  TC\_UserMgt\_007.5 |  |
| 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. | TC\_Agent\_017.1  TC\_UserMgt\_007.5 |  |
| **3.1.10       Proxy Log-in Requirements** | | | |
| 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. | CTR6 | Refer to R0054299\_B\_PLAN\_PROC Verification Connection\_Tool\_v4.0 [6] |
| 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 | CTR4 | Refer to R0054299\_B\_PLAN\_PROC Verification Connection\_Tool\_v4.0 [6] |
| SRD- 481 | The Agent shall cache all proxy log-in credentials in a secure method. | CTR5 | Refer to R0054299\_B\_PLAN\_PROC Verification Connection\_Tool\_v4.0 [6] |
| SRD- 482 | The Agent shall be able to select cached proxy credentials which match the logged in user. | CTR6 | Refer to R0054299\_B\_PLAN\_PROC Verification Connection\_Tool\_v4.0 [6] |
| SRD- 483 | The Agent shall use the last logged in user's proxy credentials when all users have logged out of the computer. | CTR7 | Refer to R0054299\_B\_PLAN\_PROC Verification Connection\_Tool\_v4.0 [6] |
| SRD- 484 | The Agent shall be able to designate one proxy login credential as a machine login. | CTR8 | Refer to R0054299\_B\_PLAN\_PROC Verification Connection\_Tool\_v4.0 [6] |
| 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. | CTR10 | Refer to R0054299\_B\_PLAN\_PROC Verification Connection\_Tool\_v4.0 [6] |
| **3.1.11       Gateway Agent-Business Rules Requirements** | | | |
| SRD-394 | The system shall provide for Gateway Agent Business Rules. | TC\_Agent\_021.1  TC\_Agent\_021.2 |  |
| SRD-395 | The system shall provide for Client Application Business Rules. | TC\_DeviceManage\_001.1 |  |
| SRD-364 | The system shall have a means to identify “Business Rules” files for use by gateway agent during interactions with gateway agent. | TC\_DeviceManage\_001.1  TC\_Agent\_021.1  TC\_Agent\_021.2 |  |
| SRD-365 | The system shall provide a means to name “Business Rules” files. | TC\_HWSW\_005.1  TC\_HWSW\_005.2 |  |
| SRD-366 | The system shall allow “Business Rules” files to be uploaded to the server. | TC\_HWSW\_005.1  TC\_HWSW\_005.2  TC\_HWSW\_005.3  TC\_HWSW\_015.1  TC\_Agent\_021.1 |  |
| SRD-367 | The system shall version the Business Rules file(s). | TC\_HWSW\_015.1  TC\_DeviceManage\_001.1 |  |
| SRD-368 | The system shall support a message requesting the Business Rule file(s) for operation. | TC\_DeviceManage\_001.1 |  |
| SRD-369 | The message shall contain the version of all existing Business Rule files on the agent. | TC\_DeviceManage\_001.1 |  |
| SRD-370 | The system shall support the downloading of the Business Rule file(s) to the agent. | TC\_DeviceManage\_001.1  TC\_RolePermission\_006.4  TC\_RolePermission\_006.5 |  |
| SRD-371 | The system shall support the transfer of the Business Rule files to the client application. | TC\_DeviceManage\_001.1 |  |
| 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. | TC\_HWSW\_015.1  TC\_DeviceManage\_001.1 |  |
| SRD-449 (Gateway-1150) | The system shall use device-type specific business rules for applying the combination of software name, part number and revision number to find a software item in the catalog.  NOTE: The business rules should be based on the following behaviors:  1. In order to match the running configuration of a docked device, the software item name should not change from one software name 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.  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  4. A user with permission to install all production versions can get all software packages which have same software name but different part number for PB980. 5. Auser with permission to install only the latest version can only get software packages which have same software name and same part number for PB980.  6. A user with permission to install all production versions can see all software packages (same name) on ESS in disconnect mode. 7. A user with permission to install only the latest software version can only see software packages which have same software name and same part number on ESS in disconnect mode.  8. A user with permission to install all production versions can get all software packages for SCD700, Emprint, VLLS10, VLFT10, and Signia which have the same name but a different part number than the running configuration of the docked device.  9. A user with permission to install only the latest software version can get only the latest software version of a package (as determined by Comparison Order setting in catalog) for SCD700, Emprint, VLLS10, VLFT10, Signia which have the same name but a different part number than the running configuration of the docked device.  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.  NOTE: Refer to Section 8.2.1.7, Software Component Match. | TC\_HWSW\_011.1  TC\_HWSW\_011.2  TC\_HWSW\_012.1  TC\_HWSW\_012.2  TC\_HWSW\_013.1  TC\_HWSW\_013.2  TC\_HWSW\_014.1  TC\_HWSW\_014.2  TC\_HWSW\_011.3  TC\_HWSW\_011.4  TC\_HWSW\_012.3  TC\_HWSW\_012.4  TC\_HWSW\_013.3  TC\_HWSW\_013.4  TC\_HWSW\_014.3  TC\_HWSW\_014.4  TC\_HWSW\_016.1-4  TC\_HWSW\_017.1-4 |  |
| SRD-393 | The gateway agent shall use business rules logic for device software selection in disconnected mode. | TC\_HWSW\_011.3  TC\_HWSW\_011.4  TC\_HWSW\_012.3  TC\_HWSW\_012.4  TC\_HWSW\_013.3  TC\_HWSW\_013.4  TC\_HWSW\_014.3  TC\_HWSW\_014.4  TC\_HWSW\_016.3  TC\_HWSW\_016.4  TC\_HWSW\_017.3  TC\_HWSW\_017.4 |  |
| SRD-396 | The gateway agent shall provide the updated Business Rule(s) Files to the Client application | TC\_HWSW\_015.1  TC\_DeviceManage\_001.1 |  |
| **3.1.12       Device Identification** | | | |
| SRD-126 | The system shall accept device identification. | TC\_Agent\_001.1  TC\_Agent\_001.2  TC\_Agent\_001.3  TC\_Agent\_001.4  TC\_Agent\_001.5  TC\_Agent\_001.6  TC\_Agent\_001.7  TC\_Agent\_001.8  TC\_Agent\_001.9  TC\_Agent\_001.10  TC\_Agent\_001.11  TC\_Agent\_001.12  TC\_Agent\_002.1  TC\_Agent\_002.2  TC\_Agent\_002.3  TC\_Agent\_002.4  TC\_Agent\_002.5  TC\_Agent\_002.6  TC\_Agent\_002.7  TC\_Agent\_002.8  TC\_Agent\_002.9  TC\_Agent\_002.10  TC\_Agent\_002.11  TC\_Agent\_002.12 |  |
| SRD-99 | The gateway agent shall collect the device information through a message exchange with client application. | TC\_Agent\_001.1  TC\_Agent\_002.1  TC\_DeviceManage\_004.1  TC\_DeviceManage\_005.1 |  |
| SRD-127 | The system shall enumerate devices by device type. | TC\_DeviceManage\_003.1 |  |
| SRD-128 | The device types shall include those identified on schedule C. | TC\_DeviceManage\_003.1 |  |
| 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 | TC\_DeviceManage\_003.1  TC\_DeviceManage\_004.1  TC\_DeviceManage\_011.1 |  |
| 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 business units so it’s important to qualify them with Device Type. | TC\_Agent\_001.1  TC\_Agent\_002.1  TC\_DeviceManage\_003.1  TC\_DeviceManage\_003.2 TC\_DeviceManage\_010.1  TC\_DeviceManage\_010.5  TC\_DeviceManage\_010.9  TC\_DeviceManage\_010.10  TC\_DeviceManage\_010.12 |  |
| SRD-140 | The system shall be capable of automatically grouping devices according to a device type for viewing at the server. | TC\_DeviceManage\_003.1  TC\_DeviceManage\_003.2 |  |
| SRD-141 | The system shall recognize a new device through device discovery. | TC\_Agent\_001.1  TC\_Agent\_001.2  TC\_Agent\_001.3  TC\_Agent\_001.4  TC\_Agent\_001.5  TC\_Agent\_001.6  TC\_Agent\_001.7  TC\_Agent\_001.8  TC\_Agent\_001.9  TC\_Agent\_001.10  TC\_Agent\_001.11  TC\_Agent\_001.12  TC\_Agent\_002.1  TC\_Agent\_002.2  TC\_Agent\_002.3  TC\_Agent\_002.4  TC\_Agent\_002.5  TC\_Agent\_002.6  TC\_Agent\_002.7  TC\_Agent\_002.8  TC\_Agent\_002.9  TC\_Agent\_002.10  TC\_Agent\_002.11  TC\_Agent\_002.12 |  |
| SRD-142 | The system shall add new devices to the device records. | TC\_Agent\_001.1  TC\_Agent\_001.2  TC\_Agent\_001.3  TC\_Agent\_001.4  TC\_Agent\_001.5  TC\_Agent\_001.6  TC\_Agent\_001.7  TC\_Agent\_001.8  TC\_Agent\_001.9  TC\_Agent\_001.10  TC\_Agent\_001.11  TC\_Agent\_001.12  TC\_Agent\_002.1  TC\_Agent\_002.2  TC\_Agent\_002.3  TC\_Agent\_002.4  TC\_Agent\_002.5  TC\_Agent\_002.6  TC\_Agent\_002.7  TC\_Agent\_002.8  TC\_Agent\_002.9  TC\_Agent\_002.10  TC\_Agent\_002.11  TC\_Agent\_002.12 |  |
| SRD-143 | The system shall categorize any new device added to the system by device type. | TC\_Agent\_001.1 – TC\_Agent\_001.12  TC\_Agent\_002.1 – TC\_Agent\_002.12  TC\_DeviceManage\_003.1  TC\_DeviceManage\_003.2 |  |
| SRD-144 | The system shall support a multidimensional lookup to determine the current software for a device. | TC\_HWSW\_009.1  TC\_HWSW\_009.2 |  |
| 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 | TC\_HWSW\_011.1- TC\_HWSW\_011.4  TC\_HWSW\_012.1- TC\_HWSW\_012.4 TC\_HWSW\_013.1- TC\_HWSW\_013.4  TC\_HWSW\_014.1- TC\_HWSW\_014.4  TC\_HWSW\_009.1  TC\_HWSW\_009.2 |  |
| SRD-133 | Device identifying information shall be exchanged in industry standard format for an example as XML. | TC\_Agent\_001.1-TC\_Agent\_001.12  TC\_Agent\_002.1-TC\_Agent\_002.12 |  |
| SRD-539 (Gateway 1597) (CRITICAL) | The Agent shall accept a message from the Client specifying device region for a specific device. | TC\_Agent\_016.1  TC\_Agent\_016.2  TC\_Agent\_016.3  TC\_DeviceManage\_006.1  TC\_ DeviceManage\_006.2  TC\_DeviceManage\_006.3  TC\_DeviceManage\_006.4 |  |
| SRD-540 (Gateway 1597) (CRITICAL) | The System shall record device region associated with a specific device, if provided by the Client. | TC\_Agent\_016.1  TC\_Agent\_016.2  TC\_Agent\_016.3 |  |
| SRD-541 (Gateway 1597) (CRITICAL) | The System shall include device region in device history reports, if included in the device record. | TC\_Agent\_016.1  TC\_Agent\_016.2  TC\_Agent\_016.3 |  |
| **3.1.13       Device Warranty Management Requirements** | | | |
| SRD-405 (High) | The system shall store the device maintenance expiration date, if available for a device. | 50RealDeviceValidationTestProcedure | This has been validated in Database Validation Plan. Refer to [9] |
| SRD-406 (High) | The system shall display the device maintenance expiration date, if available for a device. | 50RealDeviceValidationTestProcedure | This has been validated in Database Validation Plan. Refer to [9] |
| **3.1.14       Device Warranty Management Requirements** | | | |
| 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. | TC\_DeviceManage\_001.2 |  |
| 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. | TC\_DeviceManage\_001.6 |  |
| 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. | TC\_DeviceManage\_001.2 |  |
| SRD-620 (CRITICAL) | The Agent shall report remaining download time by device type. | TC\_Agent\_022.1 |  |
| SRD-621 (CRITICAL) | The Agent shall provide a means for the Client to identify itself via the Client’s GUID. | TC\_UserMgt\_009.1 |  |
| 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. . | TC\_DeviceManage\_001.2 |  |
| 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. | TC\_DeviceManage\_001.2 |  |
| 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  VLLS10VLFT10  ABLATION  Emprint Planning Software  COMPRESSION  SCD700  **STAPLING**  **Signia Stapler** | TC\_DeviceManage\_001.6 |  |
| SRD-624 (CRITICAL) | For each CoT, the Agent shall report the cumulative size on disk for all packages per device type per CoT. | TC\_Agent\_010.4 |  |
| SRD-625 (CRITICAL) | The Agent shall read in an Agent-specific business rule file for associating CoT and Device Type. | TC\_DeviceManage\_001.1 |  |
| SRD-626 (CRITICAL) | The Agent shall check the Server for new versions of the CoT/Device Business Rule File and download it as appropriate. | TC\_DeviceManage\_001.1  TC\_DeviceManage\_001.4 |  |
| **3.1.15       Device Software Upgrade Related Requirements** | | | |
| SRD-101 | The gateway agent shall manage the download of software from the server. | TC\_RolePermission\_006.1  TC\_RolePermission\_006.4  TC\_DeviceManage\_001.1  TC\_DeviceManage\_001.2  TC\_DeviceManage\_001.3  TC\_DeviceManage\_001.4  TC\_DeviceManage\_001.5  TC\_DeviceManage\_001.6  TC\_DeviceManage\_001.7 |  |
| SRD-102 | The system shall notify the client application of completed software download via message exchange. | TC\_Agent\_022.1 |  |
| SRD-103 | The gateway agent shall cache the software package locally. | TC\_DeviceManage\_001.6  TC\_RolePermission\_006.1  TC\_RolePermission\_006.4 |  |
| SRD-104 | The gateway agent shall check the package cache before downloading software packages to avoid duplication. | TC\_DeviceManage\_001.9 |  |
| SRD-356 | The gateway agent shall identify all device-type software versions in its cache that are available for installation on edge devices. | TC\_Agent\_022.2 |  |
| 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. | TC\_RolePermission\_006.1-2 |  |
| 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. | TC\_RolePermission\_006.1-2 |  |
| SRD-359 | The system shall determine which device type software is missing from the gateway agent's software list. | TC\_DeviceManage\_001.4  TC\_DeviceManage\_001.5  TC\_DeviceManage\_001.6  TC\_DeviceManage\_001.7 |  |
| 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. | TC\_DeviceManage\_001.3  TC\_DeviceManage\_001.4  TC\_DeviceManage\_001.5  TC\_DeviceManage\_001.6  TC\_DeviceManage\_001.7 |  |
| SRD-414 | The gateway agent shall download all missing software based on the users authorized device type(s). | TC\_DeviceManage\_001.3  TC\_DeviceManage\_001.4  TC\_DeviceManage\_001.5 |  |
| SRD-361 | The gateway agent shall download all missing software based on the missing software message from the server. | TC\_DeviceManage\_001.4  TC\_DeviceManage\_001.5 |  |
| SRD-158 | The system shall support software package status. | TC\_HWSW\_006.1  TC\_HWSW\_006.2  TC\_HWSW\_006.3  TC\_HWSW\_006.4  TC\_HWSW\_006.5 |  |
| SRD-159 | The software package status shall include: Limited Release In Production Archived | TC\_HWSW\_006.1  TC\_HWSW\_006.2  TC\_HWSW\_006.3  TC\_HWSW\_006.4  TC\_HWSW\_006.5 |  |
| SRD-160 | The agent shall present a list of all available software packages to the client application. | TS\_DeviceManage\_001.4  DeviceManageForVLLS10TestProcedure  DeviceManageDisconnectModeForVLLS10TestProcedure  DeviceManageForVLFT10TestProcedure  DeviceManageDisconnectModeForVLFT10TestProcedure  DeviceManageTestProcedureForVentilator  DeviceManageDisconnectModeTestProcedureForVentilator  DeviceManageTestProcedureForSCD700  DeviceManageFor\_Emprint\_Procedure\_Planning\_Application\_TestProcedure  DeviceManageDisconnectModeFor\_Emprint\_Procedure\_Planning\_Application\_TestProcedure  E2E\_SoftwareUpdate\_online  E2E\_SoftwareUpdate\_offline |  |
| SRD-161 | The software package at the agent shall have an expiration time.(default 90 days, SCD700:3700 days) | TC\_Security\_002.1  TC\_Security\_002.2  TC\_Security\_002.3  TC\_Security\_002.4 |  |
| SRD-174 | The device software installation shall be done by the client application. | TC\_Agent\_003.1-TC\_Agent\_003.4  TC\_Agent\_004.1-TC\_Agent\_004.4  TC\_Agent\_005.1-TC\_Agent\_005.4  TC\_Agent\_006.1-TC\_Agent\_006.4  TC\_Agent\_007.1-TC\_Agent\_007.4  TC\_Agent\_008.1-TC\_Agent\_008.4 |  |
| SRD-177 | The system shall confirm successful updates of device software. | TC\_Agent\_003.1-TC\_Agent\_003.4  TC\_Agent\_004.1-TC\_Agent\_004.4  TC\_Agent\_005.1-TC\_Agent\_005.4  TC\_Agent\_006.1-TC\_Agent\_006.4  TC\_Agent\_007.1-TC\_Agent\_007.4  TC\_Agent\_008.1-TC\_Agent\_008.4 |  |
| SRD-178 | The system shall prevent download of any package with ‘Limited Release’ status by users with insufficient privileges. | TC\_RolePermission\_006.2  TC\_RolePermission\_006.1 |  |
| SRD-179 | The system shall provide a user interface to allow administrative users to upload software packages to the system. | TC\_HWSW\_005.1  TC\_HWSW\_005.2  TC\_HWSW\_015.1  TC\_HWSW\_006.6 |  |
| SRD-180 | The system shall default to setting the status of new software packages to ‘Limited Release’. | TC\_HWSW\_005.1  TC\_HWSW\_005.2 |  |
| SRD-181 | The system shall allow the administrator to set the software package status of a software package. | TC\_HWSW\_005.1- TC\_HWSW\_005.2  TC\_HWSW\_015.1  TC\_HWSW\_006.3-TC\_HWSW\_006.5 |  |
| SRD-530 (Gateway 1503) (CRITICAL) | The system shall provide a means by which a user with appropriate privileges to set the release order precedence of the Software packages. NOTE: The appropriate permissions are defined in SRD-478, use SW Catalog Catalog permission for this req. | TC\_HWSW\_005.5 |  |
| SRD-531 (Gateway 1503) (CRITICAL) | The system shall use the pre specified release order precedence to download latest software. NOTE: This should operate in both connected and disconnected mode. | TC\_HWSW\_005.5  TC\_HWSW\_018.1  TC\_HWSW\_018.2 |  |
| SRD-662 (Gateway 2224) (CRITICAL) | The system shall inform the Client application of the pre-specified order precedence of the downloaded software. | TC\_HWSW\_005.5  TC\_HWSW\_018.1  TC\_HWSW\_018.2 |  |
| SRD-661 | The system shall allow devices that have a running configuration which corresponds to an archived named system configuration to upgrade to newer named system configuration. | TC\_Agent\_012.1  TC\_Agent\_012.2 |  |
| SRD-706 | Software package contains subtypes including:   * Firmware * BootCode * Software Bundle * Business Rule * Software | TC\_HWSW\_005.1  TC\_HWSW\_005.2 |  |
| 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  Note: see GW-2928, GW-2934 | TC\_HWSW\_002.1-TC\_HWSW\_002.4  TC\_HWSW\_006.1-TC\_HWSW\_006.5 |  |
| SRD-708 | The system shall automatically create software items which do not exist in the SW Catalog when the system discovers them in a device's running configuration. And these software items shall be assigned with software bundle as software subtype by default.  Note: See GW-3051 | TC\_DeviceManage\_004.1-TC\_DeviceManage\_004.3  TC\_DeviceManage\_005.1-TC\_DeviceManage\_005.3 |  |
| 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. | TC\_HWSW\_008.2 |  |
| SRD-710 | The system shall allow CoT Admin to associate the documents with software, in order to provide instructions or information to the end users. | TC\_HWSW\_005.2 |  |
| 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 | TC\_HWSW\_008.1 |  |
| SRD-714 | The system shall allow CoT Admin administrator user to clone existing software configuration(s) in order to create new software configuration(s). | TC\_NamedConf\_009.1  TC\_NamedConf\_009.2  TC\_NamedConf\_009.3  TC\_NamedConf\_009.4  TC\_NamedConf\_009.5  TC\_NamedConf\_009.6 |  |
| SRD-715 | The system shall allow user to see the clone map of a software configuration, such as parent, siblings, and children. | TC\_NamedConf\_010.1  TC\_NamedConf\_010.2  TC\_NamedConf\_010.3 |  |
| SRD-716 | The system shall allow CoT Admin to add one or more country exclusion 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. | TC\_HWSW\_009.1  TC\_HWSW\_009.2  TC\_NamedConf\_010.2  TC\_NamedConf\_010.3 |  |
| 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 | TC\_HWSW\_006.5  TC\_HWSW\_006.6  TC\_HWSW\_006.7  TC\_HWSW\_006.8  TC\_HWSW\_006.9  TC\_HWSW\_006.10  TC\_HWSW\_006.11  TC\_HWSW\_006.12  TC\_HWSW\_006.13  TC\_HWSW\_006.14  TC\_HWSW\_006.15  TC\_HWSW\_006.16  TC\_HWSW\_006.17  TC\_HWSW\_006.18  TC\_HWSW\_006.19  TC\_HWSW\_006.20 |  |
| SRD-1028 | User with appropriate permission can edit existing SW item based on below rules: | TC\_HWSW\_006.1  TC\_HWSW\_006.2  TC\_HWSW\_006.3  TC\_HWSW\_006.4 |  |
| **3.1.16       Device Log Handling** | | | |
| SRD-100 | The gateway agent shall accept logs if the client application provides them. | TC\_DeviceManage\_008.1-TC\_DeviceManage\_008.15 |  |
| SRD-164 | If a device type provides log files, then the system shall accept log files from the device before updating the software | TC\_DeviceManage\_008.1-TC\_DeviceManage\_008.15 |  |
| SRD-165 | If a device type provides log files, then the system shall store the device logs on the server. | TC\_DeviceManage\_008.1-TC\_DeviceManage\_008.15 |  |
| 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. | TC\_DeviceManage\_008.1-TC\_DeviceManage\_008.15 |  |
| SRD-173 | If a device type provides log files, then the system shall allow the retrieval of all logs from the device | TC\_DeviceManage\_008.1-TC\_DeviceManage\_008.15 |  |
| SRD-169 | The system shall capture service type with uploaded service information. | TC\_DeviceManage\_017.1  TC\_Report\_012.1-TC\_Report\_012.5 |  |
| 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). | TC\_Agent\_001.1-TC\_Agent\_001.12  TC\_Agent\_003.1-TC\_Agent\_001.4  TC\_Agent\_004.1-TC\_Agent\_001.4  TC\_Agent\_005.1-TC\_Agent\_001.4  TC\_Agent\_006.1-TC\_Agent\_001.4  TC\_Agent\_007.1-TC\_Agent\_001.4  TC\_Agent\_008.1-TC\_Agent\_001.4  TC\_DeviceManage\_008.1-TC\_DeviceManage\_008.15 TS\_DeviceManage\_017.1 |  |
| SRD-193 | The system shall store the service records for each device on the server. | TC\_Agent\_001.1-TC\_Agent\_001.12  TC\_Agent\_003.1-TC\_Agent\_001.4  TC\_Agent\_004.1-TC\_Agent\_001.4  TC\_Agent\_005.1-TC\_Agent\_001.4  TC\_Agent\_006.1-TC\_Agent\_001.4  TC\_Agent\_007.1-TC\_Agent\_001.4  TC\_Agent\_008.1-TC\_Agent\_001.4  TC\_DeviceManage\_008.1-TC\_DeviceManage\_008.15 TC\_DeviceManage\_017.1  TC\_Report\_012.1-TC\_Report\_012.5 |  |
| SRD-194 | The system shall default to reverse chronological order for the display of device service information. | TC\_DeviceManage\_017.1  TC\_DeviceManage\_017.2 |  |
| SRD-195 | The system shall provide a user Interface to review service records. | TC\_DeviceManage\_017.1  TC\_DeviceManage\_017.2 |  |
| 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 | TC\_Report\_012.1-TC\_Report\_012.5 |  |
| 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. | TC\_Security\_008.1  TC\_Security\_008.2 |  |
| 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) | TC\_DeviceManage\_017.1 |  |
| 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. | TC\_Report\_012.1-TC\_Report\_012.5 |  |
| 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. | TC\_Report\_012.1-TC\_Report\_012.5 |  |
| SRD-721 | The system shall allow a user to download a decrypted log file to his computer through the log-viewer. | TC\_DeviceManage\_008.5  TC\_DeviceManage\_008.11  TC\_DeviceManage\_008.13  TC\_DeviceManage\_008.15 |  |
| **3.1.17       Document Handling** | | | |
| SRD-152 | The system shall allow the upload of documents for distribution by CoT admin users. | TC\_Doc\_001.1-TC\_Doc\_001.8  TC\_Doc\_002.1-TC\_Doc\_002.9 |  |
| SRD-153 (CRITICAL) | The system shall allow the option of associating a document with a SW/HW/Feature catalog item | TC\_Doc\_001.1-TC\_Doc\_001.8 |  |
| SRD-154 | The system shall allow the independent download of documents based on role and access policy. | TC\_RolePermission\_006.1  TC\_RolePermission\_006.2 |  |
| SRD-156 | The system shall classify uploaded documents by document type | TC\_Doc\_001.1-TC\_Doc\_001.8 |  |
| SRD-157 | The document type enumeration shall include: Release Notes User Guides Service Manual Other | TC\_Doc\_001.1-TC\_Doc\_001.8 |  |
| 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 | DeviceManageTestProcedureForSCD700  TC\_Doc\_004.1  TC\_Doc\_004.2  TC\_Doc\_004.3 |  |
| SRD-736 | The system shall allow CoT Admin administrator user to edit an existing document item based on below rules: | TC\_Doc\_002.1-TC\_Doc\_002.3 |  |
| SRD-737 | The system shall allow CoTadmin to archive existing documents. | TC\_Doc\_002.5  TC\_Doc\_002.7 |  |
| 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 | TC\_ Doc \_002.4  TC\_ Doc \_002.5  TC\_ Doc \_002.6  TC\_ Doc \_002.7  TC\_ Doc \_002.8  TC\_ Doc \_002.9 |  |
| SRD-739 | The system shall allow user to search documents by document name, or device type. | TC\_Doc\_004.3 |  |
| SRD-740 | The system shall allow a CoT Admin user to clone existing document items in order to easily create new document item | TC\_Doc\_005.1  TC\_Doc\_005.2 |  |
| SRD-741 | The system shall allow user to see the clone map of document, such as parent, siblings, and children. | TC\_Doc\_004.2 |  |
| 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. | TC\_Doc\_001.7  TC\_Doc\_001.8 |  |
| **3.1.18       Regulatory and Trade Embargo Requirements** | | | |
| SRD-166 | If a device type provides log files, then the system shall retain the log files for a minimum of seven (7) years. | N/A | Cannot be traced to test case. This requirement can be covered by Gateway Backup Strategy and Procedure document which is listed in section 1.3 reference [3] |
| SRD-331 | The system shall not provide software to devices in countries that are denied regulatory approval. NOTE: Refer to Section 7.2.1.4, Device Regulatory Permission. | TC\_HWSW\_009.1  TC\_HWSW\_009.2 |  |
| SRD-332 | The system shall provide a means to track countries where regulatory approval has not been gained. | TC\_HWSW\_009.1  TC\_HWSW\_009.2 |  |
| SRD-334 | The system shall associate a country with the user. | TC\_UserMgt\_001.1-TC\_UserMgt\_001.4  TC\_UserMgt\_002.1-TC\_UserMgt\_001.4 |  |
| SRD-335 | The UI shall allow the selection of a country as part of the user profile screen. | TC\_UserMgt\_001.1-TC\_UserMgt\_001.4  TC\_UserMgt\_002.1-TC\_UserMgt\_001.4 |  |
| 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. | TC\_DeviceManage\_002.1 |  |
| 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. | TC\_DeviceManage\_006.1  TC\_DeviceManage\_006.2  TC\_DeviceManage\_006.3  TC\_DeviceManage\_006.4  TC\_DeviceManage\_006.5 |  |
| 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. | TC\_DeviceManage\_002.1 |  |
| 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. | N/A | This requirement is not tested because it is not used by any clients |
| **3.1.19      Device Configuration Management** | | | |
| SRD-456 | The system shall allow configuration management, including hardware, software, feature and system configuration through the web UI. | TC\_NamedConf\_001.1  TC\_NamedConf\_001.2  TC\_NamedConf\_001.3  TC\_NamedConf\_001.4  TC\_FeatureLicense\_006.1  TC\_FeatureLicense\_006.2 |  |
| 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. | SoftwareDiscrepancyCheckTestProcedureForVentilator  CheckSoftwareDiscrepancyForVLLS10TestProcedure  CheckSoftwareDiscrepancyForVLFT10TestProcedure  SoftwareDiscrepancyCheckTestProcedureForSCD700  CheckSoftwareDiscrepancyFor\_Emprint Procedure Planning Application\_TestProcedure  E2E\_Discrepancy\_Software\_offline |  |
| 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). | TC\_Agent\_003.2  TC\_Agent\_003.4  TC\_Agent\_004.2  TC\_Agent\_004.4  TC\_Agent\_005.2  TC\_Agent\_005.4  TC\_Agent\_006.2  TC\_Agent\_006.4  TC\_Agent\_007.2  TC\_Agent\_007.4 TC\_Agent\_008.2  TC\_Agent\_008.4 |  |
| SRD-197 | The system shall flag devices that have configurations that differ from the server database records. | SoftwareDiscrepancyCheckTestProcedureForSCD700  CheckSoftwareDiscrepancyForVLLS10TestProcedure  CheckSoftwareDiscrepancyForVLFT10TestProcedure  SoftwareDiscrepancyCheckTestProcedureForVentilator  E2E\_Discrepancy\_Software\_offline  CheckSoftwareDiscrepancyForEmprint ProcedurePlanningApplicationTestProcedure |  |
| 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). | SoftwareDiscrepancyCheckTestProcedureForSCD700  CheckSoftwareDiscrepancyForVLLS10TestProcedure  CheckSoftwareDiscrepancyForVLFT10TestProcedure  SoftwareDiscrepancyCheckTestProcedureForVentilator  E2E\_Discrepancy\_Software\_offline  CheckSoftwareDiscrepancyForEmprint ProcedurePlanningApplicationTestProcedure |  |
| SRD-220 | The system shall provide a UI to display discrepancy lists. | SoftwareDiscrepancyCheckTestProcedureForSCD700  CheckSoftwareDiscrepancyForVLLS10TestProcedure  CheckSoftwareDiscrepancyForVLFT10TestProcedure  SoftwareDiscrepancyCheckTestProcedureForVentilator  E2E\_Discrepancy\_Software\_offline  CheckSoftwareDiscrepancyForEmprint ProcedurePlanningApplicationTestProcedure |  |
| SRD-458 | The gateway agent shall respond to a request from the client asking if a device configuration is valid. NOTE: Refer to Section 7.2.2, Configuration Validation. | TC\_NamedConf\_011.1  TC\_NamedConf\_011.2  TC\_NamedConf\_011.3  TC\_NamedConf\_011.4 |  |
| 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 | SoftwareDiscrepancyCheckTestProcedureForSCD700  CheckSoftwareDiscrepancyForVLLS10TestProcedure  CheckSoftwareDiscrepancyForVLFT10TestProcedure  SoftwareDiscrepancyCheckTestProcedureForVentilator  E2E\_Discrepancy\_Software\_offline  CheckSoftwareDiscrepancyForEmprint ProcedurePlanningApplicationTestProcedure |  |
| SRD-496 (Gateway 664) (CRITICAL) | The system shall store all configuration items reported by the device which are defined in the HW/SW/Feature catalogs. | TC\_DeviceManage\_004.1-TC\_DeviceManage\_004.3  TC\_DeviceManage\_005.1-TC\_DeviceManage\_005.2 |  |
| 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” | TC\_DeviceManage\_004.1-TC\_DeviceManage\_004.3  TC\_DeviceManage\_005.1-TC\_DeviceManage\_005.2 |  |
| SRD-610 (Gateway 1665) (CRITICAL) | The system shall provide a means for the client to report the docked device's configuration. | TC\_DeviceManage\_004.1-TC\_DeviceManage\_004.3  TC\_DeviceManage\_005.1-TC\_DeviceManage\_005.2  TC\_Agent\_001.1-TC\_Agent\_001.12  TC\_Agent\_002.1-TC\_Agent\_002.12 |  |
| SRD-611 (Gateway 1665) (CRITICAL) | Reported device running configuration 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, activated features may also be reported. | TC\_DeviceManage\_004.1-TC\_DeviceManage\_004.3  TC\_DeviceManage\_005.1-TC\_DeviceManage\_005.2 |  |
| **3.1.20       Orion Specific Configuration Management Requirements** | | | |
| 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. | TC\_DeviceManage\_007.1  TC\_DeviceManage\_007.2  TC\_DeviceManage\_007.3 |  |
| SRD-655 (Gateway 2004) (CRITICAL) | The system shall store the serial number for all hardware components in the device record. | TC\_DeviceManage\_007.7 |  |
| SRD-658*(Gateway 2012)* | The system shall provide a view of the VLFT10 hardware component serial numbers in the device configuration history. | TC\_DeviceManage\_007.7 |  |
| **3.1.21** **Named Configuration**  ***Named Configuration Requirements- Server/Web UI*** | | | |
| SRD-297 (HIGH) | The system shall allow a user with Configuration Admin permission to create/edit/archive named configurations. | TC\_NamedConf\_001.1  TC\_NamedConf\_002.1 TC\_NamedConf\_003.1  TC\_NamedConf\_004.3  TC\_NamedConf\_006.4  TC\_NamedConf\_005.2  TC\_NamedConf\_007.1  TC\_NamedConf\_008.1  TC\_FeatureLicense\_006.1  TC\_FeatureLicense\_007.1 |  |
| SRD-499 (Gateway 1054) (HIGH) | Only users who have Configuration Administration permission shall be permitted to add/archive/modify named configurations. | TC\_NamedConf\_001.1  TC\_NamedConf\_002.1 TC\_NamedConf\_003.1  TC\_NamedConf\_004.3  TC\_NamedConf\_006.4  TC\_NamedConf\_005.2  TC\_NamedConf\_007.1  TC\_NamedConf\_008.1  TC\_FeatureLicense\_006.1  TC\_FeatureLicense\_007.1 |  |
| SRD-500 (Gateway 1054) (HIGH) | The system shall support named hardware configurations. | TC\_NamedConf\_001.1  TC\_NamedConf\_003.1  TC\_NamedConf\_004.3  TC\_NamedConf\_004.1  TC\_NamedConf\_010.1 |  |
| SRD-501 (Gateway 1054) (HIGH) | The system shall support named software configurations. | TC\_NamedConf\_001.2  TC\_NamedConf\_006.4  TC\_NamedConf\_007.1  TC\_NamedConf\_010.1 |  |
| 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. | TC\_NamedConf\_001.3  TC\_FeatureLicense\_010.1 |  |
| SRD-795 | System configuration with "In Production" status shouldn't contain software configuration in 'Limited Release' status. | TC\_NamedConf\_004.3  TC\_NamedConf\_004.1  TC\_NamedConf\_005.1  TC\_NamedConf\_006.5  TC\_NamedConf\_005.2  TC\_NamedConf\_005.6 |  |
| SRD-507 (Gateway 1054) (HIGH) | A named hardware configuration shall be composed of one or more hardware items. | TC\_NamedConf\_001.1 |  |
| 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. | TC\_NamedConf\_012.1  TC\_NamedConf\_012.2  TC\_NamedConf\_012.3 |  |
| SRD-509 (Gateway 1054) (HIGH) | A named software configuration shall be composed of one or more software configuration items. | TC\_NamedConf\_001.2 |  |
| SRD-513 (Gateway 1054) (HIGH) | System shall not present to the Client those Named System Configurations which have constituent components with either archive status. | TC\_NamedConf\_013.1  TC\_NamedConf\_013.2 |  |
| SRD-514 (Gateway 1240) (HIGH) | A device configuration shall be considered valid if it matches a valid named system configuration on the server. | TC\_NamedConf\_013.1  TC\_NamedConf\_013.2 |  |
| 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 device type. | TC\_NamedConf\_013.1  TC\_NamedConf\_013.2 |  |
| 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 item (for Catalog Configuration Devices) | TC\_HWSW\_005.1 |  |
| 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. | TC\_NamedConf\_013.1  TC\_NamedConf\_013.2 |  |
| SRD-517 (Gateway 1054) (HIGH) | The system shall allow a user to associate one or more documents with a named hardware, software, or feature item. | TC\_HWSW\_001.1  TC\_HWSW\_005.1  TC\_FeatureLicense\_001.1 |  |
| 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) | TC\_NamedConf\_001.3 |  |
| 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. | TC\_NamedConf\_013.1  TC\_NamedConf\_013.2 |  |
| SRD-627 (Gateway 1054) (HIGH) | The system shall return appropriate software list based on the device 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. | TC\_NamedConf\_013.1  TC\_NamedConf\_013.2 |  |
| 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: a. In Production b. Archived c. Limited Release | TC\_NamedConf\_004.3  TC\_NamedConf\_006.4  TC\_NamedConf\_005.2  TC\_FeatureLicense\_007.4-TC\_FeatureLicense\_007.9 |  |
| 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. | TC\_NamedConf\_012.1  TC\_NamedConf\_012.2  TC\_NamedConf\_012.3  TC\_NamedConf\_013.1  TC\_NamedConf\_013.2 |  |
| 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  Feature incompatible with Feature: Only show warning Feature configurations as candidate list  HW incompatible with Feature: Only show HW and Feature configurations as candidate list.  SW incompatible with Feature: Only show SW and Feature configurations as candidate list  HW/SW incompatible with Feature: show HW, SW and Feature configurations as candidate list. | TC\_NamedConf\_002.1  TC\_NamedConf\_002.2  TC\_NamedConf\_002.3  TC\_NamedConf\_011.1  TC\_NamedConf\_011.2  TC\_NamedConf\_011.3  TC\_NamedConf\_011.4 |  |
| SRD-745 | The system shall allow CoT Admin user to view a country exclusion that may be associated with software items in the software configuration | TC\_NamedConf\_010.2  TC\_NamedConf\_010.3 |  |
| SRD-746 | The system shall allow user to search configurations by name, or device type, or configuration type. | TC\_NamedConf\_010.4  TC\_NamedConf\_010.5 |  |
| SRD-747 | The system shall allow user to view a named hardware/software/feature/system configuration. | TC\_NamedConf\_010.1  TC\_NamedConf\_010.2  TC\_NamedConf\_010.3  TC\_NamedConf\_010.4  TC\_NamedConf\_010.5  TC\_FeatureLicense\_009.1 |  |
| SRD-748 | User with appropriate permission can edit named hardware configuration based on below rules: | TC\_NamedConf\_003.1  TC\_NamedConf\_003.2  TC\_NamedConf\_003.3 |  |
| SRD-1029 | User with appropriate permission can edit named software configuration based on below rules: | TC\_NamedConf\_007.1  TC\_NamedConf\_007.2  TC\_NamedConf\_007.3 |  |
| SRD-1030 | User with appropriate permission can edit named system configuration based on below rules: | TC\_NamedConf\_008.1  TC\_NamedConf\_008.2  TC\_NamedConf\_008.3 |  |
| 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 | TC\_NamedConf\_004.1  TC\_NamedConf\_004.2  TC\_NamedConf\_004.3  TC\_NamedConf\_004.4  TC\_NamedConf\_004.5  TC\_NamedConf\_004.6  TC\_NamedConf\_006.1  TC\_NamedConf\_006.2  TC\_NamedConf\_006.3  TC\_NamedConf\_006.4  TC\_NamedConf\_006.5  TC\_NamedConf\_006.6  TC\_NamedConf\_005.1  TC\_NamedConf\_005.2  TC\_NamedConf\_005.3  TC\_NamedConf\_005.4  TC\_NamedConf\_005.5  TC\_NamedConf\_005.6  TC\_ FeatureLicense \_007.4  TC\_ FeatureLicense \_007.5  TC\_ FeatureLicense \_007.6  TC\_ FeatureLicense \_007.7  TC\_NamedConf\_006.4 |  |
| 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. | TC\_NamedConf\_004.3  TC\_NamedConf\_006.4  TC\_NamedConf\_005.2  TC\_FeatureLicense\_007.4  TC\_FeatureLicense\_007.5  TC\_FeatureLicense\_007.6 |  |
| **3.1.22      Serial Number Reprogram** | | | |
| 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. | TC\_DeviceManage\_007.1  TC\_DeviceManage\_007.2  TC\_DeviceManage\_007.3  TC\_DeviceManage\_009.1  TC\_DeviceManage\_009.2 |  |
| SRD-647 (CRITICAL) | The system shall store serial number reprogramming information in the associated device record. | TC\_DeviceManage\_007.1  TC\_DeviceManage\_007.2  TC\_DeviceManage\_007.3  TC\_DeviceManage\_009.1  TC\_DeviceManage\_009.2 |  |
| SRD-648 (CRITICAL) | The system shall provide a serial number reprogrammed notification to those users who are subscribed. | TC\_DeviceManage\_007.1  TC\_DeviceManage\_007.2  TC\_DeviceManage\_007.3  TC\_DeviceManage\_009.1  TC\_DeviceManage\_009.2  TC\_Alert\_010.1  TC\_Alert\_010.2  TC\_Alert\_010.3 |  |
| SRD-649 (CRITICAL) | The system shall record serial number reprogramming user activity into the user audit log. | TC\_DeviceManage\_007.1  TC\_DeviceManage\_007.2  TC\_DeviceManage\_007.3  TC\_DeviceManage\_009.1  TC\_DeviceManage\_009.2 |  |
| SRD-650 (CRITICAL) | The system shall display serial number reprogramming user activity in the user activity report. | TC\_DeviceManage\_007.1  TC\_DeviceManage\_007.2  TC\_DeviceManage\_007.3  TC\_DeviceManage\_009.1  TC\_DeviceManage\_009.2 |  |
| **3.1.23      Feature Licensing** | | | |
| SRD-557 | The System shall provide a view of the feature entitlement properties which are associated with a device as part of the device record view. | TC\_FeatureLicense\_012.2 |  |
| SRD-544 | The System shall provide a means to associate a single unique device feature with one or more device configurations. | TC\_FeatureLicense\_011.1  TC\_FeatureLicense\_011.2  TC\_FeatureLicense\_011.3  TC\_FeatureLicense\_011.4 |  |
| SRD-558 | The System shall provide a Feature Catalog, which contains Feature Items. | TC\_FeatureLicense\_001.1  TC\_FeatureLicense\_001.2 |  |
| SRD-988 | 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. | TC\_FeatureLicense\_001.1  TC\_FeatureLicense\_001.2 |  |
| SRD-559 | The System shall provide a means for a user with appropriate permissions to create, edit, clone and archive feature items in the Feature Catalog. | TC\_FeatureLicense\_001.1  TC\_FeatureLicense\_001.2  TC\_FeatureLicense\_002.1  TC\_FeatureLicense\_002.2  TC\_FeatureLicense\_004.1  TC\_FeatureLicense\_004.2 |  |
| SRD-987 | The System shall provide a Feature type of Named Configuration – i.e. a Named Feature Configuration. | TC\_FeatureLicense\_006.1 |  |
| SRD-566 | The System shall provide a means to create, edit, clone and archive Named Feature Configurations. | TC\_FeatureLicense\_006.1  TC\_FeatureLicense\_006.2  TC\_FeatureLicense\_007.1-  TC\_FeatureLicense\_007.7  TC\_FeatureLicense\_008.1-  TC\_FeatureLicense\_008.3 |  |
| SRD-560 | The System shall provide a means for a user with appropriate permissions to associate Feature Items in the Feature Catalog with Named Feature Configurations. | TC\_FeatureLicense\_006.1  TC\_FeatureLicense\_006.2 |  |
| SRD-561 | 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 thethe feature should not be deployed. | TC\_FeatureLicense\_001.1  TC\_FeatureLicense\_001.2 |  |
| SRD-999 | The System shall provide a means for a user with appropriate permissions to associate a Named Feature Configuration with a Named System Configuration | TC\_FeatureLicense\_010.1 |  |
| SRD-998 | The System shall provide a means to accept feature entitlement sales record data from the corporate enterprise repository. | N/A | Refer to RL 010 PLN-RPT DB ETL Tool v4.0.  \*Note: As ETL for license requirement is not clear, test cases are not designed in v4.0. |
| SRD-997 | 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. | N/A | Refer to RL 010 PLN-RPT DB ETL Tool v4.0.  \*Note: As ETL for license requirement is not clear, test cases are not designed in v4.0. |
| SRD-554 | The System shall store feature entitlement properties in the device record for permanent storage (This will be separate from last known device configuration). | FeatureLicense\_TC070  FeatureLicense\_TC080  FeatureLicense\_TC090 |  |
| SRD-996 | 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. | TC\_FeatureLicense\_011.1  TC\_FeatureLicense\_011.2  TC\_FeatureLicense\_011.3 |  |
| SRD-552 | The System shall provide a list of last known actually enabled features to the Client which are associated with a connected device. | FeatureLicense\_TC070  FeatureLicense\_TC080  FeatureLicense\_TC090 |  |
| SRD-553 | The System shall accept a list from the Client of currently enabled features for a device connected to the Client. | FeatureLicense\_TC070  FeatureLicense\_TC080  FeatureLicense\_TC090 |  |
| SRD-555 | The System shall record device feature enabled status received from the Client in the device running configuration. | FeatureLicense\_TC090  RunningConf\_TC040 |  |
| SRD-556 | On docking, the System shall provide to the Client a list of Feature Entitlements, and their properties, together with the last known device configuration. | RunningConf\_TC040 |  |
| SRD-995 | 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. | TC\_FeatureLicense\_001.1  TC\_FeatureLicense\_001.2  TC\_FeatureLicense\_011.1  TC\_FeatureLicense\_011.2  TC\_FeatureLicense\_011.3  TC\_FeatureLicense\_011.4 |  |
| SRD-994 | 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. | TC\_FeatureLicense\_011.1  TC\_FeatureLicense\_011.2  TC\_FeatureLicense\_011.3  TC\_FeatureLicense\_011.4 |  |
| SRD-993 | 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 | FeatureLicense\_TC070  FeatureLicense\_TC080  FeatureLicense\_TC090  RunningConf\_TC040 |  |
| SRD-992 | 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 | TC\_Report\_016.1  TC\_Report\_016.2  TC\_Report\_016.4  TC\_Report\_016.3 |  |
| SRD-991 | 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 | TC\_Report\_016.1  TC\_Report\_016.2  TC\_Report\_016.4  TC\_Report\_016.3 |  |
| SRD-990 | The System Device Feature Entitlement Report View shall have an option to print (TBD: save???) the report. | TC\_Report\_016.1  TC\_Report\_016.2  TC\_Report\_016.4  TC\_Report\_016.3 |  |
| SRD-989 | The System Device Feature Entitlement Report View shall print the following information.  •Title Page  oDevice Feature Entitlement Report for <UserName>  oCountries filtered  oCustomers filtered  oDevice Type  oFeature Types filtered  oEntitled filters  oEnabled filter  •Page 2+ Header  oCountries filter  oCustomers filter  oDevice Type  oFeature Types filter  oEntitled filter  oEnabled filter  •Page 2+ Body  oSection Headings   By Country  •By Customer  oColumns/Content   Device Serial Number   Filtered Features List (one per line)  •Entitlement ID  •Entitlement State (Entitled/Not Entitled)  •Entitlement Term  •Device Feature Enabled Status | TC\_Report\_016.1  TC\_Report\_016.2  TC\_Report\_016.4  TC\_Report\_016.3 |  |
| SRD-9974 | If feature entitlement constraints are violated, GDMP should inform user when the device is next docked. | TC\_FeatureLicense\_018.1  TC\_FeatureLicense\_018.2 |  |
| 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 | FeatureLicense\_TC070  FeatureLicense\_TC080  FeatureLicense\_TC090 |  |
| SRD-722 | The system shall allow administrator user to import feature license for devices from ETL. | N/A | Refer to RL 010 PLN-RPT DB ETL Tool v4.0.  \*Note: As ETL for license requirement is not clear, test cases are not designed in v4.0. |
| SRD-9979 | The System Shall provide a device-specific license in the form which is recognizable by the device. | TC\_FeatureLicense\_011.1  TC\_FeatureLicense\_011.2  TC\_FeatureLicense\_011.3  TC\_FeatureLicense\_011.4 |  |
| SRD-9978 | The System shall be capable of creating feature licenses which are specific to a particular device instance. | TC\_FeatureLicense\_011.1  TC\_FeatureLicense\_011.2  TC\_FeatureLicense\_011.3  TC\_FeatureLicense\_011.4 |  |
| 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. | TC\_FeatureLicense\_011.1  TC\_FeatureLicense\_011.2  TC\_FeatureLicense\_011.3  TC\_FeatureLicense\_011.4 |  |
| SRD-724 | The system shall provide to the client a license intended for a specific device. | FeatureLicense\_TC020 |  |
| SRD-564 | The System shall record device feature licensing operations in the device's and user's audit trail.\_ | TC\_FeatureLicense\_015.1 |  |
| SRD-565 | The System shall provide a means to notify users of device feature licensing operations | TC\_FeatureLicense\_016.1  TC\_FeatureLicense\_016.2 |  |
| SRD-9976 | The System shall provide a means for users to subscribe to one or more different device feature license operation notifications. | TC\_FeatureLicense\_016.1  TC\_FeatureLicense\_016.2 |  |
| SRD-634 | 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. | TC\_FeatureLicense\_016.3 |  |
| SRD- 635 | 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. | TC\_FeatureLicense\_016.4 |  |
| SRD-9975 | The system should generate an alert when temporary entitlements expire according to their license term. | TC\_FeatureLicense\_016.5 |  |
| 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. | TC\_FeatureLicense\_017.1 |  |
| 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 | TC\_FeatureLicense\_002.1  TC\_ FeatureLicense \_002.2  TC\_ FeatureLicense \_002.3  TC\_FeatureLicense\_003.1  TC\_FeatureLicense\_003.2  TC\_FeatureLicense\_003.3  TC\_FeatureLicense\_003.4  TC\_FeatureLicense\_003.5  TC\_FeatureLicense\_003.6 |  |
| SRD-1031 | User with appropriate permission can edit feature item based on below rule: | TC\_FeatureLicense\_002.1  TC\_FeatureLicense\_002.2  TC\_FeatureLicense\_002.3  TC\_FeatureLicense\_002.4 |  |
| SRD-1032 | User with appropriate permission can edit feature configuration based on below rule: | TC\_FeatureLicense\_007.1  TC\_FeatureLicense\_007.2  TC\_FeatureLicense\_007.3  TC\_FeatureLicense\_007.10 |  |
| SRD-1033 | User with appropriate permission can edit feature entitlement based on below rule: | TC\_FeatureLicense\_012.3  TC\_FeatureLicense\_012.4  TC\_FeatureLicense\_012.5  TC\_FeatureLicense\_012.6 |  |
| SRD-1035 | The System shall provide a means for a user with appropriate permissions to clone feature entitlement. | TC\_FeatureLicense\_013.1  TC\_FeatureLicense\_013.2 |  |
| 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. | TC\_FeatureLicense\_014.1  TC\_FeatureLicense\_014.2  TC\_FeatureLicense\_014.3  TC\_FeatureLicense\_014.4  TC\_FeatureLicense\_014.5 |  |
| 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. | TC\_FeatureLicense\_003.1  TC\_FeatureLicense\_003.2  TC\_FeatureLicense\_003.3  TC\_FeatureLicense\_003.4  TC\_FeatureLicense\_003.5  TC\_FeatureLicense\_003.6 |  |
| 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. | TC\_FeatureLicense\_016.3 |  |
| **3.1.24       System Activity Tracking** | | | |
| SRD-199 | The system shall maintain an audit trail of system activity. | TC\_Report\_008.1  TC\_Report\_008.2  TC\_Report\_008.3  TC\_Report\_008.4 |  |
| SRD-200 | The system shall keep activity logs that track logins. | TC\_UserMgt\_008.1  TC\_UserMgt\_008.2  TC\_UserMgt\_008.3  TC\_UserMgt\_008.4  TC\_UserMgt\_009.1  TC\_UserMgt\_009.2  TC\_UserMgt\_009.3  TC\_UserMgt\_009.4  TC\_UserMgt\_009.7  TC\_UserMgt\_009.8  TC\_UserMgt\_009.9  TC\_UserMgt\_009.10 |  |
| SRD-201 | The system shall keep activity logs tracking software upgrades. | TC\_Agent\_003.1-TC\_Agent\_003.4  TC\_Agent\_004.1-TC\_Agent\_004.4  TC\_Agent\_005.1-TC\_Agent\_005.4  TC\_Agent\_006.1-TC\_Agent\_006.4  TC\_Agent\_007.1-TC\_Agent\_007.4  TC\_Agent\_008.1-TC\_Agent\_008.4  TC\_Agent\_013.1-TC\_Agent\_003.12 |  |
| SRD-202 | The system shall keep activity logs tracking user activity through the gateway agent that runs on a Windows PC. | TC\_Report\_015.1  TC\_Report\_015.2  TC\_Report\_015.3  TC\_Report\_015.4 |  |
| 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) | TC\_Report\_015.1  TC\_Report\_015.2  TC\_Report\_015.3  TC\_Report\_015.4 |  |
| 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 | TC\_Report\_015.1  TC\_Report\_015.2  TC\_Report\_015.3  TC\_Report\_015.4 |  |
| 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 | TC\_Agent\_003.1-TC\_Agent\_003.4  TC\_Agent\_004.1-TC\_Agent\_004.4  TC\_Agent\_005.1-TC\_Agent\_005.4  TC\_Agent\_006.1-TC\_Agent\_006.4  TC\_Agent\_007.1-TC\_Agent\_007.4  TC\_Agent\_008.1-TC\_Agent\_008.4  TC\_Agent\_013.1-TC\_Agent\_003.12 |  |
| **3.1.25       Gateway Agent Maintenance** | | | |
| SRD-377 | The system shall maintain latest version of agent software. | TC\_Agent\_018.2 |  |
| SRD-378 | The system shall support a message whose contents are the current revision number for the agent software. | TC\_Agent\_018.2 |  |
| SRD-379 | The system shall check for updates to the agent software when agent connects to the server. | TC\_Agent\_018.1 |  |
| SRD-380 | The agent will download new version of itself if user’s machine is idle. | TC\_Agent\_018.1 |  |
| SRD-381 | The system shall install new versions of the agent software. | TC\_Agent\_018.1 |  |
| 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. | TC\_UserMgt\_009.1  TC\_UserMgt\_009.2  TC\_UserMgt\_009.3  TC\_UserMgt\_009.4  TC\_UserMgt\_009.7  TC\_UserMgt\_009.8  TC\_UserMgt\_009.9  TC\_UserMgt\_009.10 |  |
| SRD-754 | The system shall automatically sync user credentials as well as roles and permissions from GDMP server when agent is connected with server. | TC\_UserMgt\_009.1  TC\_UserMgt\_009.2  TC\_UserMgt\_009.3  TC\_UserMgt\_009.4  TC\_UserMgt\_009.7  TC\_UserMgt\_009.8  TC\_UserMgt\_009.9  TC\_UserMgt\_009.10 |  |
| SRD-763 | Agent should enforce the device serial number formatting. | TC\_DeviceManage\_007.1  TC\_DeviceManage\_007.2  TC\_DeviceManage\_007.3 |  |
| SRD-764 | GDMP agent shall record current version of agent in the registry of machine during installation process | TC\_Agent\_018.2 |  |
| 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. | TC\_DeviceManage\_001.7 |  |
| SRD-770 | Agent shall delete notifications if they have been delivered to client or server  By default it's 24 hours later. | TC\_Security\_008.1  TC\_Security\_008.2 |  |
| SRD-771 | Client application shall be able to get agent status such as GDMP server is available, GDMP server is connected from agent | TC\_Agent\_010.1  TC\_Agent\_010.2 |  |
| **3.1.26      Client Application Software Related Requirements** | | | |
| SRD-326 | The system shall maintain a list of client application software and their versions. | TC\_DeviceManage\_018.2 |  |
| SRD-327 | The system shall support a message whose contents are the current revision numbers for the client application software. | TC\_Agent\_019.1 |  |
| SRD-328 | The system shall check for updates to the client application software when the agent connects to the server. | TC\_Agent\_019.1 |  |
| SRD-329 | The agent will download new version of the client application software if available. | TC\_Agent\_019.1 |  |
| SRD-330 | Client application shall choose to install upgrade or not per its configuration. | TC\_Agent\_019.1 |  |
| SRD-749 | System shall allow user to download an Agent Installer from GDMP web after successful login. | TC\_Agent\_018.1 |  |
| **3.1.27       Alerts** | | | |
| SRD-182 | The system shall provide a user interface to allow users to subscribe and unsubscribe to alerts per device type. | TC\_Alert\_001.1  TC\_Alert\_001.3  TC\_Alert\_002.1  TC\_Alert\_002.3  TC\_Alert\_003.1  TC\_Alert\_003.2  TC\_Alert\_004.1  TC\_Alert\_004.2 |  |
| 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 configuration  Serial Number changed (realigned ) | TC\_Alert\_007.1  TC\_Alert\_008.1  TC\_Alert\_009.1  TC\_Alert\_010.1  TC\_Alert\_011.1  TC\_Alert\_012.1  TC\_Alert\_013.1 |  |
| 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. o Invalid configuration o Not all Components Found o 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) | TC\_Alert\_014.1  TC\_Alert\_015.1  TC\_Alert\_016.1  TC\_Alert\_017.1  TC\_Alert\_018.1 |  |
| SRD-645 (CRITICAL) | A Medtronic user can subscribe to alerts for operations on all devices for a particular device type. | TC\_Alert\_001.1  TC\_Alert\_001.5  TC\_Alert\_002.5  TC\_Alert\_002.1 |  |
| SRD-636 (CRITICAL) | A user with appropriate privileges may generate a General Notification to be issues for the following events:System upgrade notice,  general notification to users associating with Device Type | TC\_Alert\_005.1  TC\_Alert\_005.2  TC\_Alert\_005.3  TC\_Alert\_005.4  TC\_Alert\_005.5 |  |
| SRD-211 | The system shall use the email to notify end users of alerts. | TC\_Alert\_007.1  TC\_Alert\_008.1  TC\_Alert\_009.1  TC\_Alert\_010.1  TC\_Alert\_011.1  TC\_Alert\_012.1  TC\_Alert\_013.1  TC\_Alert\_014.1  TC\_Alert\_015.1  TC\_Alert\_016.1  TC\_Alert\_017.1  TC\_Alert\_018.2  TC\_Alert\_019.1 |  |
| SRD-215 | The system shall provide a means to filter alerts based on alert event type, device type and CoT. | TC\_Alert\_019.1 |  |
| SRD-216 | The system shall classify alerts according to alert event type. | TC\_Alert\_019.1 |  |
| SRD-217 | The alert event type text shall be in the subject line of the email. | TC\_Alert\_007.1  TC\_Alert\_008.1  TC\_Alert\_009.1  TC\_Alert\_010.1  TC\_Alert\_011.1  TC\_Alert\_012.1  TC\_Alert\_013.1 |  |
| SRD-637 (Gateway-1377) (CRITICAL) | The system shall support the following alert notification permissions, which can be applied to any role: a. Subscribe to alert notifications for devices serviced by user (across one or more selectable device types) i. Subscribe to informational alerts ii. Subscribe to business alerts b. Subscribe to alert notifications for all devices of a specific device type by Country or groups of countries i. Subscribe to informational alerts ii. Subscribe to business alerts c. 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) i. Subscribe to informational alerts ii. 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 | TC\_Alert\_007.1  TC\_Alert\_008.1  TC\_Alert\_009.1  TC\_Alert\_010.1  TC\_Alert\_011.1  TC\_Alert\_012.1  TC\_Alert\_013.1  TC\_Alert\_007.2  TC\_Alert\_008.2  TC\_Alert\_009.2  TC\_Alert\_010.2  TC\_Alert\_011.2  TC\_Alert\_012.2  TC\_Alert\_013.2  TC\_Alert\_005.1  TC\_Alert\_005.2  TC\_Alert\_005.3  TC\_Alert\_005.4  TC\_Alert\_005.5 |  |
| 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. | TC\_Alert\_005.1  TC\_Alert\_005.2 |  |
| SRD-638 (CRITICAL) | A non- Medtronic user with appropriate permissions can subscribe to alerts related to a particular device type | TC\_Alert\_003.1  TC\_Alert\_003.2  TC\_Alert\_004.1  TC\_Alert\_004.2 |  |
| 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. | TC\_Alert\_006.1 |  |
| SRD-577 (CRITICAL) | The system shall track the state of an alert. | TC\_Alert\_007.3  TC\_Alert\_008.3  TC\_Alert\_009.3  TC\_Alert\_007.4  TC\_Alert\_008.4  TC\_Alert\_009.4  TC\_Alert\_014.3  TC\_Alert\_014.4  TC\_Alert\_014.6  TC\_Alert\_014.7  TC\_Alert\_017.2 |  |
| SRD-578 (CRITICAL) | The states of alert shall include: - Pending - Sent - Duplicate  - Acknowledged - Resolved - Closed | TC\_Alert\_014.3  TC\_Alert\_023.6  TC\_Alert\_014.6  TC\_Alert\_014.7  TC\_Alert\_017.2 |  |
| SRD-579 (CRITICAL) | The system shall allow the collection of user comments on all alert state changes which are made by user. | TC\_Alert\_014.3TC\_Alert\_015.2  TC\_Alert\_016.2 |  |
| SRD-580 (CRITICAL) | The system shall provide a means for a user with appropriate privileges to view an alert state. | TC\_Alert\_014.3  TC\_Alert\_024.3  TC\_Alert\_025.3  TC\_Alert\_017.2  TC\_Alert\_027.3  TC\_Alert\_019.1 |  |
| SRD-582 (CRITICAL) | The system shall allow a user with appropriate privileges to transition an Alert from Sent to Acknowledged. | TC\_Alert\_014.3  TC\_Alert\_014.4  TC\_Alert\_014.5  TC\_Alert\_014.6 |  |
| SRD-583 (CRITICAL) | The system shall allow a user with appropriate privileges to transition an Alert from Acknowledged to Resolved. | TC\_Alert\_014.3  TC\_Alert\_014.5  TC\_Alert\_014.6 |  |
| SRD-643 (CRITICAL) | The system shall allow a user with appropriate privileges to transition an Alert from Resolved to Closed. | TC\_Alert\_014.3  TC\_Alert\_014.5  TC\_Alert\_014.6  TC\_Alert\_014.7 |  |
| SRD-585 (Gateway 1377) (CRITICAL) | The system shall allow a user to enable/disable their individual alerts. | TC\_Alert\_001.2  TC\_Alert\_001.4  TC\_Alert\_002.2  TC\_Alert\_002.4 |  |
| SRD-586 (CRITICAL) | The system shall provide an interface to view all alerts. | TC\_Alert\_019.1 |  |
| 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. | TC\_Alert\_007.1  TC\_Alert\_008.1  TC\_Alert\_009.1  TC\_Alert\_010.1  TC\_Alert\_011.1  TC\_Alert\_012.1  TC\_Alert\_013.1  TC\_Alert\_007.2  TC\_Alert\_008.2  TC\_Alert\_009.2  TC\_Alert\_010.2  TC\_Alert\_011.2  TC\_Alert\_012.2  TC\_Alert\_013.2 |  |
| 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. | TC\_Alert\_024.1  TC\_Alert\_015.1  TC\_Alert\_025.1  TC\_Alert\_016.1  TC\_Alert\_026.1  TC\_Alert\_017.1  TC\_Alert\_018.1  TC\_Alert\_018.2 |  |
| 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. | TC\_Alert\_024.1  TC\_Alert\_015.1  TC\_Alert\_025.1  TC\_Alert\_016.1  TC\_Alert\_026.1  TC\_Alert\_017.1  TC\_Alert\_018.1  TC\_Alert\_018.2  TC\_Alert\_007.1  TC\_Alert\_008.1  TC\_Alert\_009.1  TC\_Alert\_010.1  TC\_Alert\_011.1  TC\_Alert\_012.1  TC\_Alert\_013.1  TC\_Alert\_007.2  TC\_Alert\_008.2  TC\_Alert\_009.2  TC\_Alert\_010.2  TC\_Alert\_011.2  TC\_Alert\_012.2  TC\_Alert\_013.2 |  |
| 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. | TC\_Alert\_020.1  TC\_Alert\_020.2 |  |
| SRD-1026 | 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. | TC\_Alert\_001.1  TC\_Alert\_001.2  TC\_Alert\_002.1  TC\_Alert\_002.2 |  |
| SRD-1027 | Individual user can receive alert notification mail only after subscribe the alert for himself. | TC\_Alert\_001.3 TC\_Alert\_002.3 |  |
| **3.1.28       Reporting** | | | |
| SRD-805 | *All items in filter drop down lists shall be displayed in alphabetical order.* | TC\_Report\_017.2 |  |
| SRD-806 | *All filter drop down lists shall be searchable by entering at least the first 3 characters of the item name.* | TC\_Report\_017.3 |  |
| SRD-807 | *All items in the filter drop down lists shall be displayed when the user types in 3 space characters.* | TC\_Report\_017.3 |  |
| SRD-808 | *The system shall allow the user to sort a displayed report based on any column.* | TC\_Report\_017.4 |  |
| SRD-809 | *The system shall provide tooltips on each entry of reports.* | TC\_Report\_017.5 |  |
| 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.* | TC\_Report\_001.3  TC\_Report\_002.3  TC\_Report\_003.3  TC\_Report\_004.4  TC\_Report\_005.4  TC\_Report\_006.4  TC\_Report\_007.4  TC\_Report\_008.4  TC\_Report\_009.3  TC\_Report\_010.4  TC\_Report\_011.4  TC\_Report\_012.3  TC\_Report\_013.3  TC\_Report\_014.3  TC\_Report\_015.4  TC\_Report\_016.3 |  |
| SRD-811 | *The system shall allow user to search for these filters of User name, Customer name and Device serial number with partial keyword.* | TC\_Report\_017.6 |  |
| SRD-812 | *The system shall allow user to type a date of MM/DD/YYYY format for those date type filters.* | TC\_Report\_017.7 |  |
| 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. | TC\_Report\_005.3  TC\_Report\_011.4  TC\_Report\_014.4  TC\_Report\_006.3 |  |
| SRD-639 (CRITICAL) | The system shall control access to reports based on roles, permissions, CoT, and user type. | TC\_Report\_018.1 |  |
| 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. | TC\_Report\_001.1  TC\_Report\_001.2  TC\_Report\_001.4  TC\_Report\_001.5 |  |
| 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 | TC\_Report\_002.1  TC\_Report\_002.2  TC\_Report\_002.3  TC\_Report\_003.1  TC\_Report\_003.2  TC\_Report\_003.3 |  |
| 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. | TC\_Report\_002.1  TC\_Report\_002.2  TC\_Report\_002.3 |  |
| 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. | TC\_Report\_003.1  TC\_Report\_003.2  TC\_Report\_003.3 |  |
| 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. | TC\_Report\_004.2  TC\_Report\_004.3  TC\_Report\_004.4 |  |
| 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 | TC\_Report\_005.1  TC\_Report\_005.2  TC\_Report\_005.3  TC\_Report\_005.4 |  |
| SRD-660 (GW\_RSS\_RQ\_61) (HIGH) | 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) | TC\_Report\_006.1  TC\_Report\_006.2  TC\_Report\_006.3  TC\_Report\_006.4 |  |
| 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. | TC\_Report\_006.1  TC\_Report\_006.2  TC\_Report\_006.3  TC\_Report\_006.4 |  |
| SRD-664 (HIGH) (Must Have) | 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. | TC\_Report\_007.1  TC\_Report\_007.2  TC\_Report\_007.3  TC\_Report\_007.4 |  |
| SRD-640 | 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. 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. | TC\_Report\_017.1 |  |
| 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 | TC\_Report\_008.1  TC\_Report\_008.2  TC\_Report\_008.3  TC\_Report\_008.4 |  |
| 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 | TC\_Report\_009.1  TC\_Report\_009.2  TC\_Report\_009.4  TC\_Report\_009.3 |  |
| 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 | TC\_Report\_010.1  TC\_Report\_010.2  TC\_Report\_010.3  TC\_Report\_010.4 |  |
| 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. | TC\_Report\_010.1  TC\_Report\_010.2  TC\_Report\_010.3  TC\_Report\_010.4 |  |
| 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 | TC\_Report\_011.1  TC\_Report\_011.2  TC\_Report\_011.3  TC\_Report\_011.4 |  |
| 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 | TC\_Report\_012.1  TC\_Report\_012.2  TC\_Report\_012.4  TC\_Report\_012.5  TC\_Report\_012.3 |  |
| 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. | TC\_Report\_012.1  TC\_Report\_012.2  TC\_Report\_012.4  TC\_Report\_012.5  TC\_Report\_012.3 |  |
| 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 | TC\_Report\_012.1  TC\_Report\_012.2  TC\_Report\_012.4  TC\_Report\_012.5  TC\_Report\_012.3 |  |
| 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. | TC\_Report\_013.1  TC\_Report\_013.2  TC\_Report\_013.4  TC\_Report\_013.3 |  |
| 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. | TC\_Report\_014.1  TC\_Report\_014.2  TC\_Report\_014.4  TC\_Report\_014.3 |  |
| 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) | TC\_Report\_015.1  TC\_Report\_015.2  TC\_Report\_015.3  TC\_Report\_015.4 |  |
| SRD-1004 | The system shall allow only users with User Management permissions or System Admin permissions to run the User Activity Report. | TC\_Report\_015.1  TC\_Report\_015.2  TC\_Report\_015.3  TC\_Report\_015.4 |  |
| **3.1.29      Part 11 Compliance and Related Requirements** | | | |
| SRD-134 | The system shall be 21CFR Part 11 compliant to the extent that each upgrade record is considered an electronic record. | TC\_Report\_001.1  TC\_Report\_001.2  TC\_Report\_001.4  TC\_Report\_001.3 |  |
| SRD-135 | The system shall not delete records or data rows that are part of the audit trail. | TC\_Report\_008.1  TC\_Report\_008.2 |  |
| SRD-136 | The system shall mark data records as inactive when asked to delete them. | TC\_UserMgt\_004.2 |  |
| SRD-299 | Service records shall be time-stamped with network time on the server Note: Required for Part 11 Section 7.1.8.1 | TC\_Report\_012.4  TC\_Report\_015.3 |  |
| 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. | TC\_Report\_015.3  TC\_Report\_008.3 |  |
| SRD-184 | Record changes shall append to previously recorded information | TC\_Report\_012.4  TC\_Report\_005.3 |  |
| SRD-185 | Audit trails must be retained for as long as the underlying records as required for the records. | N/A | Cannot be traced to test case. This requirement can be covered by Gateway Backup Strategy and Procedure document which is listed in section 1.3 reference [3] |
| SRD-186 | Access to modify the system or records must be limited to authorized roles. | TC\_RolePermission\_001.1  TC\_RolePermission\_001.2  TC\_RolePermission\_001.3  TC\_RolePermission\_001.4  TC\_RolePermission\_001.5 |  |
| 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 | TC\_Report\_008.4 |  |
| SRD-301 | The system shall allow selectable portion of the audit trail to be printed Note: Required for Part 11 Section 6.5.12 | TC\_Report\_008.4 |  |
| SRD-302 | The system shall allow selectable portions of the audit trail to be viewed Note: Required for Part 11 Section 6.5.12 | TC\_Report\_008.2 |  |
| SRD-303 | Users shall be able to archive software packages on the server  Note: Required for Part 11 Section 6.5.8 | TC\_HWSW\_006.4 |  |
| SRD-304 | Users shall not be able to delete software packages from the server Note: Required for Part 11 Section 6.5.8 | TC\_HWSW\_006.4 |  |
| SRD-305 | Users shall not be able to modify or delete service records Note: Required for Part 11 Section 6.5.8 | TC\_Report\_012.4 |  |
| 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 | TC\_Report\_012.4  TC\_Report\_011.4  TC\_Report\_005.4 |  |
| SRD-307 | The system shall protect the system date and time from unauthorized change Note: Required for Part 11 Section 6.5.7 | N/A | This requirement is fullfilled by GRSP SysOps Guide [13] |
| SRD-308 | Users shall not be able to disable the audit trail function Note: Required for Part 11 Section 6.5.4 | N/A | This requirement is fullfilled by GRSP SysOps Guide [13] |
| SRD-309 | The audit trail must be read-only Note: Required for Part 11 Section 6.5.3 | TC\_Report\_008.3 |  |
| SRD-310 | The system shall protect records against intentional or accidental modification or deletion Note: Required for Part 11 Section 6.4.1 | TC\_Report\_008.3 |  |
| SRD-311 | The system shall check for the expected device type connected before allowing software updates Note: Required for Part 11 Section | TC\_Agent\_003.1  TC\_Agent\_004.1  TC\_Agent\_005.1  TC\_Agent\_006.1  TC\_Agent\_007.1  TC\_Agent\_008.1 |  |
| 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 | TC\_Report\_012.3 |  |
| 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 | TC\_Report\_012.3 |  |
| 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 | TC\_Report\_012.3 |  |
|  | | | |
| **3.1.31      Gateway Agent Installer Requirements** | | | |
| SRD-432 | The system shall provide an installation tool to install the Gateway Agent and its dependent packages. | AgentSCDUInstallTestProcedure  AgentESSInstallTestProcedure  AgentVLEXInstallTestProcedure | IQ test procedures Refer to [2] |
| SRD-796 | Implement new strategy for warning user if disk space will be exceeded during system operation. | InstallAgentOnDiskLower9GB  AgentSilentInstallLower9GBTestProcedure | IQ test procedures Refer to [2] |
| SRD-433 | The installation tool shall be a single executable program. | AgentSilentInstallTestProcedure | IQ test procedures Refer to [2] |
| SRD-434 | The installation tool shall run on 32/64 bits Windows XP SP3/Windows 7 Operating Systems. | InstallAgentInDifferentOSLanguages | IQ test procedures Refer to [2] |
| SRD-435 | The installation tool shall provide a UI to guide the installation of the Gateway Agent. | InstallAgentLargerthan9GBTestProcedure  InstallAgentWithDiskSpace9GBTestProcedure  AgentSilentInstallLower9GBTestProcedure | IQ test procedures Refer to [2] |
| SRD-441 | The Agent installation tool shall ensure availability of at least 9 GB disk space before installing the Gateway Agent. | AgentSilentInstallTestProcedure | IQ test procedures Refer to [2] |
| SRD-797 | Agent installer shall display an error message and stop installing if user doesn’t have windows admin privilege to do the installation. | AgentSilentInstallTestProcedure | IQ test procedures Refer to [2] |
| **3.1.32       Recommended Requirements for Client Application Installer** | | | |
| SRD-437 | The system shall provide an installation tool to install the Client Application and its dependent packages. | AgentSCDUInstallTestProcedure  AgentESSInstallTestProcedure | IQ test procedures Refer to [2] |
| SRD-438 | The installation tool shall be a single executable program. | AgentSCDUInstallTestProcedure  AgentESSInstallTestProcedure | IQ test procedures Refer to [2] |
| SRD-439 | The installation tool shall run on 32/64 bits Windows XP SP3/Windows 7 Operating Systems. | AgentSCDUInstallTestProcedure  AgentESSInstallTestProcedure | IQ test procedures Refer to [2] |
| SRD-440 | The installation tool shall provide a UI to guide the installation of the Client Application. | AgentSCDUInstallTestProcedure  AgentESSInstallTestProcedure | IQ test procedures Refer to [2] |
| **3.1.33** **Common Client related Requirements** | | | |
| SRD-691 | The system shall return all devices of a specific facility via agent | DeviceList\_TC010  DeviceList\_TC040 |  |
| 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. | FeatureLicense\_TC020 | . |
| SRD-719 | The system shall provide a way to let client get timestamp of last uploaded log file for a given device | ScheduleLog\_TC010  ScheduleLog\_TC011  ScheduleLog\_TC012 | . |
| 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. | RetrieveLog\_TC020  RetrieveLog\_TC021 |  |
| 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 | TC\_Report\_015.3 |  |
| SRD-735 | The system shall allow client to upload/download user activities to/from the Server.. | N/A | CC is not in test scope. |
| SRD-750 | When downloading to Agent, the system shall provide download completion percentage of the completion. | RegisterMissing\_TC031 | CC is not in test scope. |
| SRD-751 | GDMP Agent shall allow multiple users to sign on concurrently. | TC\_UserMgt\_018.3 |  |
| SRD-755 | The system shall support decoding binary format device log files retrieved from device. | RetrieveLog\_TC022 | . |
| SRD-757 | The system shall allow user to search Device log file by criteria via web UI (time duration, device type). | TC\_ DeviceManage \_011.3 |  |
| 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. | TC\_Security\_008.1  TC\_Security\_008.2  TC\_Security\_008.3 |  |
| SRD-761 | The system shall enable a user to view the complete feature list of a given device along with and enabled feature list. | FeatureLicense\_TC070  FeatureLicense\_TC080  FeatureLicense\_TC090 |  |
| SRD-762 | The system shall support distribute files (configuration, Software/Hardware package, feature licensing) in streaming approach to downstream client applications. | RegisterMissing\_TC031  RegisterMissing\_TC060 |  |
| SRD-765 | Agent shall cache user activities from Common Client. The period of how long user activities cached in Agent shall be configurable. | N/A |  |
| 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. | RetrieveLog\_TC022 |  |
| **3.1.34 Trade Embargo** | | | |
| 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. | TC\_HWSW\_010.1  TC\_HWSW\_010.2  TC\_HWSW\_010.3  TC\_HWSW\_010.4  TC\_HWSW\_010.5  TC\_HWSW\_010.5 |  |
| SRD-398 | The system shall only provide software to countries where no trade embargo exists. | TC\_HWSW\_010.1  TC\_HWSW\_010.2  TC\_HWSW\_010.3  TC\_HWSW\_010.4  TC\_HWSW\_010.5  5 |  |
| **3.1.35 Device Hardware** | | | |
| SRD-694 | Hardware shall not be deleted (archived) if there is a software associated with it. | TC\_HWSW\_002.3 |  |
| SRD-695 | System shall allow CoT Admin user to associate documents with hardware in order to provide instructions or information to the end users. | TC\_HWSW\_001.1  TC\_HWSW\_001.2 |  |
| 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. | TC\_HWSW\_004.1 |  |
| SRD-699 | System shall allow user to clone existing hardware item in order to create new hardware item | TC\_HWSW\_003.1  TC\_HWSW\_003.2 |  |
| SRD-700 | System shall allow user to see the clone map of hardware items , such as parent, siblings, and children. | TC\_HWSW\_004.1 |  |
| 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. | TC\_HWSW\_001.1  TC\_HWSW\_001.2  TC\_HWSW\_001.3 |  |
| SRD-702 | System shall allow CoT Admin user to be able to edit an existing hardware item based on below rule | TC\_HWSW\_002.1  TC\_HWSW\_002.2  TC\_HWSW\_002.3  TC\_HWSW\_002.4  TC\_HWSW\_002.5 |  |
| SRD-703 | System shall allow CoT Admin user to be able to track status of hardware as in ”Limited Release”, “In Production” or “Archived”. | TC\_HWSW\_002.2  TC\_HWSW\_002.3  TC\_HWSW\_002.4 |  |
| 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 | TC\_HWSW\_002.6  TC\_HWSW\_002.7  TC\_HWSW\_002.8  TC\_HWSW\_002.9  TC\_HWSW\_002.10  TC\_HWSW\_002.11  TC\_HWSW\_002.12  TC\_HWSW\_002.13  TC\_HWSW\_002.14  TC\_HWSW\_002.15  TC\_HWSW\_002.16  TC\_HWSW\_002.17  TC\_HWSW\_002.18  TC\_HWSW\_002.19 |  |
| SRD-705 | System shall allow user to search hardware by hardware name, or device type, or hardware type. | TC\_HWSW\_004.2 |  |
| **3.1.36 Gateway Log -Viewer Requirements** | | | |
| SRD-900 (SSRD46) | The Gateway Log Viewer shall provide a link for users to view and download device logs in device log viewer page. | TC\_DeviceManage\_008.4  TC\_DeviceManage\_008.6  TC\_DeviceManage\_008.11  TC\_DeviceManage\_008.13  TC\_DeviceManage\_008.15 |  |
| SRD-901 | The Gateway Log Viewer shall provide a means for users to filter the Log Viewer list by log type. | TC\_ DeviceManage \_011.3 |  |
| 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 | TC\_ DeviceManage \_011.3 |  |
| 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) | TC\_DeviceManage\_008.6  TC\_DeviceManage\_008.15 |  |
| **3.1.37 UI Validation** | | | |
| SRD-793 | Data input on UI shall be validated. The field should include:   1. User Name: only alphabet is allowed 2. Email: follow email format 3. Role name: only alphabet, number and ‘\_’ 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 | TC\_UserMgt\_003.2  TC\_UserMgt\_010.2  TC\_RolePermission\_002.1  TC\_RolePermission\_002.2  TC\_Report\_017.7  TC\_HWSW\_001.4  TC\_HWSW\_005.4  TC\_Doc\_003.1  TC\_Doc\_003.2 |  |