1. Description

1.1. Overview

This Product Update contains modifications for the version 1.5 of the Development Library Test Packs. Development Library version 1.5 is only supported with version 4.4.0 of the 8100 Mobile Device Test System.

This update can also be found at the Spirent Customer Service Center website: http://support.spirent.com.

Use the e-mail address and password assigned to you by Spirent to log into the Members section, and select Software Downloads>All Software>Wireless Applications to access the latest release.

1.2. New Features

1.2.1. Simulated Drive Test

- HSDPA Serving Cell Change
- Rate Shift to/from R99 UL / HSDPA DL to/from R99 UL / R99 DL
- Voice + Data dormancy to PS Idle/RAB Release (Dormancy)
- CS + PS Supplementary Service with multi-RAB call
- Pre-R8 SCRI Handling
- Automatic Retry for Failed Test Cases
- SDT Report Updates

1.2.2. Radio Policy Manager

- There are no new features in the current release.

1.2.3. Voice Quality

- Support for the Quad-capture UA-55 audio capture device.

1.2.4. Device Aggression Management

- There are no new features in the current release.
1.2.5. **Service Interaction - AGPS**

- There are no new features in the current release.

1.2.6. **Fast Dormancy**

- **Signaling Connection Release Indication**: A new parameter has been added to the Network Configuration editor that enables SCRI adversarial testing. Access this parameter by selecting `System>Adversarial Testing>RRC>Signaling Connection Release Indication`.
- **New Data Inactivity Timers**: The timers have been added to the Network Configuration Editor for Primary to CELL_FACH, CELL_FACH to Idle, CELL_FACH to URA_PCH, and URA_PCH to Idle. Access these timers by selecting `NAS>SM>Data Inactivity Timer Settings`.
- **Enable Network Initiated Recovery from URA_PCH State**: A new parameter has been added to the Network Configuration Editor to allow downlink IP activity activate the RAB. Access this parameter by selecting `NAS>SM>PS RAB Recovery Settings`.
- **T323 Timer**: A new parameter has been added to the Network Configuration Editor that allows you to configure the T323 timer. Access this parameter by selecting `NAS>SM>T323 Timer`.
- **CN DRX Cycle**: A new parameter has been added to the Network Configuration Editor that allows you to configure the CN DRX Cycle length. Access this parameter by selecting `NAS>CN>CN DRX Cycle`.
- **Conditional Wait**: New Core Test Pack action step.
- **Ping**: New Core Test Pack action step.
- **Start/Stop RLC Protocol Logging**: New Core Test Pack action step.
- **Start/Stop RRC State Logging**: New Core Test Pack action step.
- **Continue – Fail Result**: New Core Test Pack Query Step Common Parameter.
- **Get SCRI Statistics**: New Core Test Pack Query Step.
- **RRC State Transition**: New Core Test Pack Query Step.

1.3. **Maintenance Updates**

1.3.1. **Simulated Drive Test**

- There are no maintenance updates for this release.

1.3.2. **Radio Policy Manager**

- Radio Policy Management Suite Installer now includes a more descriptive document on how to perform the manual verification steps.
In last release, sometimes SR3420 would release RRC connection before sending Radio GMM Attach Reject message to UE which would cause UE to resend GMM Attach Request message. This would lead to Radio Policy Management counting GMM Attach Request message incorrectly. This issue has been fixed.

1.3.3. **Voice Quality**

- Support for Quad-capture UA-55 audio capture device.

1.3.4. **Device Aggression Management**

- There are no maintenance updates for this release.

1.3.5. **Service Interaction - AGPS**

- There are no maintenance updates for this release.

1.3.6. **Fast Dormancy**

- N/A

1.4. **Known Issues**

- On Windows 7 Client Laptops, IPv6 must be disabled for the TestDrive Data Modem connection.
  
  To disable IPv6:
  - Select **Start>Control Panel>Network and Internet>Network & Sharing Center**.
  - On the left side, click **Change Adapter Settings**.
  - Right-click the **TestDrive Data Connection** icon and select **Properties**.
  - Under the **Networking** tab, deselect **Internet Protocol Version 6 (TCP/IP)**.
  - Repeat the above steps for "TestDrive Data Connection (Backup)".

- The Broadcom NIC driver on the SR3920 Application Server has been found to be the root cause of throughput related issues. The driver on the Application Server must be upgraded to the latest version. Refer to Chapter 6 to upgrade the driver.

- Secondary Cell Power is set to the Primary Cell Power for cells mapped to Channels 3 and 4 on the A304 platform (RX Diversity only).

- The NIC interface on the SR3920 Application server has a parameter called “IPv4 Large Send Offload” enabled by default. This can cause potential data throughput issues. We recommend that you disable the “IPv4 Large Send Offload” parameter to ensure reliable data throughput performance.
• There is an issue with removing the test data cards and test phones from Dell Latitude E6500 Client Laptops connected via the PCMCIA slot or USB. If the client laptop model is a Dell Latitude E6500, refer to Chapter 4 on page 23. For any other client laptop model, skip Chapter 4.

• There is a potential conflict that can occur if the device installs a Network Interface driver. Refer to Chapter 5 on page 24 for information on resolving this problem.

• Devices that utilize a Network Interface Connection (NIC) and dynamically assign an IP address to the interface may not work with Simulated Drive Test. A potential workaround is to use the *ICS* mode under the *Spirent Data Client* tab of the UE file.

• For a T-Mobile service interaction test number:
  - **TMO-1.2**: 3G Single Cell User Plane to Control Plane A-GPS session transition - Automatic 911 call dial-up.
  - **TMO-1.2**: 3G Single Cell User Plane to Control Plane A-GPS session transition - Manual 911 call dial-up or

A *TestStand Critical Message* may display at the beginning of a test case, as shown in Figure 1-1. We highly recommend that you do not close this window for the duration of the test session.

![Test Manager (TestStand Engine)](image)

Figure 1-1: TestStand Engine Critical Message Window

• The following Development Library steps may not work for RA version 4.5.0 and higher:
  - Call State query following a 2G to 3G inter-rat handover
  - Hard Handover + HSDPA to R99 rate shift action step
  - Hard Handover + R99 to HSDPA rate shift action step
2. Product Upgrade Instructions

2.1. Overview

The following section contains the steps necessary to upgrade the Development Library Test Packs to the latest release.

These steps include:

- Downloading the Radio Access Test 4.4.0 Installation Package from the Customer Support website.
- Unzipping the files into a known location. For example, "C:\Program Files\Spirent Communications\Installations\8100 4.4.0 Installer".

2.2. Verifying Microsoft .NET Framework 2.0 Service Pack 1 and 3.5 Service Pack 1

If the appropriate Microsoft .NET Framework is not installed, an Initialization Error window displays, as shown in Figure 2-1.

**NOTE:** Some 8100 System Applications have a dependency on Microsoft .NET Framework 3.5 SP1. If .NET Framework 3.5 SP1 is not installed, an error message will display.

To verify and install the appropriate software, if necessary:

1. Select **Start > Control Panel > Add/Remove Programs.**
2. Verify the Microsoft .NET Framework 2.0 Service Pack 1 is installed, as shown in Figure 2-2.
If the correct Service Pack is not installed, follow the instructions given below.

**To install Microsoft .NET Framework 2.0 SP1:**
1. Navigate to the root directory where the *8100 MDT Installation Package* is saved.
2. Open the .NET Framework folder by selecting `[root]/Microsoft/Microsoft .NET Framework 2.0 SP1`.
3. Run the `NetFx20SP1_x86.exe` file

**To install Microsoft .NET Framework 3.5 SP1:**
1. Navigate to the root directory where the *8100 MDT Installation Package* is saved.
2. Open the .NET Framework folder by selecting `[root]/Microsoft/Microsoft .NET Framework 3.5 SP1`.
3. Run the `dotnetfx35sp1.exe` file

### 2.3. Upgrading the Development Library Test Packs

**NOTE:** Contact your local Spirent Sales Manager if new or additional passwords are required for the updated features.

The table below includes 8100 MDT System applications that must be installed on completion of the installation procedure.

<table>
<thead>
<tr>
<th>Software</th>
<th>Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>AirAccess WCDMA HS</td>
<td>4.50.104</td>
</tr>
<tr>
<td>SR5500 TestKit</td>
<td>3.51.002</td>
</tr>
<tr>
<td>Spirent WCE-IAPI</td>
<td>3.51.068</td>
</tr>
<tr>
<td>UDM</td>
<td>4.7.1</td>
</tr>
<tr>
<td>Spirent Data Client</td>
<td>1.13.223</td>
</tr>
<tr>
<td>TCU Configuration Tool</td>
<td>1.1.20</td>
</tr>
<tr>
<td>Test Manager</td>
<td>2.7.333</td>
</tr>
<tr>
<td>Custom Report Engine</td>
<td>1.1.17</td>
</tr>
<tr>
<td>Spreadsheet Report Engine</td>
<td>1.5.71</td>
</tr>
<tr>
<td>Development Library Services</td>
<td>1.70.008</td>
</tr>
</tbody>
</table>
To begin the upgrade procedure:

1. On the Controller PC, close all opened applications, including Test Stand Sequence Editor, Test Manager, AirAccess WCDMA-HS, SR5500 TestKit, and Spirent Data Client.

2. Start Test Manager and select Help> About > Passwords.

3. Click the Export button and close Test Manager.

4. Select the setup.exe file to open the 8100 MDT Global Installer. The **8100 Mobile Device Test System Installer** window displays, as shown in Figure 2-3.
Figure 2-3: 8100 Mobile Device Test System Installer Window

The following list describes the different symbols in the Global Installer:

- **The software is not installed.**
- **A different version of the software is already installed.**
- **The software is selected for install (also displays in the install list).**

**NOTE:** You cannot select software already installed with the same version, as shown by the *TCU Configuration Tool* item in Figure 2-3.
To install the software:

1. In the *Global Installer* window, select the **Instruments** tab.

2. Ensure the following applications are already installed or selected for install, as shown in Figure 2-4:
   a. AirAccess WCDMA-HS
   b. Spirent Data Client
   c. Universal DM V2
   d. TCU Configuration Tool

![Global Installer Window – Instruments Tab](image)

*Figure 2-4: Global Installer Window – Instruments Tab*

3. Under the *Test Manager* tab, ensure the following applications are already installed or selected for install, as shown in Figure 2-5:
   a. Test Manager
   b. Custom Report Engine
   c. Spreadsheet Report Engine
4. Under the **Platforms** tab, select the appropriate platform for your system, as shown in Figure 2-6.

![Figure 2-6: Global Installer Window – Platform Tab](image)

**NOTE:** If you have multiple platforms in your system, we recommend you install one platform at a time.

5. Under the **Development Library** tab, select the **Development Library Test Packs**, as shown in Figure 2-7.
NOTE: You can choose not to install Test Packs that you have not purchased.

6. Click the **Installation** button, as shown in Figure 2-8 to begin all installations.

7. Restart the computer.
To complete the procedure:

1. Add the exported passwords to Test Manager.
2. Delete all older platform files.
   In Test Manager, select File>Open>Platform File.
3. Create a new platform file.
   In Test Manager, select File>New>Platform File.
4. Open all UE Files from previous versions.
   In Test Manager, select File>New>UE File and save the old UE Files again.
5. Open all Session Files from previous versions.
   In Test Manager, select File>New>Session File and save the old Session Files again.
6. Run a System Calibration for the platforms.

2.4. Upgrade Procedure for the Client Laptop

1. Select Start>Control Panel>Add/Remove Programs.
2. Uninstall the Spirent AT Control application.
3. Uninstall the Spirent Data Client application.
   If necessary, restart the computer and continue with Step 4.
4. Install the Spirent Data Client application from the "Spirent Data Client" folder in the downloaded Radio Access Package.
5. Install the Spirent AT Control application from the "Spirent AT Control" folder in the downloaded Radio Access Package.
6. Restart the Client Laptop.

**NOTE:** Due to changes to the TCP/IP OS Parameters, you must reboot the Client Laptop and Application Server after upgrading the Data Client Application.
2.5. Upgrade Procedure for the Application Server

1. From the Controller PC, go to the Remote Desktop and enter **192.168.0.70**.
2. Select **Start>Control Panel>Add/Remove Programs**.
3. Uninstall the **Spirent Data Client** application.
   If necessary, restart the PC and continue with Step 4.
4. Install the **Spirent Data Client** application from the "Spirent Data Client" folder in the downloaded Radio Access Package.
5. Open FileZilla by selecting the **FileZilla Server Interface** from the desktop.
6. Select **Edit>Settings**.
7. From the menu, select the **Miscellaneous** option, as shown in Figure 2-9.
8. Set the **Internal transfer buffer size** to **1420**.
9. Set the **Socket buffer size** to **130640**.

   ![FileZilla Server Options Window](image)

   **Figure 2-9: FileZilla Server Options Window**

10. Click **OK** and close the FileZilla application.
11. Restart the Application Server.

**NOTE:** You must reboot the Application Server after upgrading the Data Client Application due to changes to the TCP/IP OS Parameters.
3. Additional Configurations

3.1. Trigger Cable Change

1. For all platforms except the A050, refer to the Rack Setup Guide.
2. Start the Test Manager Application by selecting Start>All Programs>Spirent Communications>Test Manager.
3. In the Test Manager window, select Help>Platforms>[Installed Platform].
4. Navigate to the BNC and Data Connections section.
5. Verify the SR3420 CH2 Sync OUT BNC cable is connected properly.

3.2. Deleting Unused Test Manager Passwords

1. Start the Test Manager Application by selecting Start>All Programs>Spirent Communications>Test Manager.
2. In the Test Manager window, select Help>About.
3. Under the Passwords tab, select Network Emulation Building Block (MDTTM-NETWORK-EM-BB-SW) in the Installed Features section (if the feature is available). Delete the password.
4. Select Spirent Data Client (MDTTM-DATA-CLIENT-SW) in the Installed Features section (if the feature is available). Delete the password.
5. Click OK to close the About window.
6. Close the Test Manager Application.

3.3. Disabling the McAfee Automatic Scan Option

For optimum system performance, make sure the automatic scan option in the McAfee Virus Scan software is disabled.

To disable the Automatic Scan option:

1. Open McAfee Security Center by selecting Start>All Programs>McAfee>McAfee Security Center.
   The McAfee Security Center window displays, as shown in Figure 3-1.
2. In the Common Tasks section, select the Advanced menu.

3. In the Home section, select Configure.

4. In the Configure section, select Computer & Files. Click the Advanced button in the Virus protection is enabled section, as shown in Figure 3-2. The Advanced Options window displays, as shown in Figure 3-3.

5. In the Virus Protection section, select Scheduled Scan. Deselect the Enable scheduled scanning option.
6. Click **OK** to close the *Advanced Options* window.

7. Close the *McAfee Security Center* window.

### 3.4. Disabling Windows Warning Messages

To disable an unnecessary Windows message:

1. Open the *Windows Security Center* window by selecting **Start>Control Panel>Security Center**.

2. In the Resources section of the *Windows Security Center* window, click **Change the way Security Center alerts me**, as shown in Figure 3-4.

3. In the **Alert Settings** window, deselect the **Firewall, Automatic Updates**, and **Virus Protection** options, as shown in Figure 3-5.

4. Click **OK** to accept changes and close the **Alert Settings** window.
5. Close the *Windows Security Center* and *Control Panel* windows.

### 3.5. Disabling Microsoft Update

After installing Microsoft Security Essentials, Microsoft Update is enabled by default. Microsoft Update must be disabled on 8100 systems.

#### 3.5.1. *Windows XP and Windows Server 2003*

If you are running Windows XP or Windows Server 2003, perform the following steps for both the Controller PC and/or the Client Laptop.


2. Under the *Automatic Updates* tab, select the **Turn off Automatic Updates** option, as shown in Figure 3-6.
3. Click **OK** to save the changes and exit the window.

### 3.5.2. **Windows 7**

If you are running Windows 7, perform the following steps for both the Controller PC and/or the Client Laptop.


2. Under the *Important Updates* section, select **Never check for updates**, as shown in Figure 3-7.
3. Click **OK** to save the changes and exit the window.

4. If a "Windows update is turned off. Click to turn on." message displays on the desktop, ignore it.

### 3.5.3. **Windows Server 2008**

If you are running Windows Server 2008 on the Application Server, perform the following steps.

1. Select **Start>Control Panel>System and Maintenance>Windows Update>Change Settings**.
   
The *Change Settings* window displays.

2. Under the *Important Updates* section, select **Never check for updates**, as shown in Figure 3-8.
3. Click **OK** to save the changes and exit the window.

4. If a “Windows update is turned off. Click to turn on.” message displays on the desktop, ignore it.
4. Dell Latitude E6500 Client Laptop Issue

**NOTE:** If you have any other Client Laptop model, you can skip this chapter.

There is an issue with removing the test data cards and test phones from Dell Latitude E6500 Client Laptops connected via the PCMCIA slot or USB. The issue prevents the device from being used (after removed) until the client laptop is rebooted.

Follow the instructions below to avoid having to reboot the Client Laptop after removing a test device.

1. Before removing a device plugged into the PCMCIA slot or connected via the USB port, stop the device properly by selecting the *Safely Remove Hardware* icon from the System Tray, as shown in Figure 4-1.

2. Select the desired test device to safely remove it from the Client Laptop.
5. UE Drivers that Install a Network Interface

There is a potential conflict during data call setup, when both the Network Interface and Dial-Up Modem are enabled on the client laptop.

To avoid this conflict, we recommend that you disable the Network Interface if the TestDrive Data Connection (Dial-Up Modem) is the targeted interface for the session, as shown in the Figures below. If the Network Interface is not disabled, data call setups could fail with a RasDial exception.

![Figure 5-1: Network Connections Window – Disabling the Network Interface](image1)

![Figure 5-2: Network Connections Window – Successfully Disabled Network Interface](image2)
6. Upgrading the NIC Driver in SR3920 Application Server

NOTE: This procedure solves Data Throughput Performance issues observed with old versions of the Broadcom NIC Driver. This procedure is applicable only to Dell Server versions 1950 and R610. The recommended process to upgrade the driver is to use a keyboard/monitor/mouse connected to the server.

6.1. Upgrading the NIC Driver

1. Check the current NIC driver version by right-clicking on any of the network adapters and selecting Properties. Under the Driver tab, make sure the version is older than 6.x.x.x, as shown in Figure 6-1.

NOTE: Do not click the Uninstall button in this window.

2. Select Control Panel>Programs and Features.
3. From the Programs and Features window, uninstall Broadcom Drivers and Management Applications, as shown in Figure 6-2.

![Figure 6-2: Programs and Features Window](image)

4. From the downloaded Radio Access Package, open the "Broadcom NIC Drivers" folder and run setup.exe to install the new driver.

5. After the installation is complete, reboot the PC.

6. Check the current NIC driver version by right-clicking on any of the network adapters and selecting Properties. Under the Driver tab, make sure the version is 6.2.9.0.

7. Close all windows.

### 6.2. Verifying IP Configuration

**NOTE:** Upgrading NIC driver erases all IP configurations on the interface. The following procedure restores the configurations.

2. Under Tasks, select Manage Network Connections.
3. Insert an Ethernet cable from a router to the GB2 port on the rear of the server.
4. From the Network Connections window, observe which Local Connection is connected (the one without a red “X”), as shown in Figure 6-3.
5. Select the connected interface. Right-click and select Rename from the menu.
6. Rename the connection to “Local Area Connection UMTS-LTE”.
7. Right-click Local Area Connection UMTS-LTE and select Properties from the menu.
8. From the Properties window, select Internet Protocol 4 (TCP/IPV4) and click Properties.
9. From the Internet Protocol 4 (TCP/IPV4) Properties window, enter the following information as shown in Figure 6-4:
   a. IP Address: 192.168.0.70
   b. Subnet Mask: 255.255.255.0
   c. Default Gateway: 192.168.0.1
10. A Warning Message may display, as shown in Figure 6-5. Click Yes to proceed.
11. In the Internet Protocol 4 (TCP/IPV4) Properties window, select the Advanced tab.

12. Under the Wins tab, ensure that the “Disable NetBIOS over TCP/IP” option is selected, as shown in Figure 6-6.

13. Click OK and close the Internet Protocol Version 4 window.

14. From the Local Area Connection UMTS-LTE Properties window, select Internet Protocol 6 (TCP/IPV6) and click Properties.

15. On the Internet Protocol 6 (TCP/IPV6) Properties window, select the Use the following ipv6 address option and enter \textbf{fd00:0:20:1:0:0:0:4} for the IP Address. Enter 64 for the Subnet prefix length, as shown in Figure 6-7.
16. Click **OK** and close the Internet Protocol Version 6 window.

17. Close the Local Area Connection window.

18. Move the Ethernet cable from the GB2 Server to the GB1 Interface.

19. From the Network Connections window, observe which Local Connection is connected (the one without a red “X”).
20. Repeat steps 5 through 13 with the following changes:
   Note that the CDMA Interface does not require you to enter an IPv6 address.
   a. **Step 6:**
      Connection Name: **Local Area Connection CDMA**
   b. **Step 9:**
      IP Address = **192.168.0.125**
      Subnet = **255.255.255.0**
      Gateway = **192.168.0.1**

21. When setting the Default Gateway for the CDMA connection, an *Error Message*
    displays, as shown in Figure 6-9. 
    Click **Yes** to continue.

![Figure 6-9: Default Gateway Warning Message](image-url)