Test Plan

Plan Name: LTEOTADM Test Plan

Plan Id: LTEFIELDOA

Version Number: 3.5

Release Date: October 2024

Latest Release Date: October 2024 : Open Access

01.01 VERIFY LTE CONNMO DM TREES VZ_TC_LTEFIELDOA_8540

Test and verify that that the authentication algorithm implemented in the device is correct.

Design Steps
Step Name
1. Verify LTE ConnMO DM Tree
Pre-Conditions
1. Ensure the device is powered on and has sufficient battery power to establish and maintain a data call. 2. Ensure the device is connected to the LTE live network (can be verified by the "4G" network indicator displayed on device UI or connection manager),
Procedures
1. Using OTADM Server GUI, select the DUT. 2. Send a Get command to retrieve the LTE ConnMO DM tree. 3. Wait for the data to be retrieved from the DUT. 4. Verify the ConnMO tree nodes returned values. 5. Close the results window.
Expected Results
The device shall successfully complete the transactions without an error message, and return the values as specified in Table A-1 below.

Connectivity Node	Description	Value	Commands
./ManagedObjects/ConnMO/LTE	Internal Node	node	Get
./ManagedObjects/ConnMO/LTE/APN/*	Internal Node	node	Get
./ManagedObjects/ConnMO/LTE/APN/*/Setting	Internal Node	node	Get
./ManagedObjects/ConnMO/LTE/APN/*/Setting /Id	APN Id	1	Get
./ManagedObjects/ConnMO/LTE/APN/*/Setting /Name	APN Name	IMS	Get, Replace
./ManagedObjects/ConnMO/LTE/APN/*/Setting /IP	IP Version. Defined by	IPv4 or IPv4 and IPv6	Get, Replace

	Standards but not used by Verizon Wireless		
./ManagedObjects/ConnMO/LTE/APN/*/Setting /Enabled	Returns if the APN is enabled (True) or not (False)	True	Get
./ManagedObjects/ConnMO/LTE/APN/*/Setting/Operations	Internal Node	node	Get
./ManagedObjects/ConnMO/LTE/APN/*/Setting /Id	APN Id	2	Get
./ManagedObjects/ConnMO/LTE/APN/*/Setting /Name	APN Name	VZWADMIN	Get, Replace
./ManagedObjects/ConnMO/LTE/APN/*/Setting /IP	IP Version. Defined by Standards but not used by Verizon Wireless	IPv4 or IPv4 and IPv6	Get, Replace
./ManagedObjects/ConnMO/LTE/APN/*/Setting /Enabled	Returns if the APN is enabled (True) or not (False)	True	Get
./ManagedObjects/ConnMO/LTE/APN/*/Setting /Id	APN Id	3	Get
./ManagedObjects/ConnMO/LTE/APN/*/Setting /Name	APN Name	VZWINTERNET or V5GA01INTERNET for FWA	Get, Replace
./ManagedObjects/ConnMO/LTE/APN/*/Setting /IP	IP Version. Defined by Standards but not used by	IPv4 or IPv4 and IPv6	Get, Replace

	Verizon Wireless		
./ManagedObjects/ConnMO/LTE/APN/*/Setting /Enabled	Returns if the APN is enabled (True) or not (False)	True	Get
./ManagedObjects/ConnMO/LTE/APN/*/Setting/Operations/Enable	Enable APN	Null	Exec
./ManagedObjects/ConnMO/LTE/APN/*/Setting/Operations/Disable	Disable APN	Null	Exec
./ManagedObjects/ConnMO/LTE/APN/*/Setting /Id	APN Id	4	Get
./ManagedObjects/ConnMO/LTE/APN/*/Setting /Name	APN Name	VZWAPP	Get, Replace
./ManagedObjects/ConnMO/LTE/APN/*/Setting /IP	IP Version. Defined by Standards but not used by Verizon Wireless	IPv4 or IPv4 and IPv6	Get, Replace
./ManagedObjects/ConnMO/LTE/APN/*/Setting /Enabled	Returns if the APN is enabled (True) or not (False)	True	Get
./ManagedObjects/ConnMO/LTE/APN/*/Setting/Operations/Enable	Enable APN	Null	Exec
./ManagedObjects/ConnMO/LTE/APN/*/Setting/Operations/Disable	Disable APN	Null	Exec
./ManagedObjects/ConnMO/IMS	Interior Node	Node	Get
./ManagedObjects/ConnMO/IMS/Setting	Interior Node	Node	Get
./ManagedObjects/ConnMO/IMS/Setting/Domain	Home Domain Name for the	vzims.com	Get

	device to populate the request URI for REGISTRATION		
./ManagedObjects/ConnMO/IMS/Setting/smsformat	Device Outgoing SMS based on either 3GPP or 3GPP2 standards	3GPP or 3GPP2	Get, Replace
./ManagedObjects/ConnMO/IMS/Setting/sms_over_IP_network_indication	Turns IMS ON/OFF on the device	True (404 is an acceptable result for CDMAless devices)	Get,replace

Table A-1 LTE ConnMO DM Trees

Execute operations enable/disable APN1 and 2 should result in a 404
GET operations on APN1 and 2 for the internal node
./ManagedObjects/ConnMO/LTE/APN/*/Setting/Operations should result in a 404

Design Steps
Step Name
2. APN 1 and 2 Management
Pre-Conditions
Procedures
Perform a GET operation on ./ManagedObjects/ConnMO/LTE/APN/1/Setting/Operations and

./ManagedObjects/ConnMO/LTE/APN/2/Setting/Operations

Expected Results
Verify the device returns a 404 to the server to indicate the APN 1 and 2 operations nodes are not supported.

Design Steps
Step Name
3. APN 1 and 2 Enable/Disable

Pre-Conditions
APN 1 and 2 are enabled on the device

Procedures
Perform an EXEC operation on the node ./ManagedObjects/ConnMO/LTE/APN/1/Setting/Operations/Disable and   ./ManagedObjects/ConnMO/LTE/APN/2/Setting/Operations/Disable

Expected Results
Verify the device responds back to the server with a 404 to indicate the commands were not successful.

Design Steps
Step Name

4. Confirm APN 1 and 2 remain enabled

Pre-Conditions

Procedures

Perform a GET operation on the nodes:

./ManagedObjects/ConnMO/LTE/APN/1/Setting/Enabled

and

./ManagedObjects/ConnMO/LTE/APN/2/Setting/Enabled

Expected Results

Verify the DUT responds to the GET operations with a "True" for each node.

01.02 APN MANAGEMENT TRIGGERED BY MOBILE AUTOMATIC DEVICE DETECTION (ADD) VZ_TC_LTEFIELDOA_8549

Test and verify APN management triggered by mobile activate is successful.

This test case is not applicable for devices where the SIM cannot be removed.

Design Steps
Step Name
Pre-Conditions (APN Management Triggered by Mobile Automatic Device Detection (ADD) - LTE)
Pre-Conditions
1. Two Devices and 1 UICC are required for this test case. 2. Device 1 = DUT, shall have default values for all APNs 3. Device 2 shall have its Class 3 APN Name set to "vzwtest2" (without quotes). 4. Device 1 with UICC is powered on and registered with live LTE network 5. Access to a non-commercial (test) OTADM Server is available 6. OEM instruction of changing device bootstrap is available
Procedures
1. Follow OEM instructions to program the DUT bootstrap to the OTADM Test Server 2. Use the Test OTADM Server GUI, and retrieve the complete ConnMO tree; Get the vendor defined "*" values for all LTE APNs, and identify the * value for VZWINTERNET APN 3. From the OTADM Server, send a Get command to retrieve the LTE ConnMO DM tree. Wait for values to be returned 4. On the OTADM Server, send a Replace command to replace the "VZWINTERNET" APN3 name on the DUT with invalid name such as "vzwtest" in lower cases. 5. Disable APN4 and APN5 if supported. 6. After the DM Session ends, make an attempt to browse internet 7. Following OEMs instruction to program the second device bootstrap to the Production OTADM Server URL (if required) 8. Power down the DUT, and take out the UICC card from the DUT, and insert it in to the second LTE device, and power up the second LTE device

9. Observe the second device UI for data call indication (skip if the device does not support any UI)
10. Verify the device is attached to LTE network (by observing the 4G icon or equivalent display on the device, or from data logging)
11. Check DUT to confirm Class 3 APN Name changed to VZWINTERNET. Change may take up to 5 minutes
12. Browse the internet on the device

Expected Results
Step 2: The complete ConnMO DM Tree is retrieved. The "*" values for all APNs are obtained, the "*" value for VZWINTERNET APN nodes is identified
Step 3: Verify DUT returns APN parameters for IMS APN, VZWADMIN APN, VZWINTERNET APN, and VZWAPP APN
Step 4 : The replacement operation is successful without error
Step 5: The internet browsing attempt failed
Step 7: DUT displays active data call icon for a few seconds, then return to idle state
Step 10: Second device is attached to LTE network, and Class 3 APN Name changed to VZWINTERNET
Step 11: Internet browsing is successful: note: the internet browsing must be successful without any manual intervention or work around, if internet browsing does not work automatically, this step is a fail

01.05 OTADM-013-IPv6 Successful Connectivity Testing VZ_TC_LTEFIELDOA_8552

Verify if the device is able to connect to the OTADM server over an IPv6 connection.

Design Steps
Step Name
Step 1
Pre-Conditions
1. Program the IPv6 server URL in the DMAcc node to reach the DM server supporting IPv6 connectivity. URL information will be provided by the Verizon Wireless Authorized OTADM IOT server vendor listed in LTE 3GPP Band 13 Device Conformance Test Process document.   2. Ensure the device is powered on and has sufficient battery power to establish and maintain a data call.   3. Ensure the device is connected to the LTE live network (can be verified by the "4G" network indicator displayed on device UI or connection manager).
Procedures
Step1: Start logging on the Device and/or the DM server to see PCAP trace of device connectivity with the DM Server   Step2: On the DM server, select the Device is question and send Pkg0 to initiate DM Connectivity from the DUT   Step3: Perform a Get Command on LTE ConnMO DM Tree   Step4: Wait for the data to be retrieved   Step5: Verify the ConnMO Tree nodes returned by the device   Step6: Close the results window.
Expected Results
Step2: Device successfully opens a DM Connection over IPv6 (check PCAP logs for the device connection attempt)   Step5: The device sends the following tree (some values depend on what technologies the device supports):

Connectivity Node	*Value*
./ManagedObjects/ConnMO/LTE	node

./ManagedObjects/ConnMO/LTE/APN/*	node
./ManagedObjects/ConnMO/LTE/APN/*/Setting	node
./ManagedObjects/ConnMO/LTE/APN/*/Setting /Id	1
./ManagedObjects/ConnMO/LTE/APN/*/Setting /Name	IMS
./ManagedObjects/ConnMO/LTE/APN/*/Setting /IP	IPv6
./ManagedObjects/ConnMO/LTE/APN/*/Setting /Enabled	True
./ManagedObjects/ConnMO/LTE/APN/*/Setting/Operations	node
./ManagedObjects/ConnMO/LTE/APN/*/Setting /Id	2
./ManagedObjects/ConnMO/LTE/APN/*/Setting /Name	VZWADMIN
./ManagedObjects/ConnMO/LTE/APN/*/Setting /IP	IPv4 and IPv6
./ManagedObjects/ConnMO/LTE/APN/*/Setting /Enabled	True
./ManagedObjects/ConnMO/LTE/APN/*/Setting /Id	3
./ManagedObjects/ConnMO/LTE/APN/*/Setting /Name	VZWINTERNET
./ManagedObjects/ConnMO/LTE/APN/*/Setting /IP	IPv4 and IPv6
./ManagedObjects/ConnMO/LTE/APN/*/Setting /Enabled	True
./ManagedObjects/ConnMO/LTE/APN/*/Setting /Id	4
./ManagedObjects/ConnMO/LTE/APN/*/Setting /Name	VZWAPP
./ManagedObjects/ConnMO/LTE/APN/*/Setting /IP	IPv4 and IPv6
./ManagedObjects/ConnMO/LTE/APN/*/Setting /Enabled	True
./ManagedObjects/ConnMO/IMS	Node
./ManagedObjects/ConnMO/IMS/Setting	Node
./ManagedObjects/ConnMO/IMS/Setting/Domain	vzims.com
./ManagedObjects/ConnMO/IMS/Setting/smsformat	3GPP or 3GPP2
./ManagedObjects/ConnMO/IMS/Setting/sms_over_IP_network_indication	True

01.06 OTADM-014-IPv4 Successful Connectivity Testing VZ_TC_LTEFIELDOA_8553

Verify that device successfully falls back to IPv4 connection when IPv6 connectivity is not possible.

Design Steps
Step Name
Step 1
Pre-Conditions
1. Program the IPv4 server URL in the DMAcc node to reach the DM server supporting IPv4 connectivity. URL information will be provided by the Verizon Wireless Authorized OTADM IOT server vendor listed in LTE 3GPP Band 13 Device Conformance Test Process document. 2. Ensure the device is connected to the LTE live network (can be verified by the "4G" network indicator displayed on device UI or connection manager).
Procedures
Step1: Start logging on the Device and/or the DM server to see PCAP trace of device connectivity with the DM Server Step2: On the DM server, select the Device is question and send Pkg0 to initiate DM Connectivity from the DUT Step3: Perform a Get Command on LTE ConnMO DM Tree Step4: Wait for the data to be retrieved Step5: Verify the ConnMO Tree nodes returned by the device Step6: Close the results window.
Expected Results
Step2: Device receives IPv4 address of the DM Server from the DNS server and successfully opens a DM session with the DM server. Step5: The device sends the following tree (some values depend on what technologies the device supports):

Connectivity Node	Value
./ManagedObjects/ConnMO/LTE	node
./ManagedObjects/ConnMO/LTE/APN/*	node
./ManagedObjects/ConnMO/LTE/APN/*/Setting	node

./ManagedObjects/ConnMO/LTE/APN/*/Setting /Id	1
./ManagedObjects/ConnMO/LTE/APN/*/Setting /Name	IMS
./ManagedObjects/ConnMO/LTE/APN/*/Setting /IP	IPv6
./ManagedObjects/ConnMO/LTE/APN/*/Setting /Enabled	True
./ManagedObjects/ConnMO/LTE/APN/*/Setting/Operations	node
./ManagedObjects/ConnMO/LTE/APN/*/Setting /Id	2
./ManagedObjects/ConnMO/LTE/APN/*/Setting /Name	VZWADMIN
./ManagedObjects/ConnMO/LTE/APN/*/Setting /IP	IPv4 and IPv6
./ManagedObjects/ConnMO/LTE/APN/*/Setting /Enabled	True
./ManagedObjects/ConnMO/LTE/APN/*/Setting /Id	3
./ManagedObjects/ConnMO/LTE/APN/*/Setting /Name	VZWINTERNET
./ManagedObjects/ConnMO/LTE/APN/*/Setting /IP	IPv4 and IPv6
./ManagedObjects/ConnMO/LTE/APN/*/Setting /Enabled	True
./ManagedObjects/ConnMO/LTE/APN/*/Setting /Id	4
./ManagedObjects/ConnMO/LTE/APN/*/Setting /Name	VZWAPP
./ManagedObjects/ConnMO/LTE/APN/*/Setting /IP	IPv4 and IPv6
./ManagedObjects/ConnMO/LTE/APN/*/Setting /Enabled	True
./ManagedObjects/ConnMO/IMS	Node
./ManagedObjects/ConnMO/IMS/Setting	Node
./ManagedObjects/ConnMO/IMS/Setting/Domain	vzims.com
./ManagedObjects/ConnMO/IMS/Setting/smsformat	3GPP or 3GPP2
./ManagedObjects/ConnMO/IMS/Setting/sms_over_IP_network_indication	True

01.07 DEVINFO EXTENSION NODE TEST <mark>VZ_TC_LTEFIELDOA_8554</mark>

These test case is to confirm 1 additional Extension node is returned on top of all the other DevInfo nodes.

This test case is not applicable for devices where the SIM cannot be removed.

Design Steps
Step Name
Step 1
Pre-Conditions
These Test Cases apply to all DM Sessions, Network Initiated, User Initiated, and Client Initiated It is assumed that the DUT will return all the supported DevInfo node values as per the LTE-OTADM requirements document. These test cases are to confirm 1 additional Extension node is returned on top of all the other DevInfo nodes. For this test case, 2 valid UICCs are required The valid UICCs will be referred to as First UICC and Second UICC in the Test Cases below
Procedures
Insert the First UICC in the DUT. Power on DUT Perform a DM Session Confirm ./DevInfo/Ext/ICCID Extension node is sent in Pkg1 to the DM Server
Expected Results
DUT returns all the DevInfo Nodes as discussed in Reqs-OTADM Requirements, LTE-OTADM Requirements, and the following node: DM Server logs show ./DevInfo/Ext/ICCID with ICCID value of the First UICC received in Pkg1
Design Steps
Step Name
Step 2
Pre-Conditions

Device need Wi-Fi connection
Procedures
Remove the First UICC while DUT is powered on and connect to Wi-Fi

Perform a DM Session by checking for updates on the device.

Confirm ./DevInfo/Ext/ICCID Extension node is sent in Pkg1 to the DM Server |
| **Expected Results** |
| DUT returns all the DevInfo Nodes as discussed in Reqs-OTADM Requirements, LTE-OTADM Requirements, and the following node:

DM Server logs show ./DevInfo/Ext/ICCID with a NULL value received in Pkg1 |
| **Design Steps** |
| **Step Name** |
| Step 3 |
| **Pre-Conditions** |
| **Procedures** |
| Insert the Second UICC in the DUT while the DUT is powered on

Perform a DM Session.

Confirm ./DevInfo/Ext/ICCID Extension node is sent in Pkg1 to the DM Server |
| **Expected Results** |
| DUT returns all the DevInfo Nodes as discussed in Reqs-OTADM Requirements, LTE-OTADM Requirements, and the following node:

DM Server logs show ./DevInfo/Ext/ICCID with ICCID value of the Second UICC received in Pkg1 |
| **Design Steps** |
| **Step Name** |
| Step 4 |

Pre-Conditions

Procedures
Remove the Second UICC and insert the First UICC in the DUT while the DUT is powered on Perform a DM Session. Confirm ./DevInfo/Ext/ICCID Extension node is sent in Pkg1 to the DM Server

Expected Results
DUT returns all the DevInfo Nodes as discussed in Reqs-OTADM Requirements, LTE-OTADM Requirements, and the following node: DM Server logs show ./DevInfo/Ext/ICCID with ICCID value of the First UICC received in Pkg1

Design Steps

Step Name
Step 5

Pre-Conditions

Procedures
Power down the DUT Remove the First UICC from the DUT Power up the DUT and connect to a Wi-Fi network Perform a DM Session by checking for updates on the device. Confirm ./DevInfo/Ext/ICCID Extension node is sent in Pkg1 to the DM Server

Expected Results
DUT returns all the DevInfo Nodes as discussed in Reqs-OTADM Requirements, LTE-OTADM Requirements, and the following node: DM Server logs show ./DevInfo/Ext/ICCID with a NULL value received in Pkg1

Design Steps

Step Name

Step 6

Pre-Conditions

Procedures

Power down the DUT
Insert the First UICC in the DUT

Perform a DM Session

Confirm ./DevInfo/Ext/ICCID Extension node is sent in Pkg1 to the DM Server

Expected Results

DUT returns all the DevInfo Nodes as discussed in Reqs-OTADM Requirements, LTE-OTADM Requirements, and the following node:

DM Server logs show ./DevInfo/Ext/ICCID with ICCID value of the First UICC received in Pkg1

Design Steps

Step Name

Step 7

Pre-Conditions

Procedures

Power cycle the DUT

Perform a DM Session

Confirm ./DevInfo/Ext/ICCID Extension node is sent in Pkg1 to the DM Server

Expected Results

DUT returns all the DevInfo Nodes as discussed in Reqs-OTADM Requirements, LTE-OTADM Requirements, and the following node:

DM Server logs show ./DevInfo/Ext/ICCID with ICCID value of the First UICC received in Pkg1

01.08 APN Management by OTADM server VZ_TC_LTEFIELDOA_8555

This test case verifies a multiple Class 3 APN name changes by the OTADM server

Design Steps
Step Name
Step 1
Pre-Conditions
Need VZW active SIM card, Device under test with a sufficient battery level
Procedures
1) Confirm connectivity to the network with the existing device 2) Perform OTADM Session to change Class3 APN value to VZWTEST1 3) Check connectivity with the network. Confirm APN name being sent = VZWTEST1 4) Confirm Network denies access 5) Perform another OTADM session to change Class3 APN to VZWINTERNET 6) Confirm connectivity with the network 7) Disconnection from network
Expected Results
1. Device has connectivity to the network 2. Device perform OTADM session with DM server 3. Device changes Class3 APN value to VZWTEST1 4. Network denies the device access to the internet 5. Device perform OTADM session with DM server 6. Device changes Class3 APN value to VZWINTERNET 7. Device successfully connects to the network 8. Device successfully disconnects from the network

01.09 AUTHENTICATION SECURITY KEY MIS-MATCH VZ_TC_LTEFIELDOA_8541

Test and verify that that the authentication algorithm implemented in the device is correct.

Design Steps
Step Name
Authentication Security Key Mismatch
Pre-Conditions
1. Ensure the device is powered on and has sufficient battery power to establish and maintain a data call. 2. Obtain instructions from the Device Vendor for changing the Password on the device 3. Ensure the device is connected to the LTE live network (can be verified by the "4G" network indicator displayed on device UI or connection manager), 4. The OTADM Server contains the OTADM Authentication key.
Procedures
1. Login to DM server, and add your device to the OTADM Server, 2. On the Device, change the server password 3. Send a Get Command to retrieve APN Node (see Section 6.1)
Expected Results
Step 3: Attempt to retrieve the APN nodes failed Device does return the APN parameters. OTADM Server request states failed.

01.10 AUTHENTICATION SECURITY KEY MATCH VZ_TC_LTEFIELDOA_8542

Test and verify that that the authentication algorithm implemented in the device is correct.

Design Steps
Step Name
Authentication Security Key Match
Pre-Conditions
1. Ensure the device is powered on and has sufficient battery power to establish and maintain a data call. 2. Ensure the device is connected to the LTE live network (can be verified by the "4G" network indicator displayed on device UI or connection manager).
Procedures
1. Login into and add your device to the OTADM Server, 2. Apply the Correct MD5 password for the device password, 3. Save the device, 4. Send a Get command to retrieve the APN nodes from the OTADM Server (Refer to 6.1 test steps for details), 5. Verify the command execution is successful.
Expected Results
The device shall successfully complete the transaction (no error messages) OTADM Server request states Operation is completed successfully.

01.13 CONNMO TREE INTERNET APN VERIFICATION AND OPERATION VZ_TC_LTEFIELDOA_8545

Test and verify that all device requirements necessary to capture and modify selected LTE connectivity parameters have been met.

Design Steps
Step Name
ConnMO Tree - INTERNET APN Verification and Operation
Pre-Conditions
1. Ensure the device is powered on and has sufficient battery power to establish and maintain a data call. 2. Ensure the device is connected to the LTE live network (can be verified by the "4G" network indicator displayed on device UI or connection manager).
Procedures
1. Verify the DUT can browse internet by going to a public internet website such as www.yahoo.com, 2. Using the OTADM Server, select the DUT, 3. From the OTADM Server, send a Get command to retrieve Internet APN nodes, 4. Wait till the device returns all the APN values to the server, 5. Verify the Internet APN values, 6. From the OTADM Server, send an Exec command to disable the Internet APN, 7. Wait till the ATM transaction completes, 8. Verify the device now cannot browse internet by attempt to launch a public website such as www.yahoo.com, 9. Repeat Steps 2-4 to retrieve the Internet APN settings again, 10. Verify the current "Enabled" property is set to "false", 11. From the OTADM Server, send an Exec command to enable the Internet APN, 12. Wait till the APN transaction completes, 13. Verify the device can now browse internet by launch a public website such as www.yahoo.com.
Expected Results
Step 1: The device can browse public internet successfully, Step 5: the DUT returns the following values for Internet APN: • APN Id: 3

- APN Name: VZWINTERNET
- APN IP: "IPv4" or "IPv4 and IPv6"
- APN is Enabled,

Step 8: The device cannot browse public internet,

Step 10: The current internet APN is set to disabled,

Step 13: Device successfully launches public internet website.

01.14 CONNMO TREE APP APN VERIFICATION AND OPERATION
VZ_TC_LTEFIELDOA_8546

Test and verify that all device requirements necessary to capture and modify selected LTE connectivity parameters have been met.

Design Steps

Step Name

ConnMO Tree - APP APN Verification and Operation

Pre-Conditions

1. Ensure the device is powered on and has sufficient battery power to establish and maintain a data call.
2. Ensure the device is connected to the LTE live network (can be verified by the "4G" network indicator displayed on device UI or connection manager).

Procedures

1. Verify the DUT can launch a VZW brand application on the device, such as Verizon messages
2. Using the OTADM Server, select the DUT,
3. From the OTADM Server, send a Get command to retrieve the VZWAPP APN nodes,
4. Wait till the device returns all the APN values to the server,
5. Verify the APP APN values,
6. From the OTADM Server, send an Exec command to disable the VZWAPP APN,
7. Wait till the APN transaction completes,
8. Attempt to bring up the same VZW brand application as in Step 1,
9. Repeat Steps 2-4 to retrieve the APP APN settings again,
10. Verify the current "Enabled" property is set to "false",
11. From the OTADM Server, send an Exec command to enable the VZWAPP APN,
12. Wait till the APN transaction completes,
13. Verify the device can now launch the same VZW brand application as in Step 1.

Expected Results

Step 1: The device can bring up a VZW brand application successfully,
Step 5: the DUT returns the following values for APP APN:

- APN Id: 4
- APN Name: VZWAPP
- APN IP: "IPv4" or "IPv4 and IPv6"
- APN is Enabled,

Step 8: The attempt to bring up the same VZW brand application fails,
Step 10: the current APP APN is set to disabled,
Step 13: Device successfully launches the VZW brand application.

01.15 CONNMO TREE SMS OVER IMS VERIFICATION AND OPERATION
VZ_TC_LTEFIELDOA_8547

Test and verify that all device requirements necessary to capture and modify selected LTE
connectivity parameters have been met.
This test case is not applicable to CDMAless devices.

Design Steps
Step Name
ConnMO Tree - SMS over IMS Verification and Operation
Pre-Conditions
1. Ensure the device is powered on and has sufficient battery power to establish and maintain a data call. 2. Ensure the device is connected to the LTE live network (can be verified by the "4G" network indicator displayed on device UI or connection manager). 3. Device network mode is set to "LTE only", 4. Another device that is SMS capable is available. 5. Instructions on accessing the Device SMS log are available
Procedures
1. Verify the DUT can successfully send (MO)_ an SMS message by sending an SMS to the other device, and the other device replying the SMS back, 2. From the OTADM Server, send a Get command to retrieve the ConnMO/IMS nodes, 3. Verify the IMS settings, when device responds 4. From the OTADM Server, send a Replace command to change the "sms_over_IP_network_indication" node value from "True" to "False", 5. Wait until the ConnMO transaction completes, 6. Attempt to send SMS message on the DUT, 7. Make a voice call on the device (if supported by the device) and browse on the Internet to verify that functionality is still working. 8. , From the OTADM Server, send a Replace command to change the "sms_over_IP_network_indication" node value from "False" to "True", 9. Verify the SMS over IMS value is stored as "True" 10. Repeat Steps 2 5 to verify the SMS over IMS value is restored to "True", 11. Send SMS from the DUT.

Expected Results

Step 1: The device can send SMS successfully,

Step 3: the DUT returns the following values for IMS:

Domain: registrar.vzw.net

smsformat: 3GPP or 3GPP2

sms_over_IP_network_indication: True

Step 6: Check Device Log: Device does not send SMS over IMS

Step 7: The device is able to make a voice call (if supported by the device) and is able to browse the Internet.

Step 9: SMS IP Setting is set to "True"

Step 11: The device can send (MO)SMS successfully.

01.16 APN NAMES CASE INSENSITIVE TEST VZ_TC_LTEFIELDOA_8548

Test and verify device treat APN names case insensitive.

Design Steps
Step Name
APN Names Case Insensitive Test
Pre-Conditions
1. Ensure the device is powered on and has sufficient battery power to establish and maintain a data call,   2. Ensure the device is connected to the LTE live network (can be verified by the "4G" network indicator displayed on device UI or connection manager, or verify from data logging),   3. Launch browser and verify device has Internet PDN connection,   4. Device has default values for all APNs.
Procedures

1. Verify all 4 classes of APNs work by:
     1. IMS: verify the device is registered with LTE live network,
     2. ADMIN: will be verified in Step 2 below
     3. INTERNET: verified on #3 of previous section
     4. VZWAPP: verify the APN works properly by launching a VZW branded application, such as MyVerizon -> Data Usage.
 2. On the OTADM Server, select the DUT,
 3. From the OTADM Server, send the Replace commands to replace the APN names with opposite cases, for example, if the default APN names are capital letters, replace the APN names with lower cases, for APN3 and APN4 names,
 4. Verify the device registers with LTE live network as expected by verifying the associated service icon/indicator,
 5. Verify the devices APP APN by bringing up a VZW brand application, such as "My Verizon -> Data Usage",
 6. Verify the devices internet APN by making an attempt to browse internet,
 7. Repeat steps 4 - 7 to ensure all APNs are still functional as expected;
 8. Repeat Steps 2 - 3 to replace the APN names with mixed case letters, for example, replace the APN names with vZWinteRNEt, and VzwaPp, for the AN3 and APN4 names,
 9. Repeat steps 4 - 7 to verify all APN functions are maintained,
 10. Repeat steps 2 - 3 to restore the LTE APN names to default cases,

11. Repeat steps 4 7 to verify all APN functions are maintained.

Expected Results
Step 4: Device registers with LTE live network by displaying a "4G" icon on the handset UI, if the device is a data card, it displays the associated 4G icon on its connection manager, or display an indicator on the device, or indicated from data logging,   Step 5: MyVerizon -> data usage is brought up successfully,   Step 6: The internet connection is successful,   Step 7: The OTADM Server request is successful,   Step 7, 9, and 11: same expected results as steps 3 6.

01.17 TLS Protocol for DM sessions VZ_TC_LTEFIELDOA_8842

Test and verify that device uses TLS protocols and not SSL

Design Steps
Step Name
Step 1
Pre-Conditions
1. Ensure the device is powered on and has sufficient battery power to establish and maintain a data call. 2. Ensure the device is connected to the VZW cellular network (can be verified by the "4G" network indicator displayed on device UI or connection manager). 3. Run any tool like wireshark to capture network traffic from the DUT
Procedures
Send Pkg0 WAP Push from DM server to DUT Perform Get operation on ./ManagedObjects/ConnMO/LTE/APN/1/Setting/Name
Expected Results
DUT returns IMS Review the logs from the DUT to confirm that DUT uses TLS protocols and not the SSL

01.19 APN Settings Persistence through Factory Reset and Power Cycle
VZ_TC_LTEFIELDOA_1347842

Design Steps
Step Name
Factory Reset
Pre-Conditions
Procedures

1. Verify the DUT can browse internet by going to a public internet website such as www.yahoo.com,
2. Using the OTADM Server, select the DUT,
3. From the OTADM Server, send a Get command to retrieve all the APN nodes,
4. Wait till the device to return all the APN values to the server,
5. Verify the APN values,
6. From the OTADM Server, send an Exec command to disable the Internet APN,
7. Wait till the ATM transaction completes,
8. Verify the device now cannot browse internet by attempt to launch a public website such as www.yahoo.com,
9. Go in to DUT settings and perform a Full Factory Reset
10. Repeat Steps 2-4 to retrieve the APN settings again,
11. Verify the current "Enabled" property is set to "false",
12. From the OTADM Server, send an Exec command to enable the Internet APN,
13. Wait till the APN transaction completes,
14. Verify the device can now browse internet by launching a public website such as www.yahoo.com.
15. Using the OTADM Server, select the DUT,
16. Perform the Replace operations from the DM Server on the DUT ./ManagedObjects/ConnMO/LTE/APN/3/Setting/Name FOTATestFactoryReset
17. Wait till the ATM transaction completes,
18. Verify the device now cannot browse internet by attempt to launch a public website such as www.yahoo.com,
19. Go in to DUT settings and perform a Full Factory Reset
20. Perform the GET operations from the DM Server on the DUT for all APN values

21. Perform the Replace operations from the DM Server on the DUT
   ./ManagedObjects/ConnMO/LTE/APN/3/Setting/Name VZWINTERNET
22. Wait till the APN transaction completes,
23. Verify the device can now browse internet by launch a public website such as
   www.yahoo.com.

Expected Results

Step1: The device can browse public internet successfully,

Step 3: the DUT returns the following values for APN:

- APN Id: 1
- APN Name: IMS
- APN IP: "IPv4" or "IPv4 and IPv6"
- APN is Enabled,
- APN Id: 2
- APN Name: VZWADMIN
- APN IP: "IPv4" or "IPv4 and IPv6"
- APN is Enabled,
- APN Id: 3
- APN Name: VZWINTERNET
- APN IP: "IPv4" or "IPv4 and IPv6"
- APN is Enabled,
- APN Id: 4
- APN Name: VZWAPP
- APN IP: "IPv4" or "IPv4 and IPv6"
- APN is Enabled,

Step 8: The device cannot browse public internet,

Step 10: The current internet APN is set to disabled,

Step 14: Device successfully launches public internet website.

Step 18: The device cannot browse public internet,

Step 20: The DUT returns the following values for APN:

- APN Id: 1
- APN Name: IMS

- APN IP: "IPv4" or "IPv4 and IPv6"
- APN is Enabled,
- APN Id: 2
- APN Name: VZWADMIN
- APN IP: "IPv4" or "IPv4 and IPv6"
- APN is Enabled,
- APN Id: 3
- APN Name: FOTATestFactoryReset
- APN IP: "IPv4" or "IPv4 and IPv6"
- APN is Enabled,
- APN Id: 4
- APN Name: VZWAPP
- APN IP: "IPv4" or "IPv4 and IPv6"
- APN is Enabled,

Step 23: Device successfully launches public internet website.

Design Steps
Step Name

Power Cycle

Pre-Conditions
Procedures

1. Verify the DUT can browse internet by going to a public internet website such as www.yahoo.com,

2. Using the OTADM Server, select the DUT,

3. From the OTADM Server, send a Get command to retrieve Internet APN nodes,

4. Wait till the device returns all the APN values to the server,

5. Verify the Internet APN values,

6. From the OTADM Server, send an Exec command to disable the Internet APN,

7. Wait till the ATM transaction completes,

8. Verify the device now cannot browse internet by attempt to launch a public website such

as www.yahoo.com,

9. Power Cycle the device

10. Repeat Steps 2-4 to retrieve the Internet APN settings again,

11. Verify the current "Enabled" property is set to "false",

12. From the OTADM Server, send an Exec command to enable the Internet APN,

13. Wait till the APN transaction completes,

14. Verify the device can now browse internet by launching a public website such as www.yahoo.com.

15. Using the OTADM Server, select the DUT,

16. Perform the Replace operations from the DM Server on the DUT
./ManagedObjects/ConnMO/LTE/APN/3/Setting/Name VZWTest

17. Wait till the ATM transaction completes,

18. Verify the device now cannot browse internet by attempt to launch a public website such as www.yahoo.com,

19. Go in to DUT settings and perform a Full Factory Reset

20. Perform the GET operations from the DM Server on the DUT
./ManagedObjects/ConnMO/LTE/APN/3/Setting/Name

21. Perform the Replace operations from the DM Server on the DUT
./ManagedObjects/ConnMO/LTE/APN/3/Setting/Name VZWINTERNET

22. Wait till the APN transaction completes,

23. Verify the device can now browse internet by launch a public website such as www.yahoo.com.

Expected Results

Step1: The device can browse public internet successfully,

Step 5: the DUT returns the following values for all APNs:

- APN Id: 1
- APN Name: IMS
- APN IP: "IPv4" or "IPv4 and IPv6"
- APN is Enabled,
- APN Id: 2
- APN Name: VZWADMIN
- APN IP: "IPv4" or "IPv4 and IPv6"
- APN is Enabled,
- APN Id: 3
- APN Name: VZWINTERNET
- APN IP: "IPv4" or "IPv4 and IPv6"
- APN is Enabled,
- APN Id: 4
- APN Name: VZWAPP
- APN IP: "IPv4" or "IPv4 and IPv6"
- APN is Enabled,

Step 8: The device cannot browse public internet,

Step 10: The current internet APN is set to disabled,

Step 14: Device successfully launches public internet website.

Step 18: The device cannot browse public internet,

Step 20: The current internet APN name is set to VZWTest

Step 23: Device successfully launches public internet website.

1.22 Verify DMAcc Nodes VZ_TC_LTEFIELDOA_7373996

Test and verify that that the DMAcc nodes are implemented in the device correctly. This test case verifies support of VZ_REQ_LTEOTADM_7671.

Design Steps
Step Name
Verify the DMAcc nodes
Pre-Conditions
1. Ensure the device is powered on and has sufficient battery power to establish and maintain a data call. 2. Ensure the device is connected to the LTE live network (can be verified by the "4G" network indicator displayed on device UI or connection manager),
Procedures
1. Using OTADM Server GUI, select the DUT. 2. Send a Get command to retrieve the various node values of the DMAcc DM tree. 3. Wait for the data to be retrieved from the DUT. 4. Verify the DMAcc tree nodes returned values. 5. Close the results window.
Expected Results
The device shall successfully complete the transactions without an error message, and return the values as specified in Table below.

DMAcc Subtree			
DMAcc Subtree	*Expected Result*	Value Type	Comma nds
./DMAcc/AppID	W7	Char	Get
./DMAcc/ServerID	com.vzwdmserver	Char	Get
./DMAcc/Name	VZW DM Server	Char	Get
./DMAcc/AppAddr	Addr/AddrType/Port	Char	Get
./DMAcc/AppAddr/Addr	https://4g3.vzwdm.com	Char	Get

./DMAcc/AppAddr/AddrType	URI	Char	Get
./DMAcc/AppAddr/Port	443	Char	Get
./DMAcc/AAuthPref	syncml:auth-md5	Char	Get
./DMAcc/AppAuth	Client/Server		Get
./DMAcc/AppAuth/Client	AAuthLevel/AAuthType/AAuthName/AAuthSecret/AAuthData		Get
./DMAcc/AppAuth/Client/AAuthLevel	CLCRED	Char	Get
./DMAcc/AppAuth/Client/AAuthType	Digest	Char	Get
./DMAcc/AppAuth/Client/AAuthName	IMEI	Char	Get
./DMAcc/AppAuth/Server	AAuthLevel/AAuthType/AAuthName/AAuthSecret/AAuthData		Get
./DMAcc/AppAuth/Server/AAuthLevel	SRVCRED	Char	Get
./DMAcc/AppAuth/Server/AAuthType	Digest	Char	Get
./DMAcc/AppAuth/Server/AAuthName	com.vzwdmserver	Char	Get

Design Steps
Step Name

Verify values persist after FDR

Pre-Conditions
Procedures

Perform a factory data reset on the device.

Rerun the first step of this test case

Expected Results

Verify the values persisted through the factory data reset.

1.23 Verify REPLACE on the DMAcc nodes VZ_TC_LTEFIELDOA_7374147

Verify that the REPLACE on the DMAcc nodes are implemented in the device correctly. This test case verifies support of VZ_REQ_LTEOTADM_7671.

Design Steps
Step Name
Verify REPLACE on the DMAcc nodes
Pre-Conditions
1. Ensure the device is powered on and has sufficient battery power to establish and maintain a data call.   2. Ensure the device is connected to the LTE live network (can be verified by the "4G" network indicator displayed on device UI or connection manager).
Procedures
1. Using OTADM Server GUI, select the DUT.   2. Send a Replace command to change the AppAddr node values of the DMAcc DM tree.   3. Wait for the data to be retrieved from the DUT.   4. Verify the DMAcc tree nodes returned values.   5. Close the results window.
Expected Results
The device shall successfully complete the transactions without an error message, and return the values as specified in the Table below.

DMAcc Subtree			
DMAcc Subtree	*Expected Result*	**Value Type**	**Commands**
./DMAcc/AppAddr/Addr	Replace the value with i.e. parameters (https://, port: 8443, URI) and verify that device utilizes the new value.	Char	Replace
./DMAcc/AppAddr/AddrType	Replace the value with i.e. parameters (https://, port: 8443, URI) and verify that	Char	Replace

	device utilizes the new value.		
./DMAcc/AppAddr/Port	Replace the value with i.e. parameters (https://, port: 8443, URI) and verify that device utilizes the new value.	Char	Replace

Design Steps	
Step Name	
Verify Replaced nodes do not persist through a software flash with the service support tool or OEM provided APK	
Pre-Conditions	
Values in the DMACC subtree have been modified	
Procedures	
Perform a software flash with the service support tool or OEM provided APK. Rerun Step 1	
Expected Results	
Verify the changes to the DMACC nodes did not persist through the software flash	

1.24 Verify the DevInfo nodes VZ_TC_LTEFIELDOA_7374180

Verify that the GET on the DevInfo nodes are implemented in the device correctly. This test case verifies support of VZ_REQ_LTEOTADM_7672.

Design Steps
Step Name
Verify the DevInfo nodes
Pre-Conditions
1. Ensure the device is powered on and has sufficient battery power to establish and maintain a data call.   2. Ensure the device is connected to the LTE live network (can be verified by the "4G" network indicator displayed on device UI or connection manager).
Procedures
1. Using OTADM Server GUI, select the DUT.   2. Send a GET command to retrieve the various node values of the DevInfo DM tree.   3. Wait for the data to be retrieved from the DUT.   4. Verify the DevInfo tree nodes returned values.   5. Close the results window.
Expected Results
The device shall successfully complete the transactions without an error message, and return the values as specified in the Table below.

DevInfo Nodes	Expected Result	Value Type	Command
./DevInfo/DevId	"IMEI:x", with x being the value of the IMEI (without quotes).	Char	Get
./DevInfo/DmV	1.2	Char	Get
./DevInfo/Lang	English or en_us	Char	Get
./DevInfo/Man	<Manufacturer Name>	Char	Get

	<Model number> Note: value must match with the model number listed in Tech Survey		
./DevInfo/Mod	<Model number> Note: value must match with the model number listed in Tech Survey	Char	Get
./DevInfo/Ext	Node	Char	Get
./DevInfo/Ext/ICCID	UICC's ICCID Value, <null> is acceptable if UICC is not present in device. Device shall attempt to read the value of ICCID every time device is powered on. Device shall report the ICCID Extension Node value during a Device Management Package 1 session along with all the other DevInfo node values.		Get

Design Steps
Step Name

Verify values persist after a factory data reset

Pre-Conditions
Procedures

Perform a factory data reset on the device

Rerun step 1 of this test case

Expected Results

Verify the values persisted throught the factory data reset

1.25 Verify the DevDetail node VZ_TC_LTEFIELDOA_7374181

Verify that the GET on the DevDetail nodes are implemented in the device correctly. This test case verifies support of VZ_REQ_LTEOTADM_7673.

Design Steps
Step Name
Verify the DevDetail nodes
Pre-Conditions
1. Ensure the device is powered on and has sufficient battery power to establish and maintain a data call. 2. Ensure the device is connected to the LTE live network (can be verified by the "4G" network indicator displayed on device UI or connection manager).
Procedures
1. Using OTADM Server GUI, select the DUT. 2. Send a GET command to retrieve the various node values of the DevDetail DM tree. 3. Wait for the data to be retrieved from the DUT. 4. Verify the DevDetail tree nodes returned values. 5. Close the results window.
Expected Results
The device shall successfully complete the transactions without an error message, and return the values as specified in the Table below.

DevDetail Nodes	Expected Result	Value type	Command
./DevDetail/URI	MaxDepth/MaxSegLen/MaxTotLen	Char	Get
./DevDetail/URI/MaxDepth	12	Char	Get
./DevDetail/URI/MaxSegLen	32	Char	Get
./DevDetail/URI/MaxTotLen	127	Char	Get
./DevDetail/DevTyp	<value>	Char	Get

	Smartphone Tablet Basic Phone Home Mobile Hotspot Connected Device Wearable		
./DevDetail/FwV	<value>	Char	Get
./DevDetail/HwV	<value>	Char	Get
./DevDetail/LrgObj	True, False	Char	Get
./DevDetail/OEM	<value>	Char	Get
./DevDetail/SwV	<value> (*) Converged devices only - field used to track Operating System version.	Char	Get

Design Steps

Step Name

Verify values persist after a factory data reset

Pre-Conditions

Procedures

Perform a factory data reset on the device

Rerun step 1 of this test case

Expected Results

Verify values persist through the factory data reset.

1.26 APN MANAGEMENT TRIGGERED BY MOBILE AUTOMATIC DEVICE DETECTION (ADD) with Applications running <mark>VZ_TC_LTEFIELDOA_7374209</mark>

Test and verify APN management triggered by mobile activate is successful while any of the following applications are running:

1. Gmail

2. Google Maps

3. Google Search

4. Youtube

5. Facebook

6. WhatsApp

7. Google Text to Speech

8. Google Books

9. Facebook Messenger

10. Spotify

11. Tumblr

12. Snapchat

13. BBC News

14. Netflix

Repeat the below procedure when each of the above applications is running in the foreground.

Design Steps
Step Name
APN Management Triggered by Mobile Automatic Device Detection (ADD) - LTE
Pre-Conditions

1. Device with UICC is powered on and registered with live LTE network

2. Access to a non-commercial (test) OTADM Server is available

3. OEM instruction of changing device bootstrap is available

Procedures

1. Run one application from the above list in the foreground

2. Use the Test OTADM Server GUI, and retrieve the complete ConnMO tree; Get the vendor defined "*" values for all LTE APN names, and identify the * value for VZWINTERNET APN

3. From the OTADM Server, send a Replace command to change the VZWINTERNET APN value to "vzwtest". Wait for values to be returned

4. Replace the Internet APN name back to VZWINTERNET

5. Repeat steps 1 – 4 while each of the applications from the list above are running in the foreground

Expected Results

Step 2: Verify DUT returns all APN names

Step 3: Verify that DUT cannot access the Internet

Step 4: Verify that DUT can access the Internet

Step 5: The device should provide appropriate responses to the commands from the DM server while each of the applications is running in the foreground

1.27 Root Certificate Verification VZ_TC_LTEFIELDOA_8408737

This test case will verify that the device can setup a SSL connection with the DM server using the following Root Certificates:

- DigiCert Global Root CA (Serial #: 08:3B:E0:56:90:42:46:B1:A1:75:6A:C9:59:91:C7:4A)
- DigiCert Global Root G2 (Serial #: 03:3A:F1:E6:A7:11:A9:A0:BB:28:64:B1:1D:09:FA:E5)
- DigiCert Trusted Root G4 (Serial #: 05:9B:1B:57:9E:8E:21:32:E2:39:07:BD:A7:77:75:5C)
- DigiCert TLS ECC P384 Root G5 (Serial #: 09:E0:93:65:AC:F7:D9:C8:B9:3E:1C:0B:04:2A:2E:F3)
- DigiCert TLS RSA4096 Root G5 (Serial #: 08:F9:B4:78:A8:FA:7E:DA:6A:33:37:89:DE:7C:CF:8A)

The test will also verify whether the device uses the following Cipher Suites:

- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xC02F)
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xC030)

Design Steps
Step Name
Step 1 -- DigiCert Global Root CA
Pre-Conditions
Device has pre-loaded the following Root Certificates: DigiCert Global Root CA (Serial #: 08:3B:E0:56:90:42:46:B1:A1:75:6A:C9:59:91:C7:4A) DigiCert Global Root G2 (Serial #: 03:3A:F1:E6:A7:11:A9:A0:BB:28:64:B1:1D:09:FA:E5) DigiCert Trusted Root G4 (Serial #: 05:9B:1B:57:9E:8E:21:32:E2:39:07:BD:A7:77:75:5C) DigiCert TLS ECC P384 Root G5 (Serial #: 09:E0:93:65:AC:F7:D9:C8:B9:3E:1C:0B:04:2A:2E:F3) DigiCert TLS RSA4096 Root G5 (Serial #: 08:F9:B4:78:A8:FA:7E:DA:6A:33:37:89:DE:7C:CF:8A) Device has pre-loaded the following Cipher Suites: •   •   • TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xC02F)

- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xC030)

Procedures

1. Setup the OMADM server with only the DigiCert Global Root CA root certificate only.
2. Power on the device.
3. Initiate a DM session with the DUT from the DM Server.
4. The device should be able to successfully setup a connection with the DM server using the DigiCert Global Root CA root certificate.
5. Verify the Logs on the DM server to see whether the device used the appropriate Cipher Suites.

Expected Results

1. OMADM server is setup with only the DigiCert Global Root CA root certificate only.
2. The device powers on and attaches to the network.
3. The device responds to the WAP Push from the DM server.
4. The device successfully sets up a connection with the DM server using the DigiCert Global Root CA root certificate.
5. DM server logs show that the device connected with the DM server using the DigiCert Global Root CA root certificate and the appropriate Cipher Suite.

Design Steps

Step Name

Step 2 -- DigiCert Global Root G2

Pre-Conditions

Device has pre-loaded the following Root Certificates:

DigiCert Global Root CA (Serial #: 08:3B:E0:56:90:42:46:B1:A1:75:6A:C9:59:91:C7:4A)
DigiCert Global Root G2 (Serial #: 03:3A:F1:E6:A7:11:A9:A0:BB:28:64:B1:1D:09:FA:E5)
DigiCert Trusted Root G4 (Serial #: 05:9B:1B:57:9E:8E:21:32:E2:39:07:BD:A7:77:75:5C)

DigiCert TLS ECC P384 Root G5 (Serial #: 09:E0:93:65:AC:F7:D9:C8:B9:3E:1C:0B:04:2A:2E:F3)

DigiCert TLS RSA4096 Root G5 (Serial #:
08:F9:B4:78:A8:FA:7E:DA:6A:33:37:89:DE:7C:CF:8A)

Device has pre-loaded the following Cipher Suites:

-
-
    - TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xC02F)
    - TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xC030)

Procedures

1. Setup the OMADM server with only the DigiCert Global Root G2 root certificate only.
2. Power on the device.
3. Initiate a DM session with the DUT from the DM Server.
4. The device should be able to successfully setup a connection with the DM server using the DigiCert Global Root G2 root certificate.
5. Verify the Logs on the DM session to see whether the device used the appropriate Cipher Suites.

Expected Results

1. OMADM server is setup with only the DigiCert Global Root G2 root certificate only.
2. The device powers on and attaches to the network.
3. The device responds to the WAP Push from the DM server.
4. The device successfully sets up a connection with the DM server using the DigiCert Global Root G2 root certificate.
5. DM server logs show that the device connected with the DM server using the DigiCert Global Root G2 root certificate and the appropriate Cipher Suites.

Design Steps

Step Name

Step 3 -- DigiCert Trusted Root G4

Pre-Conditions

Device has pre-loaded the following Root Certificates:

DigiCert Global Root CA (Serial #: 08:3B:E0:56:90:42:46:B1:A1:75:6A:C9:59:91:C7:4A)
DigiCert Global Root G2 (Serial #: 03:3A:F1:E6:A7:11:A9:A0:BB:28:64:B1:1D:09:FA:E5)
DigiCert Trusted Root G4 (Serial #: 05:9B:1B:57:9E:8E:21:32:E2:39:07:BD:A7:77:75:5C)

DigiCert TLS ECC P384 Root G5 (Serial #:
09:E0:93:65:AC:F7:D9:C8:B9:3E:1C:0B:04:2A:2E:F3)

DigiCert TLS RSA4096 Root G5 (Serial #:
08:F9:B4:78:A8:FA:7E:DA:6A:33:37:89:DE:7C:CF:8A)

Device has pre-loaded the following Cipher Suites:

-
-
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xC02F)
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xC030)

Procedures

1. Setup the OMADM server with only the DigiCert Trusted Root G4 root certificate only.
2. Power on the device.
3. Initiate a DM session with the DUT from the DM Server.
4. The device should be able to successfully setup a connection with the DM server using the DigiCert Trusted Root G4 root certificate.
5. Verify the Logs on the DM session to see whether the device used the appropriate Cipher Suites.

Expected Results

1. OMADM server is setup with only the DigiCert Trusted Root G4 root certificate only.
2. The device powers on and attaches to the network.
3. The device responds to the WAP Push from the DM server.
4. The device successfully sets up a connection with the DM server using the DigiCert Trusted Root G4 root certificate.
5. DM server logs show that the device connected with the DM server using the DigiCert Trusted Root G4 root certificate and the appropriate Cipher Suites.

Design Steps

Step Name

Step 4- Verify DigiCert TLS ECC P384 Root G5

Pre-Conditions

Device has pre-loaded the following Root Certificates:

DigiCert Global Root CA (Serial #: 08:3B:E0:56:90:42:46:B1:A1:75:6A:C9:59:91:C7:4A)
DigiCert Global Root G2 (Serial #: 03:3A:F1:E6:A7:11:A9:A0:BB:28:64:B1:1D:09:FA:E5)
DigiCert Trusted Root G4 (Serial #: 05:9B:1B:57:9E:8E:21:32:E2:39:07:BD:A7:77:75:5C)

DigiCert TLS ECC P384 Root G5 (Serial #:
09:E0:93:65:AC:F7:D9:C8:B9:3E:1C:0B:04:2A:2E:F3)

DigiCert TLS RSA4096 Root G5 (Serial #:
08:F9:B4:78:A8:FA:7E:DA:6A:33:37:89:DE:7C:CF:8A)

Device has pre-loaded the following Cipher Suites:

-
-
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xC02F)
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xC030)

Procedures

1. Setup the OMADM server with only the DigiCert Trusted Root G4 root certificate only.
2. Power on the device.
3. Initiate a DM session with the DUT from the DM Server.
4. The device should be able to successfully setup a connection with the DM server using the DigiCert Trusted Root G4 root certificate.

5. Verify the Logs on the DM session to see whether the device used the appropriate Cipher Suites.

Expected Results

1. OMADM server is setup with only the DigiCert Trusted Root G4 root certificate only.
2. The device powers on and attaches to the network.
3. The device responds to the WAP Push from the DM server.
4. The device successfully sets up a connection with the DM server using the DigiCert Trusted Root G4 root certificate.
5. DM server logs show that the device connected with the DM server using the DigiCert Trusted Root G4 root certificate and the appropriate Cipher Suites.

Design Steps

Step Name

Step 5- DigiCert TLS RSA4096 Root G5

Pre-Conditions

Device has pre-loaded the following Root Certificates:

DigiCert Global Root CA (Serial #: 08:3B:E0:56:90:42:46:B1:A1:75:6A:C9:59:91:C7:4A)
DigiCert Global Root G2 (Serial #: 03:3A:F1:E6:A7:11:A9:A0:BB:28:64:B1:1D:09:FA:E5)
DigiCert Trusted Root G4 (Serial #: 05:9B:1B:57:9E:8E:21:32:E2:39:07:BD:A7:77:75:5C)

DigiCert TLS ECC P384 Root G5 (Serial #: 09:E0:93:65:AC:F7:D9:C8:B9:3E:1C:0B:04:2A:2E:F3)

DigiCert TLS RSA4096 Root G5 (Serial #: 08:F9:B4:78:A8:FA:7E:DA:6A:33:37:89:DE:7C:CF:8A)

Device has pre-loaded the following Cipher Suites:

-

-
- • TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xC02F)
- • TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xC030)

Procedures

1. Setup the OMADM server with only the DigiCert Trusted Root G4 root certificate only.
2. Power on the device.
3. Initiate a DM session with the DUT from the DM Server.
4. The device should be able to successfully setup a connection with the DM server using the DigiCert Trusted Root G4 root certificate.
5. Verify the Logs on the DM session to see whether the device used the appropriate Cipher Suites.

Expected Results

1. OMADM server is setup with only the DigiCert Trusted Root G4 root certificate only.
2. The device powers on and attaches to the network.
3. The device responds to the WAP Push from the DM server.
4. The device successfully sets up a connection with the DM server using the DigiCert Trusted Root G4 root certificate.
5. DM server logs show that the device connected with the DM server using the DigiCert Trusted Root G4 root certificate and the appropriate Cipher Suites.

01.29 HTTP Header X-Session-Type Validation VZ_TC_LTEFIELDOA_4105999311930956

This test case is to validate the device is supporting HTTP Header X-Session -Type parameter in device management scenarios.

Design Steps
Step Name
Step 1- NI
Pre-Conditions
Device is powered on and in an acceptable Verizon coverage area.
Procedures
Start a Network initiated session from the DM server and perform a GET operation on the node ./DevDetail/FwV
Expected Results
Verify in server log the device provided the expected firmware version. Logs also indicate the device connected with HTTP Header parameter X-Session-Type: network
Design Steps
Step Name
Step 2- DI
Pre-Conditions
This test step is applicable to devices supporting DI jobs with a periodic check-in mechanism. Device is in good coverage and is active for service with Verizon and powered on.
Procedures

From the DM server, initiated a session with the DUT and REPLACE the node ./ManagedObjects/DCMO/CheckIn/Value with a value of -5

Close the DM session and wait a period of 5 minutes to allow device to check in with the server

Expected Results

Validate the check in occurred at the expected interval based on server logs.

Verify the HTTP X-Session-Type Header showed a value of X-Session-Type: device

Design Steps

Step Name

Step 3- UI

Pre-Conditions

This step is only applicable to devices supporting a user initiated check in mechanism (Check for update, etc.)

Device is in good VZ coverage and is active on the network

DUT is powered on

Procedures

From the UI (or other OEM specified means) generate a check for update from the devices user interface.

Await response from server. Proceed with the defined user experience to apply the update if applicable

Expected Results

From the server logs validate the device sent a user initiated check in to the server

Verify the device supplied the X-Session-Type: user in the HTTP header

RequirementCoverageForTestPlan

01.01 VERIFY LTE CONNMO DM TREES VZ_TC_LTEFIELDOA_8540

Requirement Name	Requirement Plan Id	Created By	Created Date
ADD Flow Requirements	LTEOTADM	Admin User	11-07-0013 15:01:17
APN ID	LTEOTADM	Admin User	11-07-0013 15:01:24
APN Name	LTEOTADM	Admin User	11-07-0013 15:01:27
APN Name Format	LTEOTADM	Admin User	11-07-0013 15:01:48
Connectivity Management	LTEOTADM	Admin User	11-07-0013 15:01:19
Enabled	LTEOTADM	Admin User	11-07-0013 15:01:30
IP	LTEOTADM	Admin User	11-07-0013 15:01:29
Service Availability for APN Parameter Changes	LTEOTADM	Admin User	11-07-0013 15:01:25

01.02 APN MANAGEMENT TRIGGERED BY MOBILE AUTOMATIC DEVICE DETECTION (ADD) VZ_TC_LTEFIELDOA_8549

Requirement Name	Requirement Plan	Created By	Created Date

	Id		
ADD Flow Requirements	LTEOTADM	Admin User	11-07-0013 15:01:17
APN ID	LTEOTADM	Admin User	11-07-0013 15:01:24
APN Name	LTEOTADM	Admin User	11-07-0013 15:01:27
APN Name Format	LTEOTADM	Admin User	11-07-0013 15:01:48
Connectivity Management	LTEOTADM	Admin User	11-07-0013 15:01:19
Enabled	LTEOTADM	Admin User	11-07-0013 15:01:30
IP	LTEOTADM	Admin User	11-07-0013 15:01:29
Service Availability for APN Parameter Changes	LTEOTADM	Admin User	11-07-0013 15:01:25

01.05 OTADM-013-IPv6 Successful Connectivity Testing VZ_TC_LTEFIELDOA_8552

Requirement Name	Requirement Plan Id	Created By	Created Date
Connection Failure During a DM Session	LTEOTADM	Admin User	01-15-0014 09:32:59
Connection Setup Failure	LTEOTADM	Admin	01-15-0014

		User	09:26:51
Connectivity Management	LTEOTADM	Admin User	11-07-0013 15:01:19
IPv6 Connection	LTEOTADM	Admin User	01-15-0014 09:14:52

01.06 OTADM-014-IPv4 Successful Connectivity Testing VZ_TC_LTEFIELDOA_8553

Requirement Name	Requirement Plan Id	Created By	Created Date
Connection Failure During a DM Session	LTEOTADM	Admin User	01-15-0014 09:32:59
Connection Setup Failure	LTEOTADM	Admin User	01-15-0014 09:26:51
Connectivity Management	LTEOTADM	Admin User	11-07-0013 15:01:19
IPv6 Connection	LTEOTADM	Admin User	01-15-0014 09:14:52

01.07 DEVINFO EXTENSION NODE TEST VZ_TC_LTEFIELDOA_8554

Requirement Name	Requirement Plan Id	Created By	Created Date
ICCID Extended Node Support	LTEOTADM	Admin User	11-07-0013 15:12:09

01.08 APN Management by OTADM server VZ_TC_LTEFIELDOA_8555

Requirement Name	Requirement Plan Id	Created By	Created Date
ADD Flow Requirements	LTEOTADM	Admin User	11-07-0013 15:01:17
Service Availability for APN Parameter Changes	LTEOTADM	Admin User	11-07-0013 15:01:25

01.09 AUTHENTICATION SECURITY KEY MIS-MATCH VZ_TC_LTEFIELDOA_8541

Requirement Name	Requirement Plan Id	Created By	Created Date
DM Notification via SMS message (Trigger)	LTEOTADM	Admin User	11-07-0013 15:01:57
LTE Service Required	LTEOTADM	Admin User	11-07-0013 15:01:03
LTE Service Required	LTEOTADM	Admin User	11-07-0013 15:01:07
Network Initiated (NI) Retry	LTEOTADM	Admin User	11-07-0013 15:01:04
Update - Fatal Error	LTEOTADM	Admin User	11-07-0013 15:01:15

01.10 AUTHENTICATION SECURITY KEY MATCH VZ_TC_LTEFIELDOA_8542

Requirement Name	Requirement Plan Id	Created By	Created Date
Authentication Key	LTEOTADM	Admin User	11-07-0013 15:00:50
Confidentiality (Data Encryption)	LTEOTADM	Admin User	11-07-0013 15:01:49
DM Notification via SMS message (Trigger)	LTEOTADM	Admin User	11-07-0013 15:01:57
Factory Bootstrapping	LTEOTADM	Admin User	11-07-0013 15:01:43
Failed Authentication Attempt Handling	LTEOTADM	Admin User	11-07-0013 15:00:48
LTE Service Required	LTEOTADM	Admin User	11-07-0013 15:01:03
LTE Service Required	LTEOTADM	Admin User	11-07-0013 15:01:07
Mutual Authentication	LTEOTADM	Admin User	11-07-0013 15:01:56
Network Initiated (NI) Retry	LTEOTADM	Admin User	11-07-0013 15:01:04
PDN Provisioning for OTADM Device Management Traffic	LTEOTADM	Admin User	11-07-0013 15:01:46
Package 0 Authentication (Notification Initiation Session Message)	LTEOTADM	Admin User	11-07-0013 15:01:52

Update - Fatal Error	LTEOTADM	Admin User	11-07-0013 15:01:15
User Experience (Device)	LTEOTADM	Admin User	11-07-0013 15:00:32

01.13 CONNMO TREE INTERNET APN VERIFICATION AND OPERATION VZ_TC_LTEFIELDOA_8545

Requirement Name	Requirement Plan Id	Created By	Created Date
Connectivity Management	LTEOTADM	Admin User	11-07-0013 15:01:19

01.14 CONNMO TREE APP APN VERIFICATION AND OPERATION VZ_TC_LTEFIELDOA_8546

Requirement Name	Requirement Plan Id	Created By	Created Date
Connectivity Management	LTEOTADM	Admin User	11-07-0013 15:01:19

01.15 CONNMO TREE SMS OVER IMS VERIFICATION AND OPERATION VZ_TC_LTEFIELDOA_8547

Requirement Name	Requirement Plan Id	Created By	Created Date
Connectivity Management	LTEOTADM	Admin User	11-07-0013 15:01:19

01.16 APN NAMES CASE INSENSITIVE TEST VZ_TC_LTEFIELDOA_8548

Requirement Name	Requirement Plan Id	Created By	Created Date
ConnMO Replace Command - Values not case sensitive	LTEOTADM	Admin User	11-07-0013 15:01:20
Connectivity Management	LTEOTADM	Admin User	11-07-0013 15:01:19

01.17 TLS Protocol for DM sessions VZ_TC_LTEFIELDOA_8842

Requirement Name	Requirement Plan Id	Created By	Created Date
Authentication Key	LTEOTADM	Admin User	11-07-0013 15:00:50
Commands	LTEOTADM	Admin User	11-07-0013 15:00:54
Confidentiality (Data Encryption)	LTEOTADM	Admin User	11-07-0013 15:01:49
DMAcc Subtree	LTEOTADM	Admin User	11-07-0013 15:00:58
DevDetail Subtree	LTEOTADM	Admin User	11-07-0013 15:01:01
DevInfo Subtree	LTEOTADM	Admin User	11-07-0013 15:00:59

Failed Authentication Attempt Handling	LTEOTADM	Admin User	11-07-0013 15:00:48
Integrity	LTEOTADM	Admin User	11-07-0013 15:00:51
Mutual Authentication	LTEOTADM	Admin User	11-07-0013 15:01:56
OTA Device Management Tree Support	LTEOTADM	Admin User	11-07-0013 15:00:53
Package o Authentication (Notification Initiation Session Message)	LTEOTADM	Admin User	11-07-0013 15:01:52
Root Certificate requirements	LTEOTADM	Admin User	05-30-0014 13:31:35
Verizon Wireless Defined Base DM Tree	LTEOTADM	Admin User	11-07-0013 15:00:56

1.24 Verify the DevInfo nodes VZ_TC_LTEFIELDOA_7374180

Requirement Name	Requirement Plan Id	Created By	Created Date
DevInfo Subtree	LTEOTADM	Vipul Patel	11-07-0013 15:00:59

1.27 Root Certificate Verification VZ_TC_LTEFIELDOA_8408737

Requirement Name	Requirement Plan Id	Created By	Created Date
Confidentiality (Data Encryption)	LTEOTADM	James Paxton	11-07-0013 15:01:49
Root Certificate requirements	LTEOTADM	James Paxton	05-30-0014 13:31:35