Release Notes

SV9100 CP20 R10.60.55

Product	-	Univerge SV9100
Version	-	Release 10.60.55
Date	-	21-Sep-2020
Document Reference	-	FCO 2020.077
Category	-	New Features
Issued by	-	NEC Enterprise Solutions EMEA

Queries concerning this document can be addressed to SMB.TECHSUPPORT@EMEA.NEC.COM

Contents

1. INTRODUCTION

This FCO provides information about the Maintenance Release of Univerge SV9100 CP20 Main Software.

- SV9100 CP20 Main Software 10.60.55

2. IDENTIFICATION

This release is SV9100 CP20 Main Software 10.60.55.

3. COMPATIBILITY

Any UNIVERGE SV9100 CP20 can be upgraded with this system software.

4. UPGRADE INSTRUCTIONS

It is always advisable to save the system configuration prior to any upgrade.

WARNING: Powering off while card firmware is occurring, can cause corruption of cards. Please ensure all cards are running (up to 10 minutes after upgrade dependent on number and type of cards (LCF upgrade is longest) before performing any reset. See further explanation later in this document.

To perform a system software and firmware upgrade:

1. Turn the system power off.
2. Once the system has powered down, insert the USB Memory containing the software upgrade into the USB port on the GCD-CP20.
3. Push in and hold the **Load** button.
4. Turn the system power on.
5. Continue holding the **Load** button for approximately 10 seconds or until Status LED5 begins flashing red.
6. Release the **Load** button.
7. Wait until the Status LEDs on the GCD-CP20 have the following indications (approximately two minutes):
   LED 2: Flashing Red
   LED 3: Flashing Red
   LED 4: Flashing Red
   LED 5: Steady Red
8. Turn the system power off and un-install the USB Memory.
9. Turn the system power back on.
10. When the system has completed reloading the software, the Status LED begins flashing on the GCD-CP20. The remaining four LEDs are off.
    - To confirm the new software version has been installed, the system version number can be viewed by pressing the FEATURE + 3 keys on any display multiline terminal.
    - The existing system software in the flash memory is replaced, but the customer data (stored in the RAM) is saved.

Or via Remote

First create a remote upgrade file from the same software you would add to the USB stick.

From the ribbon bar, select Create SW file:
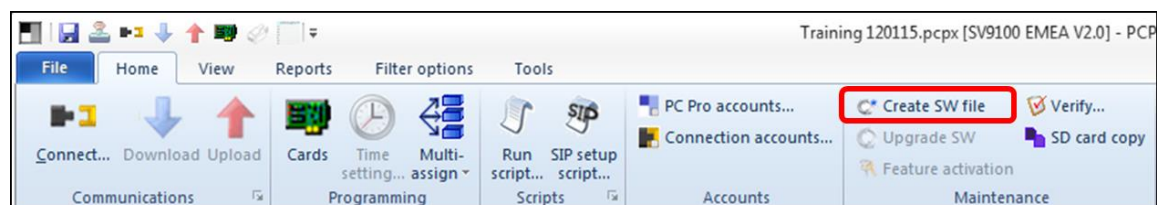
This will pop a window:
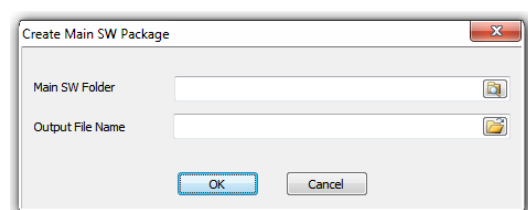
Select the area of the Main SW and where to save the output of the remote upgrade file:
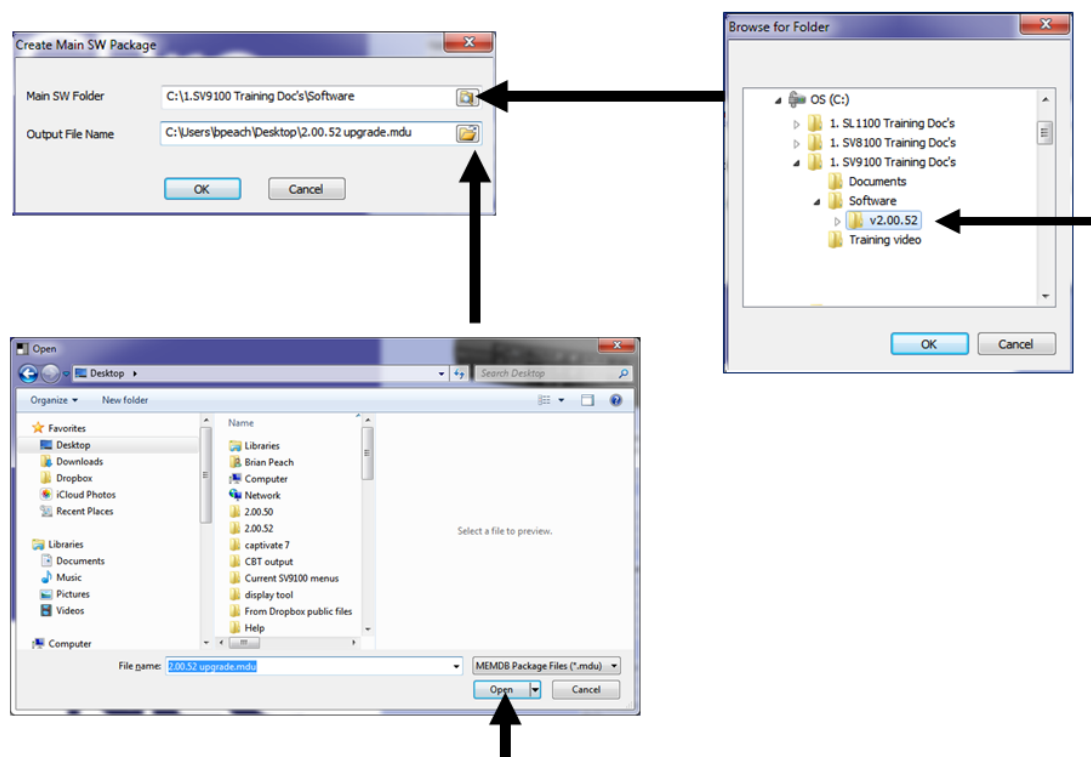
Connect to the system via PCPro in the normal manner, and from the ribbon bar select Upgrade SW
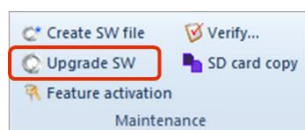
In the File box, select the mdu file you created for the upgrade, then select when the upgrade should occur (immediately or the date specified). At this point the system will perform its normal upgrade cycle and reboot.
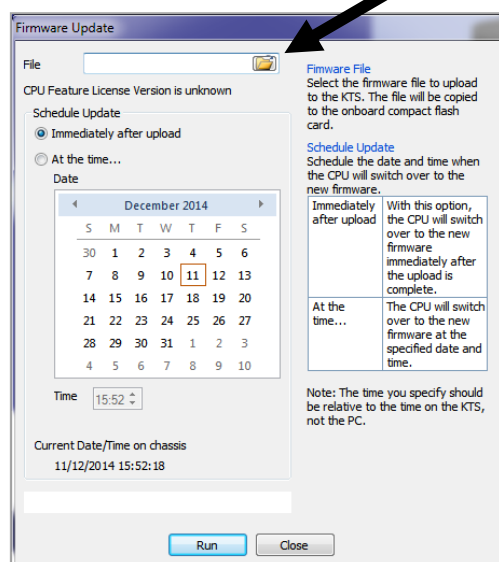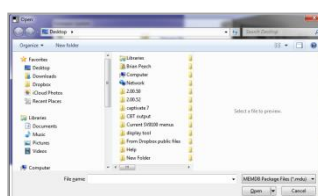
Main Software Upgrade and Option Card Firmware

After a main software upgrade the SV9100 reboots (either manually if via USB or automatically if via PcPro/Webpro).

After reboot the main software will then push out to the option cards (including IPLE) any firmware updates.

Firmware updates are not always required, it is dependent on version upgrading from and to.

It is important that during this firmware upgrade the system is not reset, as doing so interrupts the firmware upgrade and can cause corruption of the cards performing upgrade at the time.

Upgrade in a Netlink Environment

1. Access Primary system via PCPro or WebPro in NetLink network.
2. Set PRG51-16-01 to Disable.
   Note: This change prevents replication error from occurring between systems.
3. Access Secondary systems via PCPro or WebPro in NetLink network.
   Note: Upgrade should start with Secondary systems to update properly.
   As such NetLink network is kept up, and you do not need to worry about
   the presence of substitute Primary system.
4. Upgrade main system software of Secondary systems.
   Note: Check it has upgraded the main system software of all properly.
5. Upgrade main system software of Primary system.
   Note: Check it has upgraded the main system software properly.
6. Restore PRG51-16-01 to previous setting data.

5. FUNCTIONAL CHANGES

Support for SV9100 R10.60.55 Features:

- 8 Digit DDI Support

Selecting 35-02-16 as Both (8 Digits) allows 8 digit SMDR to be passed to applications. Useful when the DDI's overlap more than the 6 end digits.
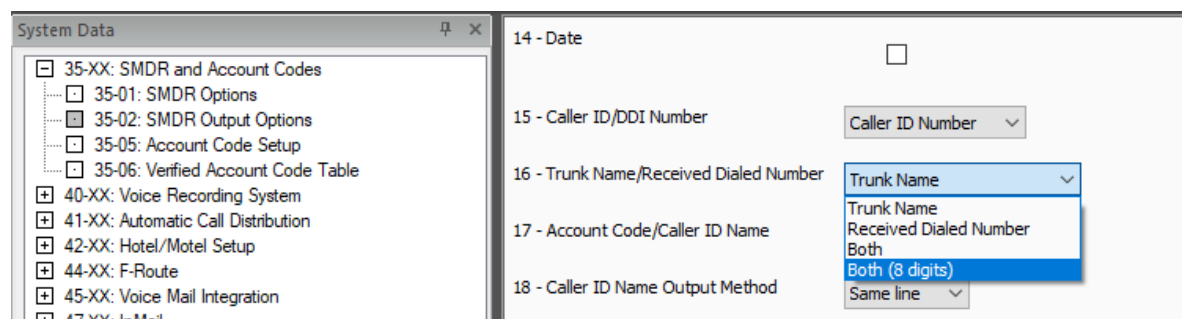
InGuard V1.8 and InReports 1.9 are required to support this feature.

6. SOLVED PROBLEMS

6.1.List of Solved Problems

The following items are fixed in this version:

F190911001	Send 480 Temporary unavailable instead of 487 request terminated when ring no answer exceeds 180 seconds
	480 Temporary unavailable sent instead of 487 request terminated when ring no answer exceeds 180 seconds. Requires CMD 84-39-51 in PCPtro version 10.51.55 to enable.

6.2. List of Previously Solved Problems

The following items are fixed in this version:

10.60.53

F200505001	PcPro and WebPro become inaccessible after O+M port use
	Seen mainly after BCT synchronises using port 8010 (10-20-01 type 11) the CPU becomes inaccessible via Web PRo and PC Pro.
F200714001	CPU stops responding to SIP Trunks connection
	SV9100 CPU card not keeps locking up with connection with SIP Trunk that receives TLS Packet from the Carrier. System reboot clears.
-	Virtual extension no longer supported in IRGs with R10.5
	virtual extension is no longer signaled on a *03 function key. In DIM it shows `chk_irg_member() >> 4003f9 is unsupported

10.50.57

Reference	Description
F160413001	restriction overide problem
	Toll restriction override issues occur if have Trunk access code set to f-Route.
F190717001	SDP Version is not incremented
	When SDP properties are changed by SIP carrier SV9100 does not increment SDP version and call is dropped by network provider.
F191219002	System doesn't play fixed message for inbound external calls if CLI is enabled
	System doesn't play fixed message for inbound external calls if CLI is enabled on the trunk. Caller may consider call has cut off.
F200206003	System is intermittently resetting
	System is intermittently resetting

10.30.53

Reference	Description
F200108001	**Intermediate Certificate not supported**
	SV9100 platform does not support use of intermediate certificates in the chain. Now corrected.

7. KNOWN PROBLEMS

The following are not problems but are listed to for awareness.

- **Virtual Extensions do not work in IRG's, introduced issue in this version, will be resolved very shortly in a new SV9100 CP20 version**

8. SECURITY

All ICT installations are at risk of unauthorized intrusion and subsequent misuse. Such intrusions may result in significant losses to the company affected, including but not limited to financial liabilities, data privacy breach, intellectual property, material assets and associated labour or legal costs.

NEC products contain a variety of features designed to help prevent and combat such misuse. To assure their effectiveness it is essential that such features are configured, deployed and maintained in an appropriate manner by the installing party in consultation with the user of the equipment.

The ultimate responsibility for assuring the overall security of the ICT installation resides with the using company. The effectiveness of their security measures depends on the quality and rigorousness of implementation of their security policy by ICT administrators and their user community.

Information about the security features in NEC products and how to configure them is contained within the product documentation.

There additions or amendments to security features in this release.

9. MATERIALS

9.1. Physical Distribution

N/A

9.2. On-line Distribution

Any software related to this release can be downloaded from the software database on BusinessNet. http://businessnet.nec-enterprise.com.