

Status:	Done
Project:	UCC_PLM
Component/s:	None
Affects Version/s:	UCC Appliance 1.1.0
Fix Version/s:	None

Type:	Bug	Priority:	Medium
Reporter:	Rajan Rajeshprasad Gupta	Assignee:	Spyros Loukopoulos (EXT)
Resolution:	Closed	Votes:	0
Labels:	None		
Remaining Estimate:	Not Specified		
Time Spent:	Not Specified		
Original Estimate:	Not Specified		

Attachments:	ENM CLI - Help Center - ieatenmc17b18 1.pdf image-2025-10-06-11-59-17-242.png image-2025-10-06-19-36-44-268.png image-2025-10-06-19-37-10-380.png image-2025-10-06-22-14-16-493.png image-2025-10-06-22-17-06-478.png image-2025-10-08-10-24-58-670.png image-2025-10-08-10-44-53-005.png image-2025-10-08-14-39-42-392.png image-2025-10-08-14-40-14-721.png
Team/s:	UCC_XFT3
Found in Build:	UCC 1.1 RC2
Requirement Status:	UCC Appliance 0.2.1 - UNCOVERED

#### Description

Hello,

We are freezing scope of work for ENM Integration with UCC for Vz.

While referring to UCC CPI document: UCC - Central O&M User Guide.

Section 2.1.1 Supported node on ENM.

It says, ENM supports the following UCC components:

| UCC - Central O&M User Guide Appliance

#### 2.1.1 Type

ENM supports the following UCC components:

- CCDM
- CCSM
- CCRC
- PCX
- SC
- UCA(EDA)
- R6675

The node-type value for each UCC node, when added to ENM, is listed in Table 2.

**Note** When a node is added as a Shared-CNF node type, release independence is mandatory. This process must be performed to retrieve the actual model for the node. For more information, see [Release Independence Manager](#).

Table 2 ENM NodeTypes

UCC Node	NodeType	neType
CCDM	CCDM	CCDM
CCSM	CCSM	CCSM
CCRC	CCRC	CCRC
PCX	Shared-CNF	Shared-CNF
SC	SC	SC
UCA	EDA	EDA
Router R6675	Router6675	Router6675

However going further reading to add nodes on ENM,

## Section 2.1 Add node

It says ENM also supports HPE servers and CCD as well.

See below:

## 2.2 Add Node

### 2.2.1 HPE Add Node to ENM

#### Prerequisites

- HPE server for UCC is already installed on site.
- ENM Custom Adaptation (CA) for HPE is installed on ENM.
- SNMP is configured for HPE server and ENM FM receiver is defined as an SNMP target.
- SNMPv3 engine-id is unique for this node.
- HPE iLO IP is reachable from ENM.
- ENM user to-add the node have the role AddNode\_Administrator assigned.

For more information on ENM configuration data, see Table 6

Table 6 ENM Configuration Data Summary

Parameter	Explanation	Value (ex.)
Type	The type of the to-be added node	HPILO
Network Element Name	Unique element name	HPE-2B
Time Zone	TMZ where UCC is located	Berlin
OSS Model Identity		1.0.0
Collection	The collection to add the NE	Transport Topology
IP Address	HPE iLO IP	214.14.143.3
SNMP Security Name	SNMP_v3_user	snmpuser
Port	SSH port	22
SNMP Agent Port	SNMP port	161
SNMP Read Community		public
SNMP Security Level	snmp-target-v3.snmp-security-level	AUTH_PRIV
SNMP Trap Port		162
SNMP Version		SNMP_V3
SNMP Write Community		public
Transport Protocol		SSH

## 2.2.2 CCD Add Node to ENM

### Prerequisites

- HPE server for UCC is already installed on site.
- SNMPv2C is configured for CCD server and ENM FM receiver is defined as an SNMP target.
- CCD OaM IP is reachable from ENM.
- ENM user to-add the node have the role AddNode\_Administrator assigned.

For more information on CCD configuration data, see Table 7

Table 7 CCD Configuration Data

Parameter	Explanation	Value (ex)
CloudInfrastructure	The cloud infrastructure MO name in ENM	CCD5A
CloudInfrastructureId	The ID of the cloud infrastructure MO when the instance is created	CCD5A
ciType	The cloud infrastructure type for the added node	CCD
clusterName	Unique element name	CCD5A
serverAddress	CCD ingress IP	214.13.22
ipAddress	Alertmanager service ingress IP	214.13.22
port	Alertmanager service port	80

### 2.2.2.1 CCD ENM GUI

Adding a CCD node to ENM topology is not supported through GUI.

### 2.2.2.2 CCD ENM CLI

CCD is added as CloudInfraStructure node in ENM for FM support. Only snmpv2 is supported for CCD

- Navigate to Provisioning > CLI in the ENM GUI.
- Prepare the Add-node script based on the node data explained in the Data collection section, using the following example add-node script. Save the script as ccd5a.txt.

Question1: Pls clarify if HPE Servers and CCD Supported on ENM and Which information is correct? To add in scope of work.

Question2: The HPE server notes indicate that the ENM Custom Adaptation (CA) for HPE is already installed on ENM. May please have more information, should I raise a support request to ENM team or open an internal request to enable the CA for this server? Basically how to get CA for ENM?

Question3: The CCD documentation indicates it uses SNMPv2, but I cannot find a way to manage or change the CCD IP addresses or community strings. Can these parameters be managed at runtime—like other CNFs designated as ‘managed nodes’?

### Comments

Comment by [Zhigang Han](#) [2025-10-08]

Hi team,

The fix is available and also Spyros has updated CPI. The ticket is closed.

Thanks,

BR/Zhigang

Comment by [Rajan Rajeshprasad Gupta](#) [2025-10-08]

Hello Spyros,

CPI document is much clear now.

FYI checked 2 updates and looks clear to me.

For more information on CCD configuration data, see Table 7

Parameter	Explanation	Value (ex.)
CloudInfrastructure	The cloud infrastructure MO name in ENM	CCD5A
CloudInfrastructureId	The ID of the cloud infrastructure MO when the instance is created	CCD5A
ciType	The cloud infrastructure type for the added node	CCD
clusterName	Unique element name	CCD5A
serverAddress	CCD ingress IP (dummy IP for ENM 25.1)	214.13.227.75
ipAddress	CCD control plane external IP	214.13.227.4
Port	Alertmanager service port	80

Table 7 - CCD Configuration Data

## Example

```
cmedit create CloudInfrastructure=CCD5A CloudInfrastructureId="CCD5A", ciType="CCD", clusterName="CCD5A", serverAddress="214.13.227.75" - ns=OSS_NE_DEF -v=1.0.0  
cmedit create CloudInfrastructure=CCD5A, CcdConnectivityInformation=1 CcdConnectivityInformationId="1", ipAddress="214.13.227.4", port="80" - ns=CCD_MED -v=1.0.0  
cmedit set CloudInfrastructure=CCD5A, FmAlarmSupervision=1 active=true
```

Comment by Spyros Loukopoulos (EXT) [2025-10-08]

Hi Rajan Rajeshprasad Gupta ,

I have updated the Central O&M User guide to align with UCC configuration for CCD.

[UCC - Central O&M User Guide.docx](#)

Please check chapter 2.2.2 and let me know of any additional comment.

The document should be available to next CPI production for UCC 1.2.

BR/Spyros

Comment by Rajan Rajeshprasad Gupta [2025-10-08]

Hello Bao and Spyros,

Thank you for clarification.

I have checked vz ucc environment and come up with below observations.

serverAddress: CCD Ingress IP and it is dummy.

ipAddress: CCD control plane external IP and It is used for getting alarm from CCD.

serverAddress extracted from CCD:

```
eccd@ucc-ccda:~> kubectl get svc -n ingress-nginx | grep ingress-nginx  
ingress-nginx   LoadBalancer   10.96.0.254   10.161.89.75   80:30187/TCP,443:31740/TCP   86d
```

ipAddress extracted from CCD:

```
eccd@ucc-ccda:~> ip a | grep ccd_oam 27: ccd_oam: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UNKNOWN group default qlen 1000  
inet 10.161.89.4/29 brd 10.161.89.7 scope global noprefixroute ccd_oam
```

prometheus-webhook-snmp-cm config verified

```
eccd@ucc-ccda:~> kubectl get cm prometheus-webhook-snmp-cm -n monitoring -o json | jq -r '.data["prometheus-webhook-snmp.conf"]'  
port: 9098
```

```
snmp_host: localhost
snmp_port: 23162
receiver_hosts: [10.161.112.27]
receiver_port: 162
snmp_community: public
snmp_retries: 5
snmp_timeout: 1
snmp_source_identifier: 10.161.89.4
snmp_user:
snmp_Engine:
snmp_authkey:
snmp_private_key:
snmp_auth_protocol:
snmp_priv_protocol:
trap_oid_prefix: 1.3.6.1.4.1.193.183.4
debug: false
heat_stack_name: ccda
host: "::"
cert: "/data/certs/tls.crt"
kev: "/data/certs/tls.kev"
```

So it means;

serverAddress: 10.161.89.75

ipAddress: 10.161.89.4

Trust above value are correctly fetched. In such case, We need to below things

1. To update CPI table to have serverAddress and ipAddress different value (Currently have same value)
2. To update description of serverAddress and ipAddress so user can clearly understand and fetch information.
3. To add CLIs as above so they can themself fetch and do validation to avoid issues.

Please let me know your views.

---

Comment by Bao Ren [ 2025-10-08 ]

Another thing I would like to highlight is that ENM only support one Node map to one IP address, so for CCD FM Integration with ENM, following IP must be configured as

ENM -> CCD: IP which used for ENM to get active alarm list from CCD:

curl -v <http://214.14.143.75/api/v1/alerts>

CCD-> ENM: IP which for SNMP trap source identifier of CCD send to ENM:

```
Data
=====
prometheus-webhook-snmp.conf:
-----
port: 9098
snmp_host: localhost
snmp_port: 23162
receiver_hosts: [10.237.5.147]
receiver_port: 162
snmp_community: public
snmp_retries: 5
snmp_timeout: 1
snmp_source_identifier: 214.14.143.75
snmp_user:
snmp_Engine:
snmp_authkey:
snmp_private_key:
snmp_auth_protocol:
snmp_priv_protocol:
trap_oid_prefix: 1.3.6.1.4.1.193.183.4
debug: false
heat_stack_name: ccda
host: ":"
```

---

Comment by Bao Ren [ 2025-10-08 ]

**Question3: The CCD documentation indicates it uses SNMPv2, but I cannot find a way to manage or change the CCD IP addresses or community strings. Can these designated as 'managed nodes'?**

Bao: All of Node's(CCD's) attributes(include IP) can be changed in ENM side. Here is the example to change CCD IP address:

```
>>> cmedit set CloudInfrastructure=CCD5B,CcdConnectivityInformation=1 ipAddress=214.13.227.7  
SUCCESS FDN : CloudInfrastructure=CCD5B,CcdConnectivityInformation=1  
  
1 instance(s) updated
```

**Question5: I see ingress Ip and Alermanager service ingress IP is same in the table(above). However, CLIs of ENM has complete different IP used in command(Is it alernaneger service IP?)**

serverAddress: This attribute represents the FQDN address of the Kube API server of the CCD instance. This is used for alarm correlation for CCD and CNF which on top of CC function, current it has NOT tested and verified in UCC(as ENM25.1 still be used in XFT3 lab).

I think you could ignore serverAddress setting for now, as it not impact standard CCD FM integration with ENM.

For more detail of this new feature, pls refer to official Tutorial: Associating CNF withCloudInfrastruture as attached.

Comment by [Spyros Loukopoulos \(EXT\)](#) [ 2025-10-07 ]

Hi Rajan Rajeshprasad Gupta ,

**Question1: Pls clarify if HPE Servers and CCD Supported on ENM and Which information is correct? To add in scope of work.**

ENM 25.1 supports CCD FM with standard functionality.

HPE FM/PM is supported only via SD-CA addon, designed for the specific ENM version.

**Question2: The HPE server notes indicate that the ENM Custom Adaptation (CA) for HPE is already installed on ENM. May please have more information, should request to enable the CA for this server? Basically how to get CA for ENM?**

Please see the Central O&M References for HPE CA addon for ordering, installation and specifications:

1. 1531-CXF1010466 Uen B: Customized FM/PM Adaptation Installation Instructions
2. 15517-CXP 906 2207 Uen B: HPILO Customized Adaptation Function Specification

UCC is not responsible for packaging, ordering and installation for the HPE SD-CA solution.

UCC has verified the solution.

For more information about ordering and installation, please contact Linn ([linn.montan.rydell@ericsson.com](mailto:linn.montan.rydell@ericsson.com))

**Question3: The CCD documentation indicates it uses SNMPv2, but I cannot find a way to manage or change the CCD IP addresses or community strings. Can these designated as 'managed nodes'?**

IP address attribute is immutable. The element should be deleted first and added again with new IP.

[Bao Ren](#) : Please comment if it is possible to update on runtime.

**Q4: CCD addition in ENM requires ccd-ingress ip address? Is this "ingress-nginx" service IP? I assume yes.**

**Question5: I see ingress Ip and Alermanager service ingress IP is same in the table(above). However, CLIs of ENM has complete different IP used in command(Is it alernaneger service IP?)**

Please refer to ENM tutorial for the description:

[https://cpistore.internal.ericsson.com/elex?LI=EN/LZN7030220R2EB&FN=1\\_1553-CNA4032979Uen.DS.html&HT=lxk1734276097349&DT=ENM+CLI](https://cpistore.internal.ericsson.com/elex?LI=EN/LZN7030220R2EB&FN=1_1553-CNA4032979Uen.DS.html&HT=lxk1734276097349&DT=ENM+CLI)

This part is confusing to me as well. It seems that the description is not consistent with the implementation. The working combination is according the example in the Centr.

serverAddress: CCD Ingress IP (Can be found in the LLD external IP Plan)

ipAddress: CCD control plane external IP

The alert manager IP address however is the same as the serverAddress and that is why I believe the ENM tutorial is confusing:

```
eccd@ucc-ccda:~> k get ingress -n monitoring  
NAME          CLASS    HOSTS          ADDRESS      PORTS      AGE  
eric-pm-alertmanager  nginx   alertmanager-ccd-stcucc5a.sero.ericsson.se  172.16.0.18  80, 443  17d  
eric-victoria-metrics-cluster-vmselect  nginx   vmselect-ccd-stcucc5a.sero.ericsson.se  172.16.0.18  80, 443  17d  
eccd@ucc-ccda:~> nslookup alertmanager-ccd-stcucc5a.sero.ericsson.se  
Server: 10.96.0.10#53  
Address: 10.96.0.10#53  
Name: alertmanager-ccd-stcucc5a.sero.ericsson.se  
Address: 214.13.227.75  
;; Got recursion not available from 10.96.0.10, trying next server
```

[Bao Ren](#) : Please add your comments.

BR/Spyros

Comment by [Rajan Rajeshprasad Gupta](#) [ 2025-10-06 ]

Hello Spyros,

Allow to ask 2 more additional questions which are not clear for CPI.

Q4: CCD addition in ENM requires ccd-ingress ip address? Is this "ingress-nginx" service IP? I assume yes.

```
eccd@ucc-ccdb:~> kubectl get svc -n ingress-nginx | grep ingress-nginx
ingress-nginx           LoadBalancer   10.96.0.254   10.161.89.106  80:32169/TCP,443:30550/TCP   84d
```

Parameter	Explanation	Value (ex.)
CloudInfrastructure	The cloud infrastructure MO name in ENM	CCD5A
CloudInfrastructureId	The ID of the cloud infrastructure MO when the instance is created	CCD5A
ciType	The cloud infrastructure type for the added node	CCD
clusterName	Unique element name	CCD5A
serverAddress	CCD ingress IP	214.13.227.75
ipAddress	Alertmanager service ingress IP	214.13.227.75
port	Alertmanager service port	80

Question5: I see ingress Ip and Alertmanager service ingress IP is same in the table(above). However, CLIs of ENM has complete different IP used in command(Is it typo?). So IP?

See below in CPI.

#### 2.2.2.2 CCD ENM CLI

CCD is added as CloudInfraStructure node in ENM for FM support. Only snmpv2 is supported for CCD

- Navigate to Provisioning > CLI in the ENM GUI.
- Prepare the Add-node script based on the node data explained in the Data collection section, using the following example add-node script. Save the file as ccd5a.txt.

Example

```
cmedit create CloudInfrastructure=CCD5A CloudInfrastructureId="CCD5A", ciType="CCD", clusterName="CCD5A"
serverAddress="214.13.227.75" -ns=OSS_NE_DEF -v=1.0.0
    cmedit create CloudInfrastructure=CCD5A,CcdConnectivityInformation=1 CcdConnectivityInformationId="1"
    ipAddress="214.13.227.4", port="80" -ns=CCD_MED -v=1.0.0
        cmedit set CloudInfrastructure=CCD5A, FmAlarmSupervision=1 active=true
```

- Drag and drop the file into ENM CLI and execute the command as follows:

Comment by [Zhigang Han](#) [2025-10-06]

Hi Rajan,

We have verified and tested ENM 25.1 with no CA. PLM believes we only support fully ENM 25.1 integration at this point. Here is the release note of UCC 1.1:

# 4

# Verification Information

## 4.1

## Compatibility Information

Matrix to show the compatibility between different products and versions.

Product From Name	Product From Version	Product To Name	Product To Version	Compatibility
ENM	25.1	UCC	1.1	Compliant
cNeLS offline	1.12	UCC	1.1	Compliant

I have assigned the ticket to XFT3 team. The design will answer your questions quickly.

Thanks,

BR/Zhigang

[UCC\_PLM-276] inactive KPIs in UCC CNOM Created: 2025-08-29 Updated: 2025-10-02 Resolved: 2025-10-02

Status:	Cancelled
Project:	UCC_PLM
Component/s:	None
Affects Version/s:	None
Fix Version/s:	None

Type:	Story	Priority:	Low
Reporter:	AURELIA DINULESCU	Assignee:	Christos Delis (EXT)
Resolution:	Cancelled	Votes:	0
Labels:	UCC-CNOM		
Remaining Estimate:	0h		
Time Spent:	2h		
Original Estimate:	Not Specified		

Requirement Status:	UCC Appliance 0.2.1 - UNCOVERED
Team/s:	UCC_XFT3

### Description

CNOM has inactive KPIs for UCC. Customer has requested to activate them; however, they are not supported by UCC. Is it possible to delete them so they are not visible anymore?

## Comments

Comment by [Zhigang Han](#) [ 2025-10-02 ]

hi AURELIA DINULESCU,

We had the answer from the design side. Unfortunately cnom doesnot support the request to deactivate some KPI. We will reject the ticket.

Thanks,

BR/Zhigang

Comment by [Christos Delis \(EXT\)](#) [ 2025-10-02 ]

Hello [Zhigang Han](#),

Excuse me but i missed your comment.

Yes, we could close this ticket.

BRs,

Christos

Comment by [Zhigang Han](#) [ 2025-09-26 ]

Hi Christos,

If it is not possible to disable them from CNOM GUI, should we reject the ticket?

Thanks,

BR/Zhigang

Comment by [Christos Delis \(EXT\)](#) [ 2025-09-18 ]

Hello,

No is not applicable to disable them from CNOM GUI.

BRs,

Christos

Comment by [Zhigang Han](#) [ 2025-09-08 ]

Hi Soner,

This is not a bug related to CNOM but for PLM it is an improvement. We do not support some KPIs from CNOM GUI, however they are visible from CNOM GUI. Could we deactivate these KPIs from CNOM GUI.

Thanks,

BR/Zhigang

[UCC\_PLM-275] UCC MANA: UCA Provisioning fail with <Cai3gFault:reasonText>External error.</Cai3gFault:reasonText> Created: 2025-08-22 Updated: 2025-09-02 Resolved: 2025-09-02

2025-09-02

Status:	Done
Project:	<a href="#">UCC_PLM</a>
Component/s:	None
Affects Version/s:	<a href="#">UCC Appliance 1.1.0</a>
Fix Version/s:	None

Type:	Bug	Priority:	Medium
Reporter:	<a href="#">Rajan Rajeshprasad Gupta</a>	Assignee:	<a href="#">Alvaro Martin</a>
Resolution:	Closed	Votes:	0
Labels:	CNF_TRs		
Remaining Estimate:	Not Specified		
Time Spent:	Not Specified		
Original Estimate:	Not Specified		

<b>Attachments:</b>	CCDM WAs for Continuous Delivery.docx.pdf          image-2025-08-23-01-11-31-257.png          image-2025-08-23-01-15-58-194.png          LOGFILE2.txt          logs_ccdm_2025-08-25-08-21-09.tgz          logs_uca_2025-08-25-08-17-29.tgz          Provision-Interface>Status.txt          scheme_1_sub_2.xml
<b>Team/s:</b>	UCC_XFT2
<b>Found in Build:</b>	UCC 1.1
<b>Requirement Status:</b>	UCC Appliance 0.2.1 - UNCOVERED

#### Description

Hello,

Team is trying to provision more UEs in CKT2.

Note: Earlier UCA Provisioning was working.

However, New provisioning fails now, UCA based subscriber Provisioning fails as UCA logs indicate External error

```
</cai3:Create>","<?xml version="1.0"" encoding=""ISO-8859-1"" standalone="yes"?>
<SOAP-ENV:Fault xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/">
  <faultcode>SOAP-ENV:Server</faultcode>
  <faultstring>This is a server fault</faultstring>
  <detail>
    <Cai3gFault:Cai3gFault xmlns="http://schemas.ericsson.com/cai3g1.2/" xmlns:Cai3gFault="http://schemas.ericsson.com/cai3g1.2/">          <Cai3gFault:faultrole>MF</Cai3gFault:faultrole>
    <Cai3gFault:reasonText>External error.</Cai3gFault:reasonText>          </Cai3gFault:faultreason>
    <Cai3gFault:faultrole>MF</Cai3gFault:faultrole>
```

UCA GUI:

← → ⌂ Not secure https://oam.uca-ckit2a.deac.ericsson.se/batchhandler/#BatchHandlerWeb

## UCA

Home

# Batch Handler

→ Filter Create batch job Manage batch files

## Batch Jobs (3 of 1000) ?

New Batch Jobs (0) ▶ Run | 🗑 Delete

Select all Sort by: Date ▾

No New Jobs

Scheduled Batch Jobs (0) ▶ Reschedule | 🗑 Cancel

Select all Sort by: Date ▾

No Scheduled Jobs

Running Batch Jobs (0) ||

Currently using 0/200 sessions

Select all Sort by: Progr ▾

No Running Jobs

Paused Batch Jobs (0) ||

Select all Sort by: Progr ▾

No Paused Jobs

<https://oam.uca-ckit2a.deac.ericsson.se/batchhandler/#BatchHandlerWeb>

Attached xml file. [scheme\\_1\\_sub\\_2.xml](#)

Attached complete error logs for UCA. [LOG\\_FILE2.txt](#)

From CPI, It says, error is for communication failure.

Fault Code	Source	Fault Reason	Comment
1001	Client	Invalid SessionId	Log in before sending any CAI3G provisioning requests
1003	Client	SessionId Syntax Error	The SessionId is not a numeric string.
2001	Client	Invalid managed object type	Ensure the MoType in the request is correct. If the problems are not solved, ensure that required Dynamic Activation components and licenses are correctly installed
2002	Client	Invalid managed object id	Ensure the MoId in the request is correct. If the problems are not solved, ensure that required Dynamic Activation components and licenses are correctly installed
2003	Client	Unsupported data type	Ensure that the Namespace in the request is correct. If the problems are not solved, ensure that required Dynamic Activation components and licenses are correctly installed
2999	Client	Request error that cannot be put into above categories	Call for support
3001	Client	Operation is not allowed because of the prerequisites are not fulfilled	Ensure that the user is allowed to perform this operation and the operation is allowed for the Mo
3002	Client	Try to access an non-existent MO instance	Ensure the MOId in the request is correct
3010	Client	Invalid MO Attribute	The value of input attribute violates XML schema definition.
3011	Client	Insufficient MO Attributes	The value of input attribute violates XML schema definition.
3012	Client	Insufficient Parameter	There are some mandatory parameters missing in the request.
3013	Client	There are invalid parameters in the request	Refer to document <a href="#">Generic CAI3G Interface 1.2</a> for correct syntax of SessionId, MoType, Manager and so on
3014	Client	Logon Failure, invalid username, invalid password	Contact Dynamic Activation administrator for correct UserId and password
3999	Client	Client error that cannot be put into above categories	Call for support
4001	Server	CAI3GAgent cannot support the operation in current request	Refer to WSDL of the CAI3G Web Service provided by the CAI3G server for mandatory parameters of CAI3G request
4004	Server	A temporary error caused by short of computing resource at CAI3GAgent	Try later. If it happens frequently, check the downstream Network Element status
4005	Server	A fatal error in CAI3GAgent when processing the request	Call for support
4006	Server	An error caused outside the CAI3GAgent causes the end of the processing request	Check the downstream Network Element status
4010	Server	Over limitation of maximum numbers of CAI3G sessions	Reduce traffic, try later, or contact your local support organization to increase the maximum number of CAI3G sessions.
4999	Server	Server error that cannot be put into any above categories	Call for support

Provisioning NE looks Ok, except mapi-1 status changed to up=false.

```
* Connection #0 to host oam.uca-ckit2a.deac.ericsson.se left intact
[
{
  "name": "hss_fe1",
  "protocolType": "ProvisioningNotification",
  "resourceId": "3",
  "active": true,
  "up": true
},
{
  "name": "ldap-1",
  "protocolType": "LDAP",
  "resourceId": "2",
  "active": true,
  "up": true
},
{
  "name": "mapi-1",
  "protocolType": "M-API",
  "resourceId": "1",
  "active": true,
  "up": false
}
```

[Provision-Interface-Status.txt](#)

Question: What additional checks should be performed on mapi-1, and what steps can be taken to recover provisioning?

#### Comments

Comment by [Zhigang Han](#) [2025-09-02]

Hi Rajan and Alvaro,

Now we have updated the installation guide and we close the ticket.

Thanks,

BR/Zhigang

Comment by [Alvaro Martin](#) [ 2025-09-01 ]

Hi,

A new Installation Guide version is being generated with the updates.

This is the preliminary version with the data updated -> [Ericsson Ultra Compact Core - Appliance - Software Installation Guide - new.docx](#)

The new version will be published and notified.

Updates:

- Added new important note in subscriber provisioning chapter (15) referring to this known issue
- Added new known issue in chapter (chapter 23.10)
- Added new reference (Ref 14) with the CCDM 1.x WAs for continuous delivery

regards/Álvaro

Comment by [Zhigang Han](#) [ 2025-08-28 ]

hi Alvaro,

Could you let us know when UCC 1.1 installation guide has been updated and we have released a new CPI?

[Rajan Rajeshprasad Gupta](#) I will reopen the ticket at this point.

Thanks,

Zhigang

Comment by [Rajan Rajeshprasad Gupta](#) [ 2025-08-28 ]

Hello [Zhigang Han](#)

We should not close ticket unless CPI is updated. This is important for tracking. We don't know when CPI will be updated.

Once CPI is updated, you can go ahead and close the ticket.

Please be noted: Not everyone using UCC, has access to UCC PLM ticket Jira queue.

Comment by [Zhigang Han](#) [ 2025-08-28 ]

Hi Rajan,

We will update the installation guide and release a new CPI for UCC 1.1. I will close the ticket.

Thanks,

BR/Zhigang

Comment by [Zhigang Han](#) [ 2025-08-26 ]

Hi Rajan,

Could we document the workaround in this ticket instead of updating CPI II then close the ticket??

Thanks,

BR/Zhigang

Comment by [Rajan Rajeshprasad Gupta](#) [ 2025-08-26 ]

Hello Sam,

Ticket can be closed after UCC 1.1 installation guide and release note are updated.

This serves as an alternative source of information regarding a known issue, which the team can use until they update to the latest release. The severity of the issue or how CU feedback is uncertain, but having some information is preferable to having none.

Comment by [Zhigang Han](#) [ 2025-08-26 ]

Hi Reema and Alex,

The fix will be available in CCDM 1.14 which UCC 1.2 has CCDM 1.14.

Rajan Rajeshprasad Gupta , Could we close the ticket because the fix will be available in UCC 1.2?

According to Alex, we will update UCC 1.1 installation guide and release note to add this known issue.

Thanks,

BR/Zhigang

Comment by Alexander Malikov [ 2025-08-26 ]

Hello,

We are not going to deliver any EP for UCC 1.1.

Reema Sidhwani, if it's a known issue and it will be fixed in UCC 1.2 than we will recommend to go with it. We just need to update Installation guide and Release note to add this known issue.

Thank you.

Comment by Rajan Rajeshprasad Gupta [ 2025-08-25 ]

attached CCDM WAs

[CCDM WAs for Continuous Delivery.docx.pdf](#)

section 7.1.1 (IB39496) EDA2 disconnected

Comment by Zhigang Han [ 2025-08-25 ]

hi Rajan,

Okay I assigned the ticket to XFT2 team and let us wait for the analysis from design!

Alexander Malikov the issue looks like a bug from ccdm.

Thanks,

BR/Zhigang

Comment by Rajan Rajeshprasad Gupta [ 2025-08-25 ]

Got feedback from colleagues, This is akka bug in CCDM 1.13.

Please send request to design to review and release for potential EP.

"

In one of my customers we have observed a similar problem between ccdm and eda2. We are running ccdm with 1.13 EP1/EP3 and according to a ticket we raised, the issue seems to be related to 3rd-party software in CCDM 1.13 for "akka" that is unreliable and will be removed completely in CCDM 1.14 - according to the ticket answer.

Our temporary WA is to restart eric-act-mapi-provisioning pods in CCDM where we observed java exceptions.

So if you have the same issue you should observe some java exceptions in eric-act-mapi-provisioning one or more pods in ccdm."

Comment by Zhigang Han [ 2025-08-25 ]

Hi Rajan,

Please update the status of mapi interface from UCA side after 3 days. If the mapi is down again, we are sure it is related to certificate at least. Right now we could see the issue from CCDM side but not from UCA side.

Thanks,

BR/Zhigang

Comment by Rajan Rajeshprasad Gupta [ 2025-08-25 ]

Thank you Sam.

as you observed in pod logs : eric-act-mapi-provisioning-76cf96ddf7-v4jlw\_provisioning

we see certificate expired ;

```
2025-07-30T11:53:15.128-05:00 [main] INFO [com.ericsson.activation.certificate.action.scheduler.CertificateActionScheduler] Schedule alarm raising for: [eric-act-mapi-provisioning-metrics], 3 days before expiry, with severity [Critical] at time: [2035-07-28T04:49:07Z]
```

We are not sure why CCDM complaints for certificate expiry.

as CA has 10 year validity;

```
ucc@ckit2-sfs:~/certificates$ openssl x509 -in ca.pem -dates -noout
notBefore=Jul 29 19:49:48 2025 GMT
notAfter=Jul 27 19:49:48 2035 GMT
ucc@ckit2-sfs:~/certificates$
```

Issue is temporary fixed by restarting ccdm pod : eric-act-mapi-provisioning, which gives again 3 more days for mapi expiry;

```
eccd@ucc-ccdb:~> kubectl get pod -n ccdm | grep eric-act-map
eric-act-mapi-provisioning-9fd78578b-gbbk5          2/2     Running     0      79s
eccc@ucc-ccdb:~> kubectl logs eric-act-mapi-provisioning-9fd78578b-gbbk5 -n ccdm --follow | grep -i critical
2025-08-25T10:28:04.318-05:00 [main] INFO [com.ericsson.activation.certificate.action.scheduler.CertificateActionScheduler] Schedule alarm raising for: [eric-act-mapi-provisioning-kafkaproclog], 3 days before expiry, with severity [Critical] at time: [2035-07-28T04:49:14Z]
2025-08-25T10:28:04.319-05:00 [main] INFO [com.ericsson.activation.certificate.action.scheduler.CertificateActionScheduler] Schedule alarm raising for: [eric-act-mapi-provisioning-alarmhandlerrestfi], 3 days before expiry, with severity [Critical] at time: [2035-07-28T04:49:27Z]
2025-08-25T10:28:04.320-05:00 [main] INFO [com.ericsson.activation.certificate.action.scheduler.CertificateActionScheduler] Schedule alarm raising for: [eric-act-mapi-provisioning-zookeeper], 3 days before expiry, with severity [Critical] at time: [2035-07-28T04:49:15Z]
2025-08-25T10:28:04.320-05:00 [main] INFO [com.ericsson.activation.certificate.action.scheduler.CertificateActionScheduler] Schedule alarm raising for: [eric-act-mapi-provisioning-oauth], 3 days before expiry, with severity [Critical] at time: [2035-07-28T04:49:15Z]
2025-08-25T10:28:04.321-05:00 [main] INFO [com.ericsson.activation.certificate.action.scheduler.CertificateActionScheduler] Schedule alarm raising for: [eric-act-mapi-provisioning-metrics], 3 days before expiry, with severity [Critical] at time: [2035-07-28T04:49:15Z]
2025-08-25T10:28:04.321-05:00 [main] INFO [com.ericsson.activation.certificate.action.scheduler.CertificateActionScheduler] Schedule alarm raising for: [eric-act-mapi-provisioning-logging], 3 days before expiry, with severity [Critical] at time: [2035-07-28T04:49:15Z]
```

we need to identify reason for such behaviour for ccdm.

license looks ok:

```
eccc@ucc-ccdb:~> kubectl exec -n ccdm deploy/eric-lm-combined-server-license-consumer-handler -c eric-lm-license-consumer-handler - /opt/LicenseConsumerHandler/listLicenses.sh CCDM | jq
{
  "operationalStatusInfo": {
    "operationalMode": "NORMAL"
  }

  "licensesInfo": [
    {
      "license": {
        "keyId": "FAT1024213/6", "type": "CAPACITY_PEAK"
      }
    }

    "licenseStatus": "VALID",
    "capacityInfo": {
      "isLimited": true, "licensedCapacity": 50, "unusedCapacity": 50
    }
  },
  {
    "license": {
      "keyId": "FAT1024213/9", "type": "CAPACITY_PEAK"
    }
  }

    "licenseStatus": "VALID",
    "capacityInfo": {
      "isLimited": true, "licensedCapacity": 50, "unusedCapacity": 50
    }
  },
  {
    "license": {
      "keyId": "FAT1024213/1", "type": "FEATURE"
    }
  }

    "licenseStatus": "VALID"
  },
}
```

```
{
  "license": {
    "keyId": "FAT1024200/51", "type": "CAPACITY_PEAK"
  },
  "licenseStatus": "VALID",
  "capacityInfo": {
    "isLimited": true, "licensedCapacity": 50, "unusedCapacity": 50
  }
}
}

eccd@ucc-ccdb:~>
```

Comment by Rajan Rajeshprasad Gupta [ 2025-08-25 ]

attached ADP logs for ccdm.logs\_ccdm\_2025-08-25-08-21-09.tgz

Comment by Zhigang Han [ 2025-08-25 ]

hi Rajan,

here is what we need to do:

from EDA we need to check eric-act-activation-engine ==> eric-act-activation-engine, it is responsible from connecting to CCDM/MAPI

from CCDM we need to check eric-act-mapi-provisioning log ==> providing mapi api service

We need the log to check the issue.

Thanks,

BR/Zhigang

Comment by Rajan Rajeshprasad Gupta [ 2025-08-25 ]

attached ADP logs

[logs\\_uca\\_2025-08-25-08-17-29.tgz](#)

## [UCC\_PLM-272] Duke-POC-4G data call failed with error System Failure (72) Created: 2025-08-20 Updated: 2025-08-20 Resolved: 2025-08-20

Status:	Done
Project:	UCC_PLM
Component/s:	None
Affects Version/s:	UCC Appliance 1.1.0
Fix Version/s:	None

Type:	Bug	Priority:	Medium
Reporter:	ETTAVENI RAJU	Assignee:	Zhigang Han
Resolution:	Closed	Votes:	0
Labels:	None		
Remaining Estimate:	Not Specified		
Time Spent:	Not Specified		
Original Estimate:	Not Specified		

Attachments:	<a href="#">B20250819.114851.316-0500-PGW.ccda.appliance_99900000001_99900700000001_IMSI.pcap</a>	<a href="#">eric-pc-sm-smf-pgw-session-5d68fb8c6-hjgmm-19-08-2025.zip</a>	<a href="#">PCX_config.txt</a>
Issue Links:	<b>Association</b>		
	Associates with	<a href="#">UCC_XFT-1602</a>	SD:UCC1.1 RC1: PGW-C reject 4G call w...
Team/s:	Done		
Found in Build:	1.1		
Requirement Status:	UCC Appliance 0.2.1 - UNCOVERED		

## Description

Hi Team,

It has been observed that 4G Data Session failed with System failure error (72). Issue has been fixed after adding "sbi udm-get-enabled-4g" (it also worked after bypassing N7). Kindly suggest if this cli needs to be enabled by default for LTE subscribers with PCF-enabled-4g? Attaching the logs and traces for the same.

## Comments

Comment by [ETTAVENI RAJU](#) [ 2025-08-20 ]

Thank You Adrian and Zhigang. Please proceed and close the ticket.

Regards,

Raju

Comment by [Zhigang Han](#) [ 2025-08-20 ]

hi Raju,

Could you close the ticket with the fix available in UCC 1.2?

Thanks,

BR/Zhigang

Comment by [Adrian-Bogdan Iliescu](#) [ 2025-08-20 ]

hi,

we'll have this config by default in UCC1.2

apn internet sbi **udm-get-enabled-4g**

## Thank you

Comment by [ETTAVENI RAJU](#) [ 2025-08-20 ]

We have used the default configuration. attaching the configuration FYR.

Comment by [Zhigang Han](#) [ 2025-08-20 ]

Hi Raju,

can you do test ?

remove the workarround with udm-get-enabled-4g

and enable this feature: n7-preliminary-features

one more question: what did you had configured in SMF at:running-config epg pgw snssai and show running-config epg pgw network-slice?

you are not using a roamer imsi for this test, right ? you have configured everyware mcc 999 and mnc 007 ?

Thanks,

BR/Zhigang

[UCC\_PLM-268] [UCC MANA: No easy way to know ucc release version](#) Created: 2025-08-14 Updated: 2025-08-18 Resolved: 2025-08-18

Status:	Rejected
Project:	<a href="#">UCC_PLM</a>
Component/s:	None
Affects Version/s:	<a href="#">UCC Appliance 1.1.0</a>
Fix Version/s:	None

Type:	Bug	Priority:	Medium
-------	-----	-----------	--------

<b>Reporter:</b>	Rajan Rajeshprasad Gupta	<b>Assignee:</b>	Zhigang Han
<b>Resolution:</b>	Rejected	<b>Votes:</b>	0
<b>Labels:</b>	None		
<b>Remaining Estimate:</b>	Not Specified		
<b>Time Spent:</b>	Not Specified		
<b>Original Estimate:</b>	Not Specified		

<b>Team/s:</b>	UCC_PLM
<b>Found in Build:</b>	UCC 1.1
<b>Requirement Status:</b>	UCC Appliance 0.2.1 - UNCOVERED

#### Description

Hello,  
as we have different ucc releases across different customers.

Some are on UCC 1.0 , UCC 1.0 CP1 and Some on UCC 1.1

eg.

UCC 1.0 (Telf )

UCC 1.0 CP1( Reaytheon, BAH, Tmo etc)

UCC 1.1 ( Vz, Tmo, Duke etc)

There is no easy way to get release information though CLI or GUI directly from cnat/sfs/ccd.

There is need to do reverse engineering to get cnf version and check mapped UCC release.

Q1: Please let us know easy way to find UCC release if available?

Q2: If answer is no, Please introduce as earliest way to get information?

#### Comments

Comment by [Zhigang Han](#) [ 2025-08-18 ]

Hi Rajan,

As we discussed from the team, we will reject the ticket at this point. Please open an improvement ticket from your side.

Thanks,

BR/Zhigang

Comment by [Zhigang Han](#) [ 2025-08-18 ]

Hi Rajan,

Unfortunately, we have no information for CPI UCC LCM at this point. At this point, you could map ccd version into UCC release version until we officially release UCC LCM information. Each UCC release has the unique CCD version at this point.

Thanks,

BR/Zhigang

Comment by [Rajan Rajeshprasad Gupta](#) [ 2025-08-16 ]

Hello Sam,

Thank you for feedback.

Question is for UCC release and not about CCD release/CNF release. Feedback for Q1 is provided for CCD release, which again remains to do reverse engineering to map UCC release.

As we have nothing about LCM GUI in CPI, Do we have internal demo/link to see UCC release information on LCM GUI? This can help to feedback to colleagues and ask to wait for LCM release to cover information.

Comment by [Zhigang Han](#) [ 2025-08-15 ]

Hi Rajan,

Q1: Please let us know easy way to find UCC release if available?

Q2: If answer is no, Please introduce as earliest way to get information?

Here are the answers for two questions:

A1: if you know ccd version in UCC release, you could run the command on CCD server

```
cat /etc/eccd/eccd_image_version.ini
```

```
eccd@ucc-ccda:~> cat /etc/eccd/eccd_image_version.ini
```

```
IMAGE_RELEASE=2.31.1
```

```
IMAGE_COMMIT=000089
```

```
IMAGE_GIT_HASH=0ca5103e
```

```
IMAGE_BUILD_NUMBER=13068eccd@ucc-ccda:~>
```

however you still need to map ccd version into UCC release

A2: LCM GUI does have the information

Thanks,

BR/Zhigang

#### [UCC\_PLM-267] UCC RTX[ UCC 1.0 ] N4 link down between both SMF and UPF of Server-B Created: 2025-08-14 Updated: 2025-09-09 Resolved: 2025-09-09

Status:	Rejected
Project:	<a href="#">UCC_PLM</a>
Component/s:	None
Affects Version/s:	<a href="#">UCC Appliance 1.0.0</a>
Fix Version/s:	None

Type:	Bug	Priority:	Medium
Reporter:	<a href="#">Rajan Rajeshprasad Gupta</a>	Assignee:	<a href="#">Zhigang Han</a>
Resolution:	Rejected	Votes:	0
Labels:	None		
Remaining Estimate:	Not Specified		
Time Spent:	Not Specified		
Original Estimate:	Not Specified		

Team/s:	<a href="#">UCC_PLM</a>
Found in Build:	UCC 1.0
Requirement Status:	UCC Appliance 0.2.1 - UNCOVERED

#### Description

Hello,

After receiving complaint for UEs not working for Raytheon UCC, We started checking healthcheck and notice, N4 link between SMF and UPF of Server-B is down.

system_admin@pcx-ccdb#epg pgw interface sx path-status				
Node Id	Peer IP	Local IP	Interface	Status
Recovery Time Stamp				
172.16.2.6	172.16.2.6	172.16.3.4	Sxb	Active
2025-06-23 16:31:00				
-	172.16.3.6	172.16.3.4	Sxb	Initializing
0000-00-00 00:00:00				

While looking into alarms, There are lot of alarms in PCG:

```
system_admin@pcx-ccdb#show alarm
WorkloadCpuUsageThresholdReached
    active-severity      Minor
    service-name        eric-pm-bulk-reporter
    event-type          ProcessingErrorAlarm
    expires             24
    source              /sys:system/x/workload-type[name=StatefulSet]/workload-name[name=eric-data-object-storage-mn]/container[name=eric-data-object-
storage-mn]
        specific-problem   Workload CPU Usage Threshold Reached
        probable-cause     207
        major-type         193
        minor-type         13041714
        last-event-time    2025-08-14T04:48:30.000470 EDT
        additional-text    The CPU resource usage threshold is reached for a workload.WorkloadCpuUsageThresholdReached
    active-severity      Minor
    service-name        eric-pm-bulk-reporter
    event-type          ProcessingErrorAlarm
    expires             24
    source              /sys:system/x/workload-type[name=Deployment]/workload-name[name=eric-data-sftp-server]/container[name=eric-data-sftp-server]
        specific-problem   Workload CPU Usage Threshold Reached
        probable-cause     207
        major-type         193
        minor-type         13041714
```

I tried to recovered N4 link for UCC-Server-B but realised that, link is broken between "UCC-Server-B" and R6K Router- Breakout port 1/32 [ native port: 1/25      breakout port: 1/29, 1/30, 1/31, 1/32] and 1/36 [ native port: 1/26      breakout port: 1/33, 1/34, 1/35, 1/36]

We have 2 breakout ports for redundancy and unfortunately both of them looks down.

I tried to do shut/no shut on router port but link didn't came up

[local]router6675#show port 1/32 detail
etherent 1/32 state is Down
Description : ccd-b sriov
Port circuit : 1/32:511:63:31/1/0/88
Link state : Down
Last link state change : Jan 1 00:00:00.000
Line state : Down
Admin state : Up
License priority : 6
License Activated : Yes
Port Type : 25ge
Link Dampening : disabled
Undampened line state : Down
Dampening Count : 0
Encapsulation : dot1q
MTU size : 1500 Bytes
Storm control mode : off
Evpn MH ES Setting : off
Forward error correction : cl74-fc-fec
FEC state : cl74-fc-fec
NAS-Port-Type : none
NAS-Port-Id : none
MAC address : 1c:90:be:88:f0:20
Optical Transport : None
Media type : 100GBase-CR4
Flow control : off
Speed : 25 Gbps
Duplex mode : full
Clock-Source : local

Link Length Supported	: 3 meters
Loopback	: off
SFP+ Transceiver Status	
Additional Features	: None
Diag Monitor	: NO
Port Alarms	: Link down
Link-delay-time	: 0
Last line state down	: Jun 23 20:38:15.262
Trigger faults	: LinkDown

[local]router6675#show port 1/36 detail	
ethernet 1/36 state is Down	
Description	: ccd-b sriov
Port circuit	: 1/36:511:63:31/1/0/158
Link state	: Down
Last link state change	: Jan 1 00:00:00.000
Line state	: Down
Admin state	: Up
License priority	: 6
License Activated	: Yes
Port Type	: 25ge
Link Dampening	: disabled
Undampened line state	: Down
Dampening Count	: 0
Encapsulation	: dot1q
MTU size	: 1500 Bytes
Storm control mode	: off
Evpn MH ES Setting	: off
Forward error correction	: cl74-fc-fec
FEC state	: cl74-fc-fec
NAS-Port-Type	: none
NAS-Port-Id	: none
MAC address	: 1c:90:be:88:f0:24
Optical Transport	: None
Media type	: 100GBase-CR4
Flow control	: off
Speed	: 25 Gbps
Duplex mode	: full
Clock-Source	: local
Link Length Supported	: 3 meters
Loopback	: off
SFP+ Transceiver Status	
Additional Features	: None
Diag Monitor	: NO
Port Alarms	: Link down
Link-delay-time	: 0
Last line state down	: Jun 23 20:38:20.172
Trigger faults	: LinkDown

Question1: Is there a way to confirm from router if connection failed due to loose cable / faulty sfp / due to physical cable itself?

Question2: Can we do anything to recover port from router?

FYI, I requested customer to check loose cable/ physical cable and send picture of LED light to know more.

#### Comments

Comment by [Zhigang Han](#) [ 2025-09-09 ]

Hi Rajan,

We will reject the ticket due to the issue related to hardware and mistakes from customer side.

Thanks,

BR/Zhigang

Comment by [Rajan Rajeshprasad Gupta](#) [ 2025-09-09 ]

Hello Sam, This is fixed. Please close this ticket.

During joint troubleshooting:

ServerB: The cabling was re-verified and corrected. During the UPS setup, the customer's engineer accidentally changed the cabling while trying to prevent power outages from a power failure. We figured out with help of customer and fixed it.

As router ports are connected on wrong slot, on router port reflect as "up" however no arp/traffic was coming as connection was wrong.

Comment by [Zhigang Han](#) [ 2025-08-19 ]

Hi Rajan,

Have you tried to restart some pods under ep5g? or after we fixed router issue, we could perform the whole server B reboot?

Thanks,

BR/Zhigang

Comment by [Rajan Rajeshprasad Gupta](#) [ 2025-08-19 ]

Hello Sam,

Physical lose cabling is recovered by Raytheon team.

Now ports are up.

However, Still N4 is down as DP pod ips are undiscovered by L2. Please feedback if you have seen such problem?

[sig]router6675#show port

Port	Type	State
1/1	ethernet	Up
1/2	ethernet	Up
1/3	ethernet	Up
1/4	ethernet	Up
1/5	ethernet	Up
1/11	ethernet	Up
1/12	ethernet	Up
1/20	ethernet	Up
1/21	ethernet	Down
1/22	ethernet	Down
1/23	ethernet	Down
1/24	ethernet	Up
1/29	ethernet	Up
1/30	ethernet	Up
1/31	ethernet	Up
1/32	ethernet	Up
1/33	ethernet	Up
1/34	ethernet	Up
1/35	ethernet	Up
1/36	ethernet	Up

```
[sig]router6675#show arp
Total number of arp entries in cache: 12
Resolved entry : 12
Incomplete entry : 0

Host      Hardware address   Ttl   Type Circuit
172.16.0.1 1c:90:be:88:f0:00 - ARPA bvi-ecfe-sig vlan-id 1104
172.16.0.2 06:b5:10:73:d1:47 3448 ARPA bvi-ecfe-sig vlan-id 1104
172.16.0.3 ea:e8:51:19:ba:4a 2112 ARPA bvi-ecfe-sig vlan-id 1104
172.16.0.65 1c:90:be:88:f0:00 - ARPA bvi-pcx-sig-a vlan-id 1200
172.16.0.66 42:6a:e4:4a:0f:ff 1441 ARPA bvi-pcx-sig-a vlan-id 1200
172.16.0.67 86:06:ba:52:93:7e 2713 ARPA bvi-pcx-sig-a vlan-id 1200
172.16.0.68 e2:98:ab:f0:4b:c6 1077 ARPA bvi-pcx-sig-a vlan-id 1200
172.16.0.69 1a:23:41:c7:97:31 1787 ARPA bvi-pcx-sig-a vlan-id 1200
172.16.1.65 1c:90:be:88:f0:00 - ARPA bvi-pcx-sig-b vlan-id 1300
172.16.1.66 1e:7d:8c:fe:e1:c2 2378 ARPA bvi-pcx-sig-b vlan-id 1300
172.16.1.68 12:fb:e2:66:af:07 2834 ARPA bvi-pcx-sig-b vlan-id 1300
172.16.1.69 56:3d:15:1f:60:d3 1552 ARPA bvi-pcx-sig-b vlan-id 1300

[sig]router6675#ping 172.16.1.67
PING 172.16.1.67 (172.16.1.67): source 172.16.1.65, 36 data bytes,
timeout is 1 second
.....
---172.16.1.67 PING Statistics---
5 packets transmitted, 0 packets received, 100.0% packet loss

[sig]router6675#
[sig]router6675#show port
[sig]router6675#show port 1/36
Port          Type       State
-----
1/36          ethernet   Up

[sig]router6675#show port 1/36 de
[sig]router6675#show port 1/36 detail
ethernet 1/36 state is Up
Description      : ccd-b sriov
Port circuit     : 1/36:511:63:31/1/0/158
Link state       : Up
Last link state change : Aug 19 18:15:56.353
Line state       : Up
Admin state      : Up
License priority : 6
License Activated : Yes
Port Type        : 25ge
Link Dampening   : disabled
Undampened line state : Up
Dampening Count  : 0
Encapsulation    : dot1q
MTU size         : 1500 Bytes
Storm control mode : off
Evpn MH ES Setting : off
Forward error correction : cl74-fc-fec
FEC state        : cl74-fc-fec
NAS-Port-Type    : none
NAS-Port-Id      : none
MAC address      : 1c:90:be:88:f0:24
Optical Transport : None
Media type       : 100GBase-CR4
Flow control     : off
Speed            : 25 Gbps
Duplex mode      : full
Clock-Source     : local
Link Length Supported : 3 meters
Loopback         : off
SFP+ Transceiver Status
Additional Features : None
Diag Monitor     : NO
Port Alarms       : NONE
Link-delay-time  : 0
Last line state down : Aug 19 18:15:54.791
Trigger faults   : NONE
```

```
[sig]router6675#show port 1/32 detail
ethernet 1/32 state is Up
Description          : ccd-b sriov
Port circuit        : 1/32:511:63:31/1/0/88
Link state          : Up
  Last link state change : Aug 19 18:15:49.066
Line state          : Up
Admin state         : Up
License priority   : 6
License Activated  : Yes
Port Type          : 25ge
Link Dampening     : disabled
Undampened line state : Up
Dampening Count    : 0
Encapsulation      : dot1q
MTU size           : 1500 Bytes
Storm control mode : off
Evpn MH ES Setting : off
Forward error correction : cl74-fc-fec
  FEC state       : cl74-fc-fec
NAS-Port-Type      : none
NAS-Port-Id        : none
MAC address        : 1c:90:be:88:f0:20
Optical Transport   : None
Media type         : 100GBase-CR4
Flow control       : off
Speed              : 25 Gbps
Duplex mode        : full
Clock-Source       : local
Link Length Supported : 3 meters
Loopback           : off
SFP+ Transceiver Status
  Additional Features : None
  Diag Monitor       : NO
  Port Alarms        : NONE
  Link-delay-time   : 0
Last line state down : Aug 19 18:15:46.987
  Trigger faults    : NONE
```

[sig]router6675#

Comment by [Zhigang Han](#) [ 2025-08-14 ]

hi Rajan,

here is the answer for two questions from you:

1, from the output of show port detail, there are two parameters

a, overall status of the port state:

Port status (combination of the Admin and Line state fields):

Down—Port has been configured but is not working.

No card—Port has been configured, but the card is not installed.

Unconfigured—Port is not configured and is down.

Up—Port is working (active).

b, the status of link state:

Physical state of the line:

Down—Port has been configured but is not working.

No card—Port has been configured, but the card is not installed.

Unconfigured—Port is not configured and is down.

Up—Port is working (active).

From our case, we could see link state is down which means there is something wrong with physical link. As you suggested, we should check the physical cable and cable connection.

2, here are a few ways we could try:

- a, If we have no physical issue with the ports, we could try to shut down the port and bring it up;
- b, If not working and if rebooting router will not corrupt the ccd and cnf, we could try to reboot the router
- c, we could also delete port configuration and reconfigure the port then reboot the router.

Thanks,

BR/Zhigang

#### [UCC\_PLM-266] UCC RTX[ UCC 1.0 ] Unable to re-deploy CCSM(Unable to connect to the server: proxyconnect tcp: dial tcp 192.1.16.250:3128: i/o timeout)

Created: 2025-08-14 Updated: 2025-08-20 Resolved: 2025-08-20

Status:	Rejected
Project:	UCC_PLM
Component/s:	None
Affects Version/s:	UCC Appliance 1.0.0
Fix Version/s:	None

Type:	Bug	Priority:	Medium
Reporter:	Rajan Rajeshprasad Gupta	Assignee:	Zhigang Han
Resolution:	Rejected	Votes:	0
Labels:	None		
Remaining Estimate:	Not Specified		
Time Spent:	Not Specified		
Original Estimate:	Not Specified		

Attachments:	<a href="#">CNAT_install_20250812171300.log</a> <a href="#">CNAT_uninstall_20250814181743.log</a> <a href="#">LowLevelDesignUCC1_0_RaytheonUSA.xlsx</a> <a href="#">CNAT_install_20250812172054.log</a> <a href="#">CNAT_install_20250814182202.log</a>
Team/s:	UCC_PLM
Found in Build:	UCC 1.0
Requirement Status:	UCC Appliance 0.2.1 - UNCOVERED

#### Description

Hello,

Customer Raytheon has mistakenly deleted ccsm name-space.

In-order to recover ccsm, we have run ccsm CNF , re-deployment from SFS.

However, CNAT is complaining for proxyconnect tcp timeout.

See below :

```
2025/08/12 17:20:54 INFO [orchestrator.helm._initialize_k8s:54]: clusterName: ccda
2025/08/12 17:20:54 INFO [orchestrator.helm._initialize_k8s:55]: namespace: ccsm
2025/08/12 17:20:54 INFO [orchestrator.helm._initialize_value_file:63]: Values yaml file: /home/ucc/config/ccda/ccsm/values.yaml
2025/08/12 17:20:54 DEBUG [utils.misc.wrap:209]: ==> Duration measurement start <=-
2025/08/12 17:20:54 DEBUG [k8s.cli.run:53]: Running k8s command: kubectl --kubeconfig=/home/ucc/config/ccda/ccd/kubeconfig-ccda -n ccsm version -o json
2025/08/12 17:21:24 DEBUG [utils.misc.newfn:239]: Failed to run <function KubeCmd.run at 0x715571f48c20>: Failed to run K8s command: Unable to connect to the
server: proxyconnect tcp: dial tcp 192.1.16.250:3128: i/o timeout.
2025/08/12 17:21:24 DEBUG [utils.misc.newfn:240]: Wait 3 seconds and try again. Retry 1/3
2025/08/12 17:21:27 DEBUG [k8s.cli.run:53]: Running k8s command: kubectl --kubeconfig=/home/ucc/config/ccda/ccd/kubeconfig-ccda -n ccsm version -o json
2025/08/12 17:21:57 DEBUG [utils.misc.newfn:239]: Failed to run <function KubeCmd.run at 0x715571f48c20>: Failed to run K8s command: Unable to connect to the
server: proxyconnect tcp: dial tcp 192.1.16.250:3128: i/o timeout.
2025/08/12 17:21:57 DEBUG [utils.misc.newfn:240]: Wait 3 seconds and try again. Retry 2/3
2025/08/12 17:22:00 DEBUG [k8s.cli.run:53]: Running k8s command: kubectl --kubeconfig=/home/ucc/config/ccda/ccd/kubeconfig-ccda -n ccsm version -o json
2025/08/12 17:22:30 DEBUG [utils.misc.newfn:239]: Failed to run <function KubeCmd.run at 0x715571f48c20>: Failed to run K8s command: Unable to connect to the
server: proxyconnect tcp: dial tcp 192.1.16.250:3128: i/o timeout.
2025/08/12 17:22:30 DEBUG [utils.misc.newfn:240]: Wait 3 seconds and try again. Retry 3/3
2025/08/12 17:22:33 DEBUG [k8s.cli.run:53]: Running k8s command: kubectl --kubeconfig=/home/ucc/config/ccda/ccd/kubeconfig-ccda -n ccsm version -o json
2025/08/12 17:23:04 ERROR [__main__.<module>:62]: Traceback (most recent call last):
```

```
File "cnat.py", line 59, in <module>
  File "vnflcm/install.py", line 76, in single_install
    execute_pipeline(vnf)
  File "utils/misc.py", line 211, in wrap
```

While checking kubectl command and connection from SFS works fine.

```
ucc@sfs:~$ kubectl --kubeconfig=/home/ucc/config/ccda/ccd/kubeconfig-ccda -n ccsm version -o json
{
  "clientVersion": {
    "major": "1", "minor": "31", "gitVersion": "v1.31.0", "gitCommit": "9edcffcde5595e8a5b1a35f88c421764e575afce", "gitTreeState": "clean", "buildDate": "2024-08-13T07:37:34Z", "goVersion": "go1.22.5", "compiler": "gc", "platform": "linux/amd64" }
  ,
  "kustomizeVersion": "v5.4.2",
  "serverVersion": {
    "major": "1", "minor": "30", "gitVersion": "v1.30.1", "gitCommit": "a17c4c44e0d1462c20dda13a66fe2dab2baa0a6d", "gitTreeState": "clean", "buildDate": "2024-06-08T21:04:40Z", "goVersion": "go1.22.2", "compiler": "gc", "platform": "linux/amd64" }
}
ucc@sfs:~$ ls -lrt /home/ucc/config/ccda/ccd/kubeconfig-ccda
rw----- 1 ucc ucc 5634 Nov 22 2024 /home/ucc/config/ccda/ccd/kubeconfig-ccda
ucc@sfs:~$ ccda
ucc@sfs:~$ kubectl get ns -A
NAME      STATUS   AGE
ccd-task-exec-fw  Active  264d
ccda-standalone  Active  264d
ccdm       Active  260d
ccrc       Active  261d
cert-manager  Active  264d
cnom       Active  260d
default     Active  264d
eda        Active  260d
ep5g        Active  261d
eric-crd-ns  Active  264d
etcd       Active  264d
ingress-nginx  Active  264d
kube-node-lease  Active  264d
kube-public    Active  264d
kube-system    Active  264d
kyverno      Active  264d
monitoring    Active  264d
ucc@sfs:~$ date
Thu Aug 14 10:37:58 AM UTC 2025
ucc@sfs:~$
```

Attached logs,

[CNAT\\_install\\_20250812171300.log](#)  
[CNAT\\_install\\_20250812172054.log](#)  
[CNAT\\_install\\_20250812172054.log](#)

CLI used:

```
export config_dir=/home/ucc
export software_dir=/home/ucc/software
cd $config_dir/config/ccda/ccsm
cnat -k ccda --install --no-cfggen
```

Question1: What is proxyconnect in CNF deployment?

Question2: Do we already seen such errors?

## Comments

Comment by [Zhigang Han](#) [2025-08-20]

Hi Rajan,

Could we close the ticket? we will reject the ticket because the issue is not UCC bug but the issue is related to the configuration error.

Thanks,

BR/Zhigang

Comment by [Rajan Rajeshprasad Gupta](#) [2025-08-20]

Hello Sam,

Thank you for the clue.

Issue was with value.yaml generated with cnat has old nels IP which was no more used.

Fixed after updating value.yaml will correct nels IP which was reachable from CNF/CCDM.

Summary: <error-type>application</error-type> <error-tag>unknown-namespace</error-tag>: Comes when CNF cant get license during installation.

Comment by [Zhigang Han](#) [2025-08-19]

Hi Rajan,

Could you also check license for ccsm if ccsm is able to fetch the license keys from NeLs server or not?

```
kubectl exec -n ccsm deploy/eric-lm-combined-server-license-consumer-handler -c eric-lm-license-consumer-handler -- /opt/LicenseConsumerHandler/listLicenses.sh  
CCSM | jq
```

Thanks,

BR/Zhigang

Comment by [Rajan Rajeshprasad Gupta](#) [2025-08-19]

Hello Sam,

Thank you for suggestion. I see you get same error while doing manual commit though netconf.

See below:

```
ucc@sfs:~/config/ccda/ccsm$ ssh ccsmoam@192.1.16.69 -p 830 -s netconf < ausf_conf.xml  
The authenticity of host '[192.1.16.69]:830 ([192.1.16.69]:830)' can't be established.  
ED25519 key fingerprint is SHA256:RgjrflopMUSXAbFt0wGEHv0vHt4AbFzH616YCqtBFfo.  
This key is not known by any other names.  
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes  
Warning: Permanently added '[192.1.16.69]:830' (ED25519) to the list of known hosts.  
IF YOU ARE NOT AN AUTHORIZED USER, PLEASE EXIT IMMEDIATELYThis system processes personal information. Handle personal information with care. Misuse, including unauthorized access, is grounds for legal action. Version: 1.0, Date: October 27, 2020.(ccsmoam@192.1.16.69) Password:  
<?xml version="1.0" encoding="UTF-8"?>  
<hello xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">  
<capabilities>  
<capability>urn:ietf:params:netconf:base:1.0</capability>  
<capability>urn:ietf:params:netconf:base:1.1</capability>  
<capability>urn:ietf:params:netconf:capability:writable-running:1.0</capability>  
<capability>urn:ietf:params:netconf:capability:rollback-on-error:1.0</capability>  
<capability>urn:ietf:params:netconf:capability:validate:1.0</capability>  
<capability>urn:ietf:params:netconf:capability:validate:1.1</capability>  
<capability>urn:ietf:params:netconf:capability>xpath:1.0</capability>  
<capability>urn:ietf:params:netconf:capability:notification:1.0</capability>  
<capability>urn:ietf:params:netconf:capability:interleave:1.0</capability>  
<capability>urn:ietf:params:netconf:capability:with-defaults:1.0?basic-mode=explicit&also-supported=report-all-tagged,report-all</capability>  
<capability>urn:ietf:params:netconf:capability:with-operational-defaults:1.0?basic-mode=explicit&also-supported=report-all-tagged,report-all</capability>
```

I also see from logs of yang pod, I can see "confd Start of a transaction by usid 190 was rejected since node is in upgrade mode"

```
{"message":"confd Start of a transaction by usid 190 was rejected since node is in upgrade mode","metadata":{"pod_name":"eric-cm-yang-provider-5b645f5599-ch4pv","container_name":"yang-engine","namespace":"ccsm"}, "service_id": "eric-cm-yang-provider", "severity": "error", "timestamp": "2025-08-18T02:43:57.843-04:00", "version": "1.2.0"}  
{"message": " {error,{badmatch,{error,{cs_error,undefined,misc,upgrade_in_progress}},", "metadata": {"pod_name": "eric-cm-yang-provider-5b645f5599-ch4pv", "container_name": "yang-engine", "namespace": "ccsm"}, "service_id": "eric-cm-yang-provider", "severity": "info", "timestamp": "2025-08-18T02:43:57.843-04:00", "version": "1.2.0"}  
{"message": "devel-aaa path \"/ccsm-common/capture-decrypt\" in access Rule \"ericsson-ccsm-4-admin/ericsson-ccsm-capture-decrypt-permit-exec-rule\" is not valid
```

```

for URN 'urn:rdns:com:ericsson:oammodel:ericsson-ccsm-common',"metadata":{"pod_name":"eric-cm-yang-provider-5b645f5599-ch4pv","container_name":"yang-engine","namespace":"ccsm"},"service_id":"eric-cm-yang-provider","severity":"error","timestamp":"2025-08-18T02:43:58.231-04:00","version":"1.2.0"} {"message":"devel-aaa path \"/ccsm-common/capture-decrypt\" in access Rule \\"ericsson-ccsm-4-admin/ericsson-ccsm-capture-decrypt-permit-exec-rule\\\" is not valid for URN 'urn:rdns:com:ericsson:oammodel:ericsson-ccsm-common',"metadata":{"pod_name":"eric-cm-yang-provider-5b645f5599-ch4pv","container_name":"yang-engine","namespace":"ccsm"},"service_id":"eric-cm-yang-provider","severity":"error","timestamp":"2025-08-18T02:43:58.716-04:00","version":"1.2.0"} {"message":"devel-aaa path \"/ccsm-common/capture-decrypt\" in access Rule \\"ericsson-ccsm-4-admin/ericsson-ccsm-capture-decrypt-permit-exec-rule\\\" is not valid for URN 'urn:rdns:com:ericsson:oammodel:ericsson-ccsm-common',"metadata":{"pod_name":"eric-cm-yang-provider-5b645f5599-ch4pv","container_name":"yang-engine","namespace":"ccsm"},"service_id":"eric-cm-yang-provider","severity":"error","timestamp":"2025-08-18T02:43:59.733-04:00","version":"1.2.0"} ecd@ucc-ccda:~> ecd@ucc-ccda:~>

```

Comment by [Zhigang Han](#) [2025-08-18]

Hi Rajan,

Could you try manually to load the configuration into cm yang?

The command should run under ccsm configuration directory:

```
ssh ccsmoam@"ccsm yang IP" -p 830 -s netconf < ausf_conf.xml
```

Thanks,

BR/Zhigang

Comment by [Rajan Rajeshprasad Gupta](#) [2025-08-18]

Hello Sam

Thank you for feedback.

Indeed there was reachability problem towards vNELS.

I could fixed reachability problem also I see license available in vNELS with no expiry

```
(Fm=1)>dn ManagedElement=1,NelsFunction=1,LicenseInventory=980408_RAYTHEON-UCC-1-0-SMALL-BP_CCSM
(LicenseInventory=980408_RAYTHEON-UCC-1-0-SMALL-BP_CCSM)>
(LicenseInventory=980408_RAYTHEON-UCC-1-0-SMALL-BP_CCSM)>show -r
LicenseInventory=980408_RAYTHEON-UCC-1-0-SMALL-BP_CCSM
  timeOfLastLicenseInventoryUpdate="2025-08-18T02:57:25"
  CumulativeCapacityLicense=FAT1024210/2
    activationTime="2024-11-21T00:00:00"
    customerId="980408"
    expirationTime="License has no expiration date"
    key="FAT1024210/2"
    name="CCSM UDM/ARPF eMBB Base Package"
    periodLength=MONTH
    periodStart=CALENDAR_BASED
    productType="CCSM"
    softwareLicenseTarget="RAYTHEON-UCC-1-0-SMALL-BP"
    usedCapacity=0
    version=""
    totalCapacity
      value=50000
  CumulativeCapacityLicense=FAT1024210/1
    activationTime="2024-11-21T00:00:00"
    customerId="980408"
    expirationTime="License has no expiration date"
```

Nels connectivity from CCD:

```
ecd@ucc-ccda:~> curl -v 192.1.16.193:9095 -m 1
*   Trying 192.1.16.193:9095...
* Connected to 192.1.16.193 (192.1.16.193) port 9095 (#0)
> GET / HTTP/1.1
> Host: 192.1.16.193:9095
> User-Agent: curl/8.0.1
> Accept: */*
>
* Operation timed out after 1000 milliseconds with 0 bytes received
* Closing connection 0
curl: (28) Operation timed out after 1000 milliseconds with 0 bytes received
ecd@ucc-ccda:~>
```

However, I am still facing same error for commit failure for day1 config.

```
2025/08/14 18:32:48 INFO: Loading CMYP config from file: /home/ucc/config/ccda/ccsm/ausf_conf.xml
2025/08/14 18:32:59 WARNING: Failed to load config file: Timeout waiting for string: '<ok></rpc-reply>'. But received:
<?xml version="1.0" encoding="UTF-8"?>
<hello xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
<capabilities>
<capability>urn:ietf:params:netconf:base:1.0</capability>
</capabilities>
</hello>]]>]]
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<rpc xmlns="urn:ietf:params:xml:ns:netconf:base:1.0" message-id="0">
<edit-config>
<target><running></target>
<config xmlns:xc="urn:ietf:params:xml:ns:netconf:base:1.0">
<ausf xmlns="urn:rdns:com:ericsson:oammodel:ericsson-ausf">
<ausf-engine>
<session-timer>5</session-timer>
<retry-number>2</retry-number>
<udm-url>https://udm-ccsm-bbncam1a.5gc.mnc480.mcc999.3gppnetwork.org:443/nudm-ueau/v1</udm-url>
</ausf-engine>
<nf-profile>
<instance-id>76f4b62e-f3f7-454e-9562-415553a1c1d1</instance-id>
<requested-status>registered</requested-status>
</ausf>
</ausf>
</config>
</edit-config>
</rpc>
```

Comment by [Zhigang Han](#) [ 2025-08-15 ]

hi Rajan,

we had the similar issue for one site related to <error-tag>unknown-namespace</error-tag> when we had NeLs issue. Please make sure NeLs server is available during the redeployment.

Thanks,

BR/Zhigang

Comment by [Zhigang Han](#) [ 2025-08-14 ]

hi Rajan,

from the first failed deployment cnat log, we could see :

```
2025/08/12 17:20:54 DEBUG [k8s.cli.run:53]: Running k8s command: kubectl --kubeconfig=/home/ucc/config/ccda/ccd/kubeconfig-ccda -n ccsm version -o json
2025/08/12 17:21:24 DEBUG [utils.misc.newfn:239]: Failed to run <function KubeCmd.run at 0x715571f48c20>: Failed to run K8s command: Unable to connect to the server: proxyconnect tcp: dial tcp 192.1.16.250:3128: i/o timeout.
```

K8 is running this command:

```
kubectl --kubeconfig=/home/ucc/config/ccda/ccd/kubeconfig-ccda -n ccsm version -o json
```

I believe kubeconfig-ccda might be corrupted which k8 might find 192.1.16.250 from kubeconfig-ccda file during the deployment.

could you recopy the file from ccda under /home/ucc/config/ccda/ccd/kubeconfig-ccda from ccda server?

here is the location of config file on ccda server:

```
eccc@ucc-ccda:~/kube> pwd
/home/eccc/kube
eccc@ucc-ccda:~/kube> ll
total 8
drwxr-x--- 4 eccc eccc 47 Jun 16 20:27 cache
rw----- 1 eccc users 6079 Jun 16 20:19 config
eccc@ucc-ccda:~/kube>
```

we might need to update server IP in config file from internal IP to oam IP of ccda server.

For the later issue related to " installation is not successful as after step-15, configuration via netconf has started failing with "<error-tag>unknown-namespace</error-tag>"" ,

here is the suggestion to redo all steps for ccsm part:

configuration part and chapter 12 network function deployment.

Thanks,

BR/Zhigang

Comment by Rajan Rajeshprasad Gupta [ 2025-08-14 ]

Installation proceed by applying below work-around

```
cnat --cfggen-info $config_dir/config/ccda/ccsm/cfggen.yaml --cfggen
cd $config_dir/config/ccda/ccsm
cnat -k ccda --install --no-cfggen
```

However, installation is not successful as after step-15, configuration via netconf has started failing with "<error-tag>unknown-namespace</error-tag>" see below;

```
2025/08/14 18:32:48 INFO: Pipeline job 'step-15' succeeded
2025/08/14 18:32:48 INFO: Running pipeline job with timeout 5400 seconds
2025/08/14 18:32:48 INFO: ==> Running pipeline job 'step-16' using module 'load-cmvp-app-config'
2025/08/14 18:32:48 INFO: Loading CMVP config from file: /home/ucc/config/ccda/ccsm/ausf_conf.xml
2025/08/14 18:32:59 WARNING: Failed to load config file: Timeout waiting for string: '<ok/></rpc-reply>'. But received:
<?xml version="1.0" encoding="UTF-8"?>
<hello xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
<capabilities>
<capability>urn:ietf:params:netconf:base:1.0</capability>
</capabilities>
</hello>]]>
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<rpc xmlns="urn:ietf:params:xml:ns:netconf:base:1.0" message-id="0">
<edit-config>
<target><running/></target>
<config xmlns:xc="urn:ietf:params:xml:ns:netconf:base:1.0">
<ausf xmlns="urn:rdns:com:ericsson:oammodel:ericsson-ausf">
<ausf-engine>
<session-timer>5</session-timer>
```

Tried, termination of cnat and installing back again, however it does not work.

It seems we are hitting adp bug as below;

[ADPPRG-22810](#) CM-Yang-Provider test traffic failure - eTeamProject Alpha

Let me know your views.

attached cnat logs.

[CNAT\\_uninstall\\_20250814181743.log](#)

[CNAT\\_install\\_20250814182202.log](#)

Comment by Rajan Rajeshprasad Gupta [ 2025-08-14 ]

Hello Sam,

Pls find, I could not find IP.

```
ucc@sfs:~$ echo $config_dir
echo $software_dir
/home/ucc
/home/ucc/software
ucc@sfs:~$ echo $HTTP_PROXY
echo $HTTPS_PROXY
echo $http_proxy
echo $https_proxy
```

```
ucc@sfs:~$
ucc@sfs:~$
ucc@sfs:~$ env | grep -i proxy; kubectl config view --raw
apiVersion: v1
clusters: null
contexts: null
current-context: ""
kind: Config
preferences: {}
users: null
ucc@sfs:~$
```

Should we check with CNAT colleagues to know how cnat is picking up such weird IP, I too could not find this ip from cnat logs.

From journalctl, I could see some logs for same IP but those logs are old in 2024 and nothing in 2025.

```

ucc@sfs:~$ journalctl | grep 192.1.16.250
Hint: You are currently not seeing messages from other users and the system.
      Users in groups 'adm', 'systemd-journal' can see all messages.
      Pass -q to turn off this notice.
Nov 21 18:01:54 sfs sshd[26840]: Received disconnect from 192.1.16.250 port 51504:11: disconnected by user
Nov 21 18:01:54 sfs sshd[26840]: Disconnected from user ucc 192.1.16.250 port 51504
Nov 21 20:21:48 sfs sshd[31377]: Received disconnect from 192.1.16.250 port 37352:11: disconnected by user
Nov 21 20:21:48 sfs sshd[31377]: Disconnected from user ucc 192.1.16.250 port 37352
Nov 22 03:35:34 sfs sshd[41848]: Received disconnect from 192.1.16.250 port 33896:11: disconnected by user
Nov 22 03:35:34 sfs sshd[41848]: Disconnected from user ucc 192.1.16.250 port 33896
Nov 22 03:40:01 sfs sshd[41966]: Received disconnect from 192.1.16.250 port 50950:11: disconnected by user
Nov 22 03:40:01 sfs sshd[41966]: Disconnected from user ucc 192.1.16.250 port 50950
Nov 22 03:41:58 sfs sshd[42043]: Received disconnect from 192.1.16.250 port 48246:11: disconnected by user
Nov 22 03:41:58 sfs sshd[42043]: Disconnected from user ucc 192.1.16.250 port 48246
Nov 22 03:42:08 sfs sshd[42097]: Received disconnect from 192.1.16.250 port 51950:11: disconnected by user
Nov 22 03:42:08 sfs sshd[42097]: Disconnected from user ucc 192.1.16.250 port 51950
Nov 22 06:39:36 sfs sshd[42156]: Received disconnect from 192.1.16.250 port 47186:11: disconnected by user
Nov 22 06:39:36 sfs sshd[42156]: Disconnected from user ucc 192.1.16.250 port 47186
Nov 22 12:09:18 sfs sshd[48625]: Received disconnect from 192.1.16.250 port 53332:11: disconnected by user
Nov 22 12:09:18 sfs sshd[48625]: Disconnected from user ucc 192.1.16.250 port 53332
Nov 22 13:15:11 sfs sshd[51664]: Received disconnect from 192.1.16.250 port 47496:11: disconnected by user
Nov 22 13:15:11 sfs sshd[51664]: Disconnected from user ucc 192.1.16.250 port 47496
Nov 22 20:25:01 sfs sshd[52011]: Received disconnect from 192.1.16.250 port 32051:11: disconnected by user

```

Comment by [Zhigang Han](#) [ 2025-08-14 ]

Hi Rajan,

We have searched "port 3128 and proxyconnect" from the jinja2 scripts. unfortunately I donot see these information defined in jinja2 scripts.

here are questions from our side:

how did customer deploy UCC from jumphost? was there a proxy server between jumphost and ucc servers? the error below showed kubectl was not able to connect the proxy server 192.1.16.250:3128

Failed to run K8s command: Unable to connect to the server: proxyconnect tcp: dial tcp 192.1.16.250:3128: i/o timeout.

Could you also check if there are proxy setting in the environment?

the following clis from them where they run cnat + kubectl under it.

Check if proxy is set in environment

```

echo $HTTP_PROXY
echo $HTTPS_PROXY
echo $http_proxy
echo $https_proxy

```

and also run this command:

```
env | grep -i proxy; kubectl config view --raw
```

Hopefully we could find where is 192.1.16.250 defined.

Thanks,

BR/Zhigang

Comment by [Rajan Rajeshprasad Gupta](#) [ 2025-08-14 ]

attached LLD [LowLevelDesignUCC1\\_0\\_RaytheonUSA.xlsx](#)

[UCC\_PLM-264] TMO: UCC 1.1 # AMF complaints for "CertM Certificate Not Available"-2 Created: 2025-07-25 Updated: 2025-08-20 Resolved: 2025-08-20

<b>Status:</b>	Done
<b>Project:</b>	UCC_PLM
<b>Component/s:</b>	None
<b>Affects Version/s:</b>	UCC Appliance 1.0.1
<b>Fix Version/s:</b>	None

<b>Type:</b>	Bug	<b>Priority:</b>	Medium
--------------	-----	------------------	--------

<b>Reporter:</b>	Rajan Rajeshprasad Gupta	<b>Assignee:</b>	Adrian-Bogdan Iliescu
<b>Resolution:</b>	Closed	<b>Votes:</b>	0
<b>Labels:</b>	None		
<b>Remaining Estimate:</b>	Not Specified		
<b>Time Spent:</b>	Not Specified		
<b>Original Estimate:</b>	Not Specified		

<b>Attachments:</b>	
<b>Team/s:</b>	UCC_XFT2
<b>Found in Build:</b>	UCC 1.1
<b>Requirement Status:</b>	UCC Appliance 0.2.1 - UNCOVERED

#### Description

Hello,

Refer ticket [UCC\\_PLM-251](#) TMO: UCC 1.1 # AMF complaints for "CertM Certificate Not Available" - eTeamProject Alpha

Upon reviewing the Installation Guide for CPI, Chapter 2 provides detailed information about the number of Certificate Authorities (CAs) required. Specifically, it explains the different CA certificates and key pairs needed for various components within the system to ensure secure communication and proper installation.

- A pair of CA certificate and corresponding asymmetric keys is required for CCD installation (ca-ccd.crt and ca-ccd.key), and another pair is needed to generate certificates for secure communication with/between network functions included in UCC (ca.crt, ca.pem, and ca.key). These files must be secured by the customer and uploaded to the Jump Host server according to the instructions in Section 9.

Also; Chapter 5.2 PKCS#1 format is mentioned.

## 5.2 Requirements for Certificates

- The SSL keys provided with certificates must be unencrypted and not password protected.
- The certificates must use private keys in the PKCS#1 format (RSA) with a key size of minimum 2048 bits.
- The certificates must use SHA-256 (also known as SHA-2).

There is no information available about CNF CA format which is required to be PKCS#8 to work.

While the current documentation states that the certificates must use private keys in PKCS#1 format (RSA) with a minimum key size of 2048 bits, this is not entirely accurate. The CNF components actually require CA private keys to be in PKCS#8 format.

Please improve Installation guide CPI so engineer can read and understand clearly to avoid issue occur in [UCC\\_PLM-251](#) TMO: UCC 1.1 # AMF complaints for "CertM Certificate Not Available" - eTeamProject Alpha

#### Comments

Comment by [Zhigang Han](#) [ 2025-08-19 ]

Hi Rajan,

Could we close plm 264 ticket?

Thanks,

BR/Zhigang

Comment by Adrian-Bogdan Iliescu [ 2025-08-19 ]

I just checked for the updates, the document has been also updated.:

"Yes actually we have reviewed the Installation Instruction Mirac + Alexander + Marco, the final information will be looks like this"

## 5.2 Requirements for CA Certificates

- The keys used for TLS must be unencrypted and not password protected.
- The CA certificates must use private keys in the PKCS#1 format (RSA) with a key size of 2048 bits for CCD.
- The CA certificates must use private keys in the PKCS#8 format (RSA) with a key size of 2048 bits for CNFs.
- The certificates must use SHA-256 (also known as SHA-2).

Comment by Rajan Rajeshprasad Gupta [ 2025-08-19 ]

Fix is shared in earlier ticket [UCC\\_PLM-251](#) TMO: UCC 1.1 # AMF complaints for "CertM Certificate Not Available" - eTeamProject Alpha.

After generating correct certificate in PKCS#8 for CNFs, No-more error is reported.

Comment by Adrian-Bogdan Iliescu [ 2025-08-19 ]

Sorry for late feedback,

I discuss this topic with Marco and Soner, some improvements will be done in documentation, indeed it is not very clear.  
but the name of the ticket is pointing to an error, do you have a problem with the certificates ?

Comment by Zhigang Han [ 2025-07-25 ]

Hi Rajan,

I totally agree on your point. We should clearly mention the formats of these two sets of keys( ccd PKCS#1 and cnf PKCS#8) in the installation instruction. I have assigned the ticket to XFT2 team. Let us wait for the answer from the design.

Thanks,

BR/Zhigang

[UCC\_PLM-263] UCC VZ [ UCC 1.1 ] subscriber management in cnom generating error Created: 2025-07-23 Updated: 2025-07-29 Resolved: 2025-07-25

Status:	Rejected
Project:	<a href="#">UCC_PLM</a>
Component/s:	None
Affects Version/s:	<a href="#">UCC Appliance 1.1.0</a>
Fix Version/s:	None

Type:	Bug	Priority:	Medium
Reporter:	<a href="#">Mohit Tomar</a>	Assignee:	<a href="#">Christos Delis (EXT)</a>
Resolution:	Rejected	Votes:	0
Labels:	UCC-CNOM		
Remaining Estimate:	Not Specified		
Time Spent:	Not Specified		
Original Estimate:	Not Specified		

Attachments:	
Team/s:	UCC_XFT3
Found in Build:	UCC 1.1
Requirement Status:	UCC Appliance 0.2.1 - UNCOVERED

## Description

Hello,

we had our calls successful, just that when we are seeing the subs management in cnom there is no subscribers visible here, adp logs also attached, the snip is from ONGOING

The screenshot shows the CNOM (Customer Network Operations Manager) interface. The left sidebar has a blue header 'Subscriber Management' and a list of other modules like Status Overview, Alarm Viewer, Health Check, APN/DNN Viewer, UE Status Viewer, KPI and Alert Management, Data Collection Management, Node Monitor, Tracing, Settings, Backup and Restore Management, and User Management. The main area is titled 'Subscriber Management ccda\_Appliance - Select item' and shows a 'Subscription list'. It includes filters for 'IMSI' and 'MSISDN' and a '5G subscription' button. The 'Subscribers' tab is selected.

## Comments

Comment by [Zhigang Han](#) [2025-07-25]

Hi Mohit,

In UCC 1.1 installation instructions 18.1, we have the clear instructions and commands to show the engineer how to set extra values in UCA:

*For UCC Appliance, extra values need to set in UCA.*

### Note:

*UCA is installed only on cluster A and for that reason, CNOM must be integrated only with this.*

1. For **hostname, the provisioning FQDN from UCA need to be used:**

```
export KUBECCDA=$config_dir/config/ccda/ccd/kubeconfig-ccda
kubectl --kubeconfig $KUBECCDA get httpproxies.projectcontour.io -n uca | grep prov-ingress | awk '\{print $2\}'
```

We are glad you are able to identify the wrong hostname and fix the issue. We close the ticket!

[Christos Delis \(EXT\)](#) the root cause is identified and the issue is fixed.

The engineer used the wrong FQDN as hostname when he configured UCA which caused cnom was not able to reach UCA with the correct network:

[oam.uca-ericucc1a.ericucc1.internal.ericsson.com](#)

The correct hostname should be:

[prov.uca-ericucc1a.ericucc1.internal.ericsson.com](#)

Thanks,

Comment by Mohit Tomar [ 2025-07-25 ]

```
ucc@sfs:~$ export KUBECCDA=$config_dir/config/ccda/ccd/kubeconfig-ccda
kubectl --kubeconfig $KUBECCDA get httpproxies.projectcontour.io \
-n uca | grep prov-ingress | awk '\{print $2\}'
prov.uca-ericucc1a.ericucc1.internal.ericsson.com
ucc@sfs:~$
```

Comment by Mohit Tomar [ 2025-07-25 ]

Node list 1 of 19 selected			
<input type="checkbox"/> Node type ◊	Node name ◊	Network service ◊	Node IP or hostname ◊
<input checked="" type="checkbox"/> UCA	UCA_ccda	UCC_CCDa	prov.uca-ericucc1a.ericucc1.internal.ericsson.com
<input type="checkbox"/> PCC-MM	PCC-MM_ccdb	UCC_CCDb	10.161.89.6
<input type="checkbox"/> PCG	PCG_ccda	UCC_CCDa	10.161.89.64
<input type="checkbox"/> PCC-MM	PCC-MM_ccda	UCC_CCDa	10.161.89.64
<input type="checkbox"/> PCC-SM	PCC-SM_ccda	UCC_CCDa	10.161.89.64
<input type="checkbox"/> CCSM	CCSM_ccdb	UCC_CCDb	10.161.89.101
<input type="checkbox"/> CCPC	CCPC_ccdb	UCC_CCDb	10.161.89.96
<input type="checkbox"/> CCPC	CCPC_ccda	UCC_CCDa	10.161.89.64
<input type="checkbox"/> CCRC	CCRC_ccdb	UCC_CCDb	10.161.89.102
<input type="checkbox"/> CCRC	CCRC_ccda	UCC_CCDa	10.161.89.70
<input type="checkbox"/> SC	SC_ccdb	UCC_CCDb	10.161.89.107
<input type="checkbox"/> ROUTER6000	UCC_Router6k	UCC_CCDa	10.161.89.161
<input type="checkbox"/> PCG	PCG_ccdb	UCC_CCDb	10.161.89.96
<input type="checkbox"/> PCC-SM	PCC-SM_ccdb	UCC_CCDb	10.161.89.96
<input type="checkbox"/> HPE	HPE_cccd	UCC_CCDb	10.161.89.3
<input type="checkbox"/> HPE	HPE_ccda	UCC_CCDa	10.161.89.2
<input type="checkbox"/> CCSM	CCSM_ccda	UCC_CCDa	10.161.89.69
<input type="checkbox"/> CCDM	CCDM_ccdb	UCC_CCDb	10.161.89.98
<input type="checkbox"/> CCDM	CCDM_ccda	UCC_CCDa	10.161.89.66

← [1](#) →

Comment by Mohit Tomar [ 2025-07-25 ]

Thanks! case can be closed.

Comment by Mohit Tomar [ 2025-07-25 ]

X Menu

Subscriber Management ccdb\_Appliance - Select item

Status Overview

Alarm Viewer

Health Check

APN/DNN Viewer

Subscriber Management

UE Status Viewer

KPI and Alert Management

Data Collection Management

Node Monitor

&gt; Tracing

v Settings

Subscribers Provisioning history

Subscription list Last updated 6 minutes ago

IMSI ▾ Filter: IMSI

IMSI	MSISDN	5G subscription
999480400007159	860810000007159	(1)
999480400007160	860810000007160	(1)
999480400007161	860810000007161	(1)
999480400007162	860810000007162	(1)
999480400007163	860810000007163	(1)

Comment by Mohit Tomar [2025-07-25]

hello, I fixed the problem, the problem is with the hostname, we configured oam.uca-ericucc1a.ericucc1.internal.ericsson.com in place of prov.uca-ericucc1a.ericucc1.interna but i was just wondering why with this incorrect hostname the node monitoring is showing green.

Comment by Mohit Tomar [2025-07-25]

```
eccd@ucc-ccda:~> kubectl get pods -n uca
NAME                               READY   STATUS    RESTARTS   AGE
eric-act-aaa-5b95479dd7-qnmjg      1/1    Running   0          10d
eric-act-activation-engine-7cdc59f49b-w4z29   1/1    Running   0          10d
eric-act-activation-orchestrator-54659b7fdf-17nqp   1/1    Running   0          10d
eric-act-activation-deployer-59fc94c9d8-cv4vh     1/1    Running   4 (2d17h ago) 10d
eric-act-application-resource-monitor-69444947bf-jhs8p  1/1    Running   1 (2d17h ago) 10d
eric-act-backup-restore-preparation-agent-55f85b495d-2zx96  1/1    Running   0          10d
eric-act-csr-data-collection-5464cd5d4b-66sm4     1/1    Running   0          10d
eric-act-inbound-batch-handler-794487969b-xhg15    1/1    Running   0          10d
eric-act-inbound-interfaces-5778ff78dd-xn5zj       1/1    Running   0          10d
eric-act-proclog-cassandra-stasher-7f65b46469-g5kzq  1/1    Running   0          10d
eric-act-proclog-manager-799db494c8-wr24d        1/1    Running   0          10d
eric-act-rest-provisioning-5954f4f898-gttwm       1/1    Running   0          10d
eric-act-service-locator-registry-0              1/1    Running   0          10d
eric-act-tomcat-6745968995-njcbt                1/1    Running   0          10d
eric-cnom-server-54f5b5b5d8-6j427                2/2    Running   0          10d
eric-ctrl-bro-0                                1/1    Running   0          10d
eric-data-coordinator-zk-0                      2/2    Running   0          10d
eric-data-coordinator-zk-agent-757567f5b4-vwhm7   2/2    Running   0          10d
eric-data-distributed-coordinator-ed-0           2/2    Running   0          10d
eric-data-distributed-coordinator-ed-agent-b6d5fc98-2d918 2/2    Running   0          10d
eric-data-document-database-cc-0                 2/2    Running   2          10d
```

Comment by Mohit Tomar [2025-07-25]

Menu

## Node Monitor

Status Overview

Alarm Viewer

Health Check

APN/DNN Viewer

Subscriber Management

UE Status Viewer

KPI and Alert Management

Data Collection Management

**Node Monitor**

&gt; Tracing

&gt; Settings

Backup and Restore Management

User Management

### Select columns

- Node IP or hostname
- SSH port
- SFTP IP or hostname
- SFTP port
- HTTP port
- HTTPS port
- EBM port
- vTap server IP
- UTC time offset
- SSH host key status
- Links

### Node list 1 of 19 selected

All Filter: All

Node type	Node name	Network service	Monitor status	Monitor status changed	RT
CCDM	CCDM_ccda	UCC_CCDa	<span>Started</span>	2025-07-23 17:04	-
CCDM	CCDM_ccdb	UCC_CCDb	<span>Started</span>	2025-07-23 17:06	-
CCPC	CCPC_ccda	UCC_CCDa	<span>Started</span>	2025-07-23 17:18	-
CCPC	CCPC_ccdb	UCC_CCDb	<span>Started</span>	2025-07-23 18:16	-
CCRC	CCRC_ccda	UCC_CCDa	<span>Started</span>	2025-07-23 17:06	-
CCRC	CCRC_ccdb	UCC_CCDb	<span>Started</span>	2025-07-23 17:04	-
CCSM	CCSM_ccda	UCC_CCDa	<span>Started</span>	2025-07-23 17:04	-
CCSM	CCSM_ccdb	UCC_CCDb	<span>Started</span>	2025-07-23 18:10	-
HPE	HPE_ccda	UCC_CCDa	<span>Started</span>	2025-07-23 21:21	-
HPE	HPE_ccdb	UCC_CCDb	<span>Started</span>	2025-07-22 23:42	-
PCC-MM	PCC-MM_ccda	UCC_CCDa	<span>Started</span>	2025-07-23 15:02	-
PCC-MM	PCC-MM_ccdb	UCC_CCDb	<span>Started</span>	2025-07-23 00:13	-
PCC-SM	PCC-SM_ccda	UCC_CCDa	<span>Started</span>	2025-07-23 15:01	-
PCC-SM	PCC-SM_ccdb	UCC_CCDb	<span>Started</span>	2025-07-23 00:12	-
PCG	PCG_ccda	UCC_CCDa	<span>Started</span>	2025-07-23 15:01	-
PCG	PCG_ccdb	UCC_CCDb	<span>Started</span>	2025-07-23 00:12	-
ROUTER6000	ROUTER6000_ccda	UCC_CCDa	<span>Started</span>	2025-07-18 13:47	-
SC	SC_ccdb	UCC_CCDb	<span>Started</span>	2025-07-25 09:03	-
<input checked="" type="checkbox"/> UCA	UCA_ccda	UCC_CCDa	<span>Started</span>	2025-07-22 20:32	-

< 1 >

Comment by Mohit Tomar [ 2025-07-25 ]

Left sidebar:

- Node Monitor** (selected)
- Status Overview
- Alarm Viewer
- Health Check
- APN/DNN Viewer
- Subscriber Management
- UE Status Viewer
- KPI and Alert Management
- Data Collection Management
- Tracing
- Settings
- Backup and Restore Management
- User Management

Header bar:

CNOM https://oam-cnom-ericucc1b.ericucc1.internal.ericsson.com/cnom/#node-monitor

Main content area:

### Monitor status

Started (19) | Stopped (0) | Scheduled (0) | Start error (0) | Stop error (0) | Schedule error (0) | Starting (0) | Stopping (0)

#### Select columns

<input type="checkbox"/> Node IP or hostname	<input type="checkbox"/> SSH port	<input type="checkbox"/> SFTP IP or hostname	<input type="checkbox"/> SFTP port	<input type="checkbox"/> HTTP port	<input type="checkbox"/> HTTPS port	<input type="checkbox"/> EBM port	<input type="checkbox"/> vTap server IP	<input type="checkbox"/> UTC time offset	<input type="checkbox"/> SSH host key status	<input type="checkbox"/> Links
--	-----------------------------------	--	------------------------------------	------------------------------------	-------------------------------------	-----------------------------------	---	--	--	--------------------------------

#### Node list

0 of 19 selected

<input type="checkbox"/> Node type	<input type="checkbox"/> Node name	<input type="checkbox"/> Network service	<input type="checkbox"/> Monitor status	<input type="checkbox"/> Monitor status changed	<input type="checkbox"/> RT monitor status
<input type="checkbox"/> CCDM	CCDM_ccda	UCC_CCDA	<span>Started</span>	2025-07-23 17:09	-
<input type="checkbox"/> CCDM	CCDM_ccdb	UCC_CCDb	<span>Started</span>	2025-07-23 17:09	-
<input type="checkbox"/> CCPC	CCPC_ccda	UCC_CCDA	<span>Started</span>	2025-07-23 17:19	-
<input type="checkbox"/> CCPC	CCPC_ccdb	UCC_CCDb	<span>Started</span>	2025-07-23 18:18	-
<input type="checkbox"/> CCRC	CCRC_ccda	UCC_CCDA	<span>Started</span>	2025-07-23 17:09	-
<input type="checkbox"/> CCRC	CCRC_ccdb	UCC_CCDb	<span>Started</span>	2025-07-23 17:10	-
<input type="checkbox"/> CCSM	CCSM_ccda	UCC_CCDA	<span>Started</span>	2025-07-23 17:09	-
<input type="checkbox"/> CCSM	CCSM_ccdb	UCC_CCDb	<span>Started</span>	2025-07-23 18:23	-
<input type="checkbox"/> HPE	HPE_ccda	UCC_CCDA	<span>Started</span>	2025-07-23 21:22	-
<input type="checkbox"/> HPE	HPE_cccdb	UCC_CCDb	<span>Started</span>	2025-07-22 23:16	-
<input type="checkbox"/> PCC-MM	PCC-MM_ccda	UCC_CCDA	<span>Started</span>	2025-07-23 18:41	-
<input type="checkbox"/> PCC-MM	PCC-MM_ccdb	UCC_CCDb	<span>Started</span>	2025-07-23 18:45	-
<input type="checkbox"/> PCC-SM	PCC-SM_ccdb	UCC_CCDb	<span>Started</span>	2025-07-23 00:12	-
<input type="checkbox"/> PCC-SM	PCC-SM_ccda	UCC_CCDA	<span>Started</span>	2025-07-23 18:41	-
<input type="checkbox"/> PCG	PCG_ccdb	UCC_CCDb	<span>Started</span>	2025-07-23 00:12	-
<input type="checkbox"/> PCG	PCG_ccda	UCC_CCDA	<span>Started</span>	2025-07-23 18:42	-
<input type="checkbox"/> ROUTER6000	UCC_Router6k	UCC_CCDA	<span>Started</span>	2025-07-21 19:50	-
<input type="checkbox"/> SC	SC_ccdb	UCC_CCDb	<span>Started</span>	2025-07-23 00:04	-
<input type="checkbox"/> UCA	UCA_ccda	UCC_CCDA	<span>Started</span>	2025-07-22 20:32	-

Page navigation: ← 1 →

https://oam-cnom-ericucc1a.ericucc1.internal.ericsson.com/cnom/#node

## CNOM

**Menu**

- Status Overview
- Alarm Viewer
- Health Check
- APN/DNN Viewer
- Subscriber Management
- UE Status Viewer
- KPI and Alert Management
- Data Collection Management
- Node Monitor**
- > Tracing
- > Settings
- Backup and Restore Management
- User Management

### Node Monitor

Select columns

All <input type="button" value="▼"/>	Filter: All <input type="text" value=""/>	Node type <input type="button" value="▼"/>	Node name <input type="button" value="▼"/>	Network service <input type="button" value="▼"/>	Monitor status <input type="button" value="▼"/>	Monitor status changed <input type="button" value="▼"/>	RT
<input type="checkbox"/>		CCDM	CCDM_ccda	UCC_CCDa	<span style="color: green;">● Started</span>	2025-07-23 17:04	-
<input type="checkbox"/>		CCDM	CCDM_ccdb	UCC_CCDb	<span style="color: green;">● Started</span>	2025-07-23 17:06	-
<input type="checkbox"/>		CCPC	CCPC_ccda	UCC_CCDa	<span style="color: green;">● Started</span>	2025-07-23 17:18	-
<input type="checkbox"/>		CCPC	CCPC_ccdb	UCC_CCDb	<span style="color: green;">● Started</span>	2025-07-23 18:16	-
<input type="checkbox"/>		CCRC	CCRC_ccda	UCC_CCDa	<span style="color: green;">● Started</span>	2025-07-23 17:06	-
<input type="checkbox"/>		CCRC	CCRC_ccdb	UCC_CCDb	<span style="color: green;">● Started</span>	2025-07-23 17:04	-
<input type="checkbox"/>		CCSM	CCSM_ccda	UCC_CCDa	<span style="color: green;">● Started</span>	2025-07-23 17:04	-
<input type="checkbox"/>		CCSM	CCSM_ccdb	UCC_CCDb	<span style="color: green;">● Started</span>	2025-07-23 18:10	-
<input type="checkbox"/>		HPE	HPE_ccda	UCC_CCDa	<span style="color: green;">● Started</span>	2025-07-23 21:21	-
<input type="checkbox"/>		HPE	HPE_ccdb	UCC_CCDb	<span style="color: green;">● Started</span>	2025-07-22 23:42	-
<input type="checkbox"/>		PCC-MM	PCC-MM_ccda	UCC_CCDa	<span style="color: green;">● Started</span>	2025-07-23 15:02	-
<input type="checkbox"/>		PCC-MM	PCC-MM_ccdb	UCC_CCDb	<span style="color: green;">● Started</span>	2025-07-23 00:13	-
<input type="checkbox"/>		PCC-SM	PCC-SM_ccda	UCC_CCDa	<span style="color: green;">● Started</span>	2025-07-23 15:01	-
<input type="checkbox"/>		PCC-SM	PCC-SM_ccdb	UCC_CCDb	<span style="color: green;">● Started</span>	2025-07-23 00:12	-
<input type="checkbox"/>		PCG	PCG_ccda	UCC_CCDa	<span style="color: green;">● Started</span>	2025-07-23 15:01	-
<input type="checkbox"/>		PCG	PCG_ccdb	UCC_CCDb	<span style="color: green;">● Started</span>	2025-07-23 00:12	-
<input type="checkbox"/>		ROUTER6000	UCC_Router6k	UCC_CCDa	<span style="color: green;">● Started</span>	2025-07-18 13:47	-
<input type="checkbox"/>		SC	SC_ccdb	UCC_CCDb	<span style="color: green;">● Started</span>	2025-07-25 09:03	-
<input type="checkbox"/>		UCA	UCA_ccda	UCC_CCDa	<span style="color: green;">● Started</span>	2025-07-22 20:32	-

← 1 →

Comment by Christos Delis (EXT) [ 2025-07-25 ]

Good morning,

Could you please check from CNOM Node Monitor tab if UCA node is up and running?

Also could you please check if all network elements are UP and Active from UCA ?

BRs,  
Christos

Comment by Zhigang Han [ 2025-07-24 ]

Hi Soner,

Could you check the issue from your side? Here is what we have done:

1, originally we thought the issue was related to the wrong user, however after creating new user for network runner, we saw the same error in eric-cnom-data-ingester log

2, we also checked the subscribers manually which we could see the subscribers do exist. the output of manually checking subscribers is attached.

Here is the error message we saw in the log:

```
{"version": "1.2.0", "timestamp": "2025-07-23T10:55:24-0400", "severity": "error", "service_id": "eric-cnom-data-ingester", "message": "Failed to request in thread ID\n\"metadata\": \\"{\"function\": \"_process_core\", \"proc_id\": \"subscribers_sync.UCA_ccda/18634\"}\"}
```

Thanks,

BR/Zhigang

Comment by [Mohit Tomar](#) [2025-07-24]

hello Zhigang, we have created user enterprise\_admin with enterprise\_security\_admin role to be used for network runner gives the same error.

Comment by [Zhigang Han](#) [2025-07-23]

Hi Mohit,

Here is the log which you showed me:

```
{"version":"1.2.0","timestamp":"2025-07-22T14:42:19.096-04:00","severity":"info","service_id":"eric-cnom-server","message":"POST /cnom/api/subscriber-manager/uestatus call this route {color}(URL). The scopes required to access the route: [subscribers:write]","metadata":\{"node_name":"ucc-ccda","namespace":"cnom","pod_name":"eric-cn audit","subject":"sec_admin","resp_code":403,"resp_message":403}}
```

from the diagram, we could see customer used **sec\_admin** user which didnot have the right to perform the activity.

subscriber management is under cloud native network runner. In UCC 1.1 II, here is the information about network runner user:

Network Runner Application does not have a default user, and a new user must be created via CNOM Application. The predefined roles for Network Runner described

Role	Description
ENTERPRISE_ADMINISTRATOR	The ENTERPRISE_ADMINISTRATOR role is specially added for enterprise users. A user with the ENTERPRISE_ADMINISTRATOR role has unrestricted access to all features and services.
ENTERPRISE_OPERATOR	The ENTERPRISE_OPERATOR role is specially added for enterprise users. A user with the ENTERPRISE_OPERATOR role has read-only privileges.
ENTERPRISE_SECURITY_ADMIN	The ENTERPRISE_SECURITY_ADMIN role is specially added for enterprise users. A user with the ENTERPRISE_SECURITY_ADMIN role can add, edit, and delete security-related configurations.

\*\*

Could you access cnom gui with network runner user and check if you are able to perform subscriber management?

Thanks,

BR/Zhigang

[UCC\_PLM-260] [UCC MELA: UCC CNOM and Network Runner - expose the FM/PM service for Zabbix integration](#) Created: 2025-07-16 Updated: 2025-07-16 Resolved: 2025-07-16

Status:	Rejected
Project:	<a href="#">UCC_PLM</a>
Component/s:	None
Affects Version/s:	<a href="#">UCC Appliance 1.0.0-rc2</a>
Fix Version/s:	None

Type:	Bug	Priority:	Medium
Reporter:	<a href="#">Rajan Rajeshprasad Gupta</a>	Assignee:	<a href="#">Zhigang Han</a>
Resolution:	Rejected	Votes:	0
Labels:	None		
Remaining Estimate:	Not Specified		
Time Spent:	Not Specified		
Original Estimate:	Not Specified		

Team/s:	UCC_PLM
Found in Build:	UCC 1.1
Requirement Status:	UCC Appliance 0.2.1 - UNCOVERED

#### Description

Hello,

refer to ticket, [UCCSUPPORT-52](#) UCC CNOM and Network Runner - expose the FM/PM service for Zabbix integration - eTeamProject Alpha

There is a request to open UCC CNOM towards the third-party alarm monitoring server, Zabbix. Based on my understanding of UCC and CNOM, this functionality is currently not supported. Feedback has been provided accordingly

I would like to double check

1. Is there any plan to do such integration in roadmap?

2. Is understanding correct or we have some backdoor available to support colleagues during POC/Trial.

#### Comments

Comment by [Zhigang Han](#) [2025-07-16]

Hi Rajan,

We do not support the integration of UCC CNOM to the third party Zabbix. And also there is no roadmap to support this integration at this point. Customer could open a feature request.

Thanks,

BR/Zhigang

#### [UCC\_PLM-259] MANA [ UCC 1.1 GA ] Overheating of HP servers used in UCC

Status:	Rejected
Project:	<a href="#">UCC_PLM</a>
Component/s:	None
Affects Version/s:	<a href="#">UCC Appliance 1.0.1</a>
Fix Version/s:	None

Type:	Bug	Priority:	Medium
Reporter:	<a href="#">Rajan Rajeshprasad Gupta</a>	Assignee:	<a href="#">Reema Sidhwani</a>
Resolution:	Rejected	Votes:	0
Labels:	None		
Remaining Estimate:	Not Specified		
Time Spent:	Not Specified		
Original Estimate:	Not Specified		

Attachments:	Auto-reboot-overheating-ccda_20250709_0921.txt
Found in Build:	<a href="#">UCC 1.1</a>
Requirement Status:	UCC Appliance 0.2.1 - UNCOVERED

#### Description

Hello,

There is feedback from colleagues from MANA.

Now and then as temperature has increased in US.

UCC HP servers are unable to tolerate increases in temperatures and outdoor keeping of UCC is not feasible which may block one of the tactical use-cases of UCC.

HP server reboots frequently and alarms are logged into HP ILO:

```
/system1/log1/record189
```

```
Targets
```

```
Properties
```

```
number=189
```

```
severity=Critical
```

```
date=07/08/2025
```

```
time=22:01:19
description=Automatic Operating System Shutdown Initiated Due to Overheat Condition
Verbs
cd version exit show
```

Please assist in exploring potential airflow management solutions within the UCC cabinet to prevent HP servers from rebooting.

## Comments

Comment by [Zhigang Han](#) [ 2025-07-15 ]

Hi Rajan,

We are rejecting the ticket. Currently we don't support outdoor high temperature situation.

Thanks,

BR/Zhigang

Comment by [Zhigang Han](#) [ 2025-07-10 ]

hi Rajan,

Here is the information of the alarm and action from HPE support:

Automatic Operating System Shutdown Initiated Due to Overheat Condition...

...Fatal Exception (Number X, Cause)

**Event Type:** Overheating condition

**Action:** Check fans. Also, be sure the server is properly ventilated and the room temperature is set within the required range.

The room temperature within the required range cannot be 43 Celsius degree. We are checking internally now and will update you as soon as possible.

Thanks,

BR/Zhigang

Comment by [Rajan Rajeshprasad Gupta](#) [ 2025-07-10 ]

Hello Sam,

Temperature 43. Attached ILO logs.[Auto-reboot-overheating-ccda\\_20250709\\_0921.txt](#)

```
/system1/log1/record135
Targets
Properties
number=135
severity=Repaired
date=07/08/2025
time=20:13:18
description=System Overheating (Temperature Sensor 1, Location Ambient, Temperature 43)
Verbs
cd version exit show

/system1/log1/record136
Targets
Properties
number=136
severity=Repaired
date=07/08/2025
time=20:13:18
description=Automatic Operating System Shutdown Initiated Due to Overheat Condition
Verbs
cd version exit show
```

```
/system1/log1/record137
Targets
Properties
number=137
severity=Informational
date=07/08/2025
time=20:13:21
description=Automatic Operating System Shutdown Due to Overheat Aborted
```

Verbs  
cd version exit show

Comment by [Zhigang Han](#) [ 2025-07-10 ]

Hi Rajan,

Here is the answer:

what temperature it was where the error showed up?

Thanks,

BR/Zhigang

**[UCC\_PLM-258] MANA Tmo [ UCC 1.1 GA ] After power on UCC servers, serverb ILO complaints "Failed to start containerd container runtime"** Created: 2025-07-09 Updated: 2025-07-15 Resolved: 2025-07-15

Status:	Done
Project:	<a href="#">UCC_PLM</a>
Component/s:	None
Affects Version/s:	<a href="#">UCC Appliance 1.0.1</a>
Fix Version/s:	None

Type:	Bug	Priority:	Medium
Reporter:	<a href="#">Rajan Rajeshprasad Gupta</a>	Assignee:	<a href="#">Zhigang Han</a>
Resolution:	Closed	Votes:	0
Labels:	None		
Remaining Estimate:	Not Specified		
Time Spent:	Not Specified		
Original Estimate:	Not Specified		

Attachments:	<a href="#">ccdb_all_ilog_logs.txt</a> <a href="#">ccdb_fsck.txt</a> <a href="#">ccdb_logs_20250709-1.txt</a> <a href="#">ccdb_logs_20250709.txt</a> <a href="#">ccdb_power_on.txt</a> <a href="#">ccdb_reboot_panic.tar.gz</a> <a href="#">ilo_logs_20250709.zip</a> <a href="#">image-2025-07-09-10-04-55-915.png</a> <a href="#">image-2025-07-09-14-19-31-475.png</a> <a href="#">image-2025-07-10-12-22-39-027.png</a> <a href="#">journalctl_containerd-1.txt</a> <a href="#">journalctl_containerd.txt</a> <a href="#">ovs_logs.zip</a> <a href="#">Tmo-ucc-1.jfif</a> <a href="#">Tmo-ucc-2-1.jfif</a> <a href="#">Tmo-ucc-2.jfif</a> <a href="#">Tmo-ucc-3.jfif</a> <a href="#">Tmo-ucc-3-1.jfif</a> <a href="#">Tmo-ucc-4.jfif</a> <a href="#">Tmo-ucc-5.jfif</a>
Found in Build:	UCC 1.1
Requirement Status:	UCC Appliance 0.2.1 - UNCOVERED

#### Description

Hello,

Upon powering on the UCC server, the iLO interface indicates a failure to start the containerd container runtime.

To provide logs for see bahviour, an SSH connection to the iLO is established, and the logs are collected for ticket analysis.

```
</>hpiLO-> power on
--
--

[ 59.020080] cloud-init[8737]: Unused interfaces below are shut down.
[ 59.036087] cloud-init[8737]: ['enp134s1f2', 'enp134s1f3', 'enp134s1f4', 'enp134s1f5', 'ens1f2', 'ens1f3', 'ens1f4', 'ens1f5', 'ens22f0', 'ens22f1', 'ens22f2', 'ens22f3']
[ 59.060130] cloud-init[8737]: Cloud-init v. 23.3-150100.8.85.4 running 'modules:final' at Tue, 08 Jul 2025 20:40:59 +0000. Up 56.42 seconds.
[ 59.084065] cloud-init[8737]: Cloud-init v. 23.3-150100.8.85.4 finished at Tue, 08 Jul 2025 20:41:01 +0000. Datasource DataSourceConfigDrive [net,ver=2]
[source=/dev/nvme2n1p5]. Up 58.76 seconds
```

```
[FAILED] Failed to start containerd container runtime.  
See 'systemctl status containerd.service' for details.
```

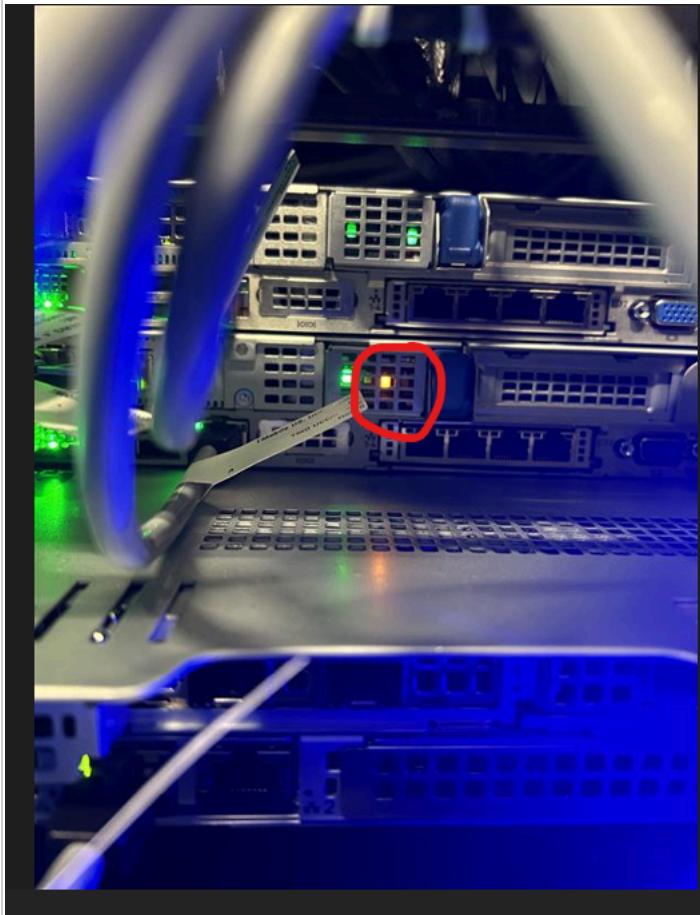
ILO is complaints, too many errors for Slot 7:

```
/map1/log1/record61  
Targets  
Properties  
  number=61  
  severity=Caution  
  date=07/08/2025  
  time=23:50:36  
  description=The iLO health monitoring status of the device / adapter located in Slot 7 is not responsive.  
Verbs  
  cd version exit show
```

Slot\_7 is used for NVMe. However, I am not sure if this is due to hardware failure or due to loose connection or any other reasons.

```
/system1/slot7  
Targets  
Properties  
  type=Other(37)  
  width=4x  
  name=NVMe Slot 26  
Verbs  
  cd version exit show
```

Physically, colleagues see physical LED as below.



I have requested to collect more information about journalctl.

Also requested to check by restarting containerd, Will update more as get information.

Question.

1. Is this known issue already observed?
2. Are there any additional logs or methods that can help determine whether this issue is caused by hardware failure, driver problems, or other factors?

attached ilo logs.

[ccdb\\_power\\_on.txt](#)

[ccdb\\_all\\_ilos\\_logs.txt](#)

## Comments

Comment by Zhigang Han [ 2025-07-15 ]

Hi team,

The main reason of containerD failure is the error line:

Jul 08 13:41:23 ucc-ccdb containerd[11256]: time="2025-07-08T13:41:23.852941711-07:00" level=fatal msg="Failed to run CRI service" error="failed to recover state: failed to

We do find the similar issue from this link:

containerd fails on start: "failed to get metadata for stored sandbox" · Issue #10848 · containerd/containerd

The solution is to clean up /var/lib/containerd directory which is the solution from Rajan's suggested below.

we might have the fix from ccd for this kind of issue from later version. right now for ccd 2.31, we could use the workaround to fix containerd failure issue.

Thanks,

BR/Zhigang

Comment by Rajan Rajeshprasad Gupta [ 2025-07-15 ]

## Received feedback:

3 reboots of ccdb, and it came up every time.

Root cause of problem is not clear "why problem actually happen"

Work-around which fix problem as below:

```
sudo systemctl stop containerd  
sudo rm -rf /var/lib/containerd/*  
sudo systemctl start containerd
```

I think, lets close as fix available with work-around, without root-cause or suggest

Comment by Rajan Rajeshprasad Gupta [ 2025-07-11 ]

## Update received

After doing containerd cleanup and restart, ccd and cnf has come up

However after reboot of server is resulting into lot of error.

Please see as below:

```
Jul 09 16:22:52 ucc-ccdb containerd[11062]: time="2025-07-09T16:22:52.298531867-07:00" level=warning msg="Ignoring unknown key in TOML for plugin" error="strict mode"
Jul 09 16:22:52 ucc-ccdb containerd[11062]: time="2025-07-09T16:22:52.298540020-07:00" level=warning msg="Ignoring unknown key in TOML for plugin" error="strict mode"
Jul 09 16:22:52 ucc-ccdb containerd[11062]: time="2025-07-09T16:22:52.359784631-07:00" level=error msg="failed to recover sandbox state" error="unable to find sandbox"
Jul 09 16:22:52 ucc-ccdb containerd[11062]: time="2025-07-09T16:22:52.360032565-07:00" level=error msg="failed to recover sandbox state" error="unable to find sandbox"
Jul 09 16:22:52 ucc-ccdb containerd[11062]: time="2025-07-09T16:22:52.360154889-07:00" level=error msg="failed to recover sandbox state" error="unable to find sandbox"
Jul 09 16:22:52 ucc-ccdb containerd[11062]: time="2025-07-09T16:22:52.360420329-07:00" level=fatal msg="Failed to run CRI service" error="failed to recover state: failed to start containerd container runtime."
Jul 09 16:22:52 ucc-ccdb systemd[1]: containerd.service: Main process exited, code=exited, status=1/FAILURE
Jul 09 16:22:52 ucc-ccdb systemd[1]: containerd.service: Failed with result 'exit-code'.
Jul 09 16:22:52 ucc-ccdb systemd[1]: Failed to start containerd container runtime.
Jul 09 16:22:55 ucc-ccdb sudo[11218]:      ecdc : TTY=pts/0 ; PWD=/home/eccd ; USER=root ; COMMAND=/usr/bin/systemctl status containerd
Jul 09 16:22:55 ucc-ccdb sudo[11218]: pam_unix(sudo:session): session opened for user root by ecdc(uid=1001)
Jul 09 16:22:57 ucc-ccdb systemd[1]: containerd.service: Scheduled restart job, restart counter is at 5.
Jul 09 16:22:57 ucc-ccdb systemd[1]: Starting containerd container runtime...
Jul 09 16:22:57 ucc-ccdb containerd[11224]: time="2025-07-09T16:22:57.460362868-07:00" level=warning msg="Configuration migrated from version 2, use `containerd config` to migrate to version 3"
Jul 09 16:22:57 ucc-ccdb containerd[11224]: time="2025-07-09T16:22:57.524757821-07:00" level=warning msg="Ignoring unknown key in TOML for plugin" error="strict mode"
Jul 09 16:22:57 ucc-ccdb containerd[11224]: time="2025-07-09T16:22:57.524803069-07:00" level=warning msg="Ignoring unknown key in TOML for plugin" error="strict mode"
Jul 09 16:22:57 ucc-ccdb containerd[11224]: time="2025-07-09T16:22:57.524813895-07:00" level=warning msg="Ignoring unknown key in TOML for plugin" error="strict mode"
Jul 09 16:22:57 ucc-ccdb containerd[11224]: time="2025-07-09T16:22:57.524822538-07:00" level=warning msg="Ignoring unknown key in TOML for plugin" error="strict mode"
Jul 09 16:22:57 ucc-ccdb containerd[11224]: time="2025-07-09T16:22:57.524831342-07:00" level=warning msg="Ignoring unknown key in TOML for plugin" error="strict mode"
Jul 09 16:22:57 ucc-ccdb containerd[11224]: time="2025-07-09T16:22:57.524839484-07:00" level=warning msg="Ignoring unknown key in TOML for plugin" error="strict mode"
Jul 09 16:22:57 ucc-ccdb containerd[11224]: time="2025-07-09T16:22:57.524847656-07:00" level=warning msg="Ignoring unknown key in TOML for plugin" error="strict mode"
Jul 09 16:22:57 ucc-ccdb containerd[11224]: time="2025-07-09T16:22:57.52485678-07:00" level=warning msg="Ignoring unknown key in TOML for plugin" error="strict mode"
Jul 09 16:22:57 ucc-ccdb containerd[11224]: time="2025-07-09T16:22:57.524903201-07:00" level=warning msg="Ignoring unknown key in TOML for plugin" error="strict mode"
```

By looking logs , It looks like The logs show that containerd cannot start due to missing or corrupted sandbox metadata, causing kubelet to fail connecting.

Could you please consult with a CCD expert to identify the root cause of the issue and advise on recovery steps? The next few reboots may cause the CCD service to crash.

Also received email from team-mate from MANA, HP support has responded there is no issue with hardware in their analysis.

ccdb reboot panic.tar.gz

---

Comment by [Zhigang Han](#) [ 2025-07-10 ]

Hi Rajan,

from the last log, I could see this is the last slot 7 error message:

```
/map1/log1/record238
Targets
Properties
number=238
severity=Caution
date=07/09/2025
time=01:35:34
description=The iLO health monitoring status of the device / adapter located in Slot 7 is not responsive.
Verbs
cd version exit show
```

after record 238, this error message is gone:

from next log message record 239, there is poweroff

```
/map1/log1/record239
Targets
Properties
number=239
severity=Caution
date=07/09/2025
time=01:35:34
description=Power-Off signal sent to host server by: ericsson.
Verbs
cd version exit show
```

Here is the question:

is amber LED gone after the poweroff signal or before the poweroff signal?

Thanks,

BR/Zhigang

---

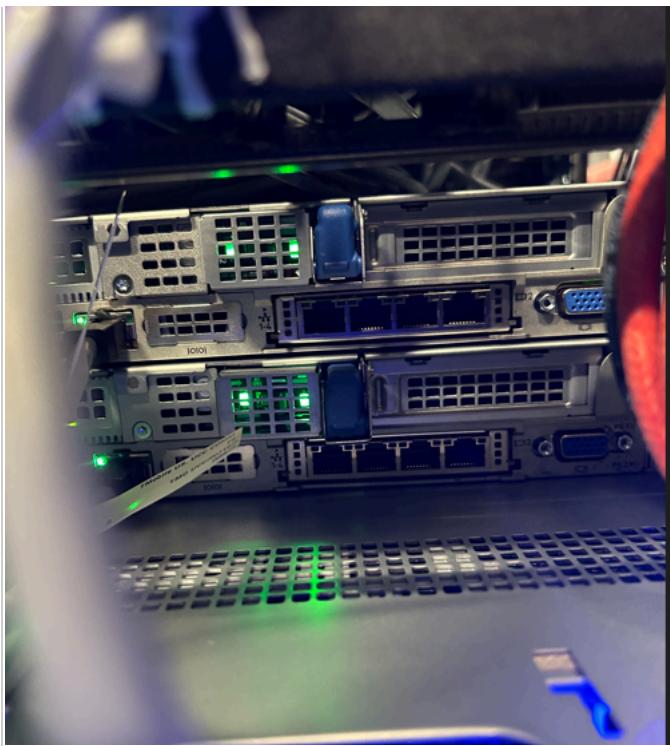
Comment by [Rajan Rajeshprasad Gupta](#) [ 2025-07-10 ]

Hello Sam,

Feedback received.

After some time, we dont see "amber LED" anymore. So there is no hardware failure physically visible.

Refer attached new photos shared.



[Tmo-ucc-1.jif](#)

[Tmo-ucc-2.jif](#)

[Tmo-ucc-3.jif](#)

attached logs.

[ccdb\\_fsck.txt](#)

[journalctl\\_containerd.txt](#)

[ccdb\\_logs\\_20250709.txt](#)

containerd restart didnt worked.

```
sudo systemctl restart containerd
```

there was fsck errors reported and cleanup is done you can find in fsck.txt.

It seems some data is corrupted for ccd and due to which containerd is not coming up and always in starting mode. It can be seen from journalctl logs.

other requested logs available as above.

Next step:

I am planning to share containerd cleanup and restart.

```
sudo systemctl stop containerd
sudo rm -rf /var/lib/containerd/*
sudo systemctl start containerd
```

Please suggest if you can find good solution and reason for failure.

ILO logs.

[ilo\\_logs\\_20250709.zip](#)

Comment by [Zhigang Han](#) [ 2025-07-09 ]

Hi Rajan,

As we discussed, please collect the logs from HP server B and at the same time, please raise HP support to fix the amber light issue in case there is a need to replace the fau

Here is the HPE support link:

[HPE ProLiant DL325 Gen11 | Product Support|[https://support.hpe.com/connect/s/product?language=en\\_US&kmpmoid=1014689141&tab=manuals&manualsFilter=66000](https://support.hpe.com/connect/s/product?language=en_US&kmpmoid=1014689141&tab=manuals&manualsFilter=66000)

on-site engineer could use ILO gui and the link above to identify if the server is facing hardware issues or not.

from ILO gui, we could find two logs:

1, IML integrated management log

2, ilo event log

we also check three locations from gui:

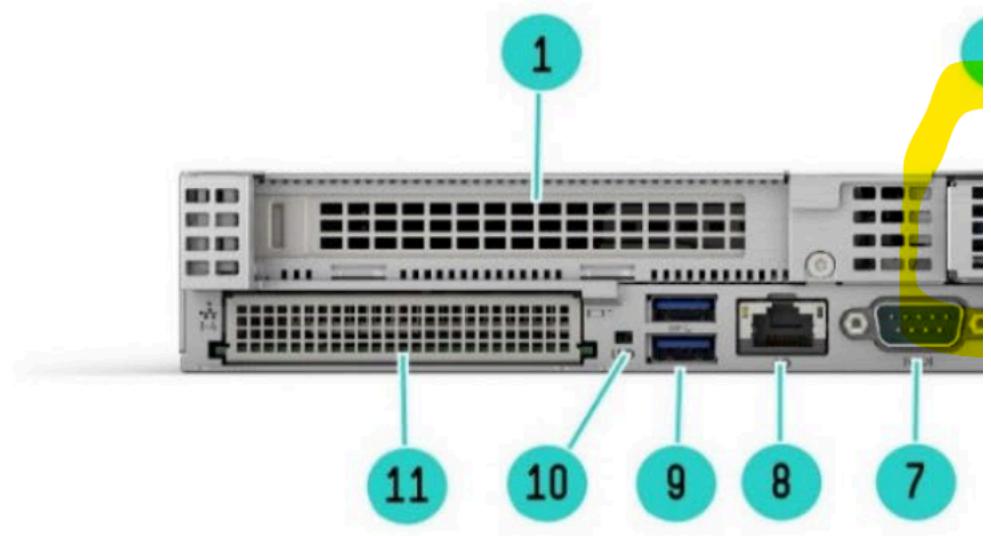
1, overview dashboard shows green, amber, and red light

2, system health --> summary

3, system health --> sensors or subcomponents

## QuickSpecs

### Overview



### Rear View

1. Slot 1 Primary PCIe 5.0 Riser
2. Optional NS204i-u hot-plug NVMe boot device
3. Slot 2 Secondary PCIe 5.0 Riser<sup>1</sup>
4. Hot-plug Power Supply 1 and 2<sup>2</sup>
5. Video (VGA) port
6. OCP 3.0 Slot 22

comparing with the picture attached, it looks like number 2 nvme boot device is having the issue.

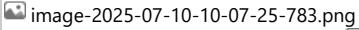
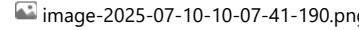
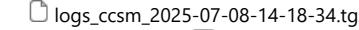
From the analysis above, slot 7 is related to nvme

/map1/log1/record61

Targets

Properties

number=61  
 severity=Caution  
 date=07/08/2025  
 time=23:50:36  
 description=The iLO health monitoring status of the device / adapter located in Slot 7 is not responsive.  
 Verbs  
 cd version exit sho  
 Thanks,  
 BR/Zhigang

[UCC_PLM-257] MANA Tmo [ UCC 1.1 GA ] After power on UCC servers, PCX and CCSM pods didnt came up					Created: 2025-07-09 Updated: 2025-07-14 Resolved: 2025-07-14																																																																																																																		
Status:	Done																																																																																																																						
Project:	UCC_PLM																																																																																																																						
Component/s:	None																																																																																																																						
Affects Version/s:	UCC Appliance 1.0.1																																																																																																																						
Fix Version/s:	None																																																																																																																						
Type:	Bug	Priority:	High																																																																																																																				
Reporter:	Rajan Rajeshprasad Gupta	Assignee:	Alexander Malikov																																																																																																																				
Resolution:	Closed	Votes:	0																																																																																																																				
Labels:	None																																																																																																																						
Remaining Estimate:	Not Specified																																																																																																																						
Time Spent:	Not Specified																																																																																																																						
Original Estimate:	Not Specified																																																																																																																						
Attachments:	     																																																																																																																						
Team/s:	UCC_XFT2																																																																																																																						
Found in Build:	UCC 1.1																																																																																																																						
Requirement Status:	UCC Appliance 0.2.1 - UNCOVERED																																																																																																																						
Description																																																																																																																							
Hello, Tmo ucc was powered off (after prestaging) : 2025-06-13 Tmo ucc was powered on (on customer location) : 2025-07-08 ServerA: After power on UCC servers, PCX and CCSM pods didnt came up properly. PCX:																																																																																																																							
<table border="1"> <thead> <tr> <th>NAME</th><th>READY</th><th>STATUS</th><th>RESTARTS</th><th>AGE</th></tr> </thead> <tbody> <tr><td>eric-cm-mediator-db-pg-0</td><td>2/2</td><td>Running</td><td>52 (47s ago)</td><td>26d</td></tr> <tr><td>eric-ctrl-bro-0</td><td>0/1</td><td>Running</td><td>18 (6m31s ago)</td><td>142m</td></tr> <tr><td>eric-data-coordinator-zk-0</td><td>1/1</td><td>Running</td><td>0</td><td>26d</td></tr> <tr><td>eric-data-distributed-coordinator-ed-0</td><td>1/1</td><td>Running</td><td>0</td><td>26d</td></tr> <tr><td>eric-data-message-bus-kf-0</td><td>0/1</td><td>Init:0/1</td><td>0</td><td>142m</td></tr> <tr><td>eric-data-object-storage-mn-0</td><td>0/2</td><td>Init:0/1</td><td>21 (2m45s ago)</td><td>142m</td></tr> <tr><td>eric-data-search-engine-data-0</td><td>1/3</td><td>Running</td><td>2 (41m ago)</td><td>142m</td></tr> <tr><td>eric-data-search-engine-master-0</td><td>1/3</td><td>Running</td><td>10 (7m7s ago)</td><td>142m</td></tr> <tr><td>eric-fh-alarm-handler-db-pg-0</td><td>2/2</td><td>Running</td><td>52 (49s ago)</td><td>26d</td></tr> <tr><td>eric-lm-combined-server-db-pg-0</td><td>2/2</td><td>Running</td><td>52 (25s ago)</td><td>26d</td></tr> <tr><td>eric-log-shipper-nxqzb</td><td>1/2</td><td>Running</td><td>9 (7m13s ago)</td><td>142m</td></tr> <tr><td>eric-mesh-controller-6bb4499545-19ck7</td><td>1/1</td><td>Running</td><td>0</td><td>26d</td></tr> <tr><td>eric-odca-isp-event-monitor-db-pg-0</td><td>1/2</td><td>CrashLoopBackOff</td><td>53 (91s ago)</td><td>162m</td></tr> <tr><td>eric-pcf-dms-1-admin-mgr-0</td><td>2/2</td><td>Running</td><td>0</td><td>26d</td></tr> <tr><td>eric-pcf-dms-1-locator-0</td><td>4/4</td><td>Running</td><td>0</td><td>26d</td></tr> <tr><td>eric-pcf-dms-1-server-0</td><td>3/3</td><td>Running</td><td>0</td><td>26d</td></tr> <tr><td>eric-pcf-kvdb-supervisor-0</td><td>0/4</td><td>Init:CrashLoopBackOff</td><td>32 (77s ago)</td><td>142m</td></tr> <tr><td>eric-pm-server-0</td><td>3/4</td><td>CrashLoopBackOff</td><td>31 (3m39s ago)</td><td>142m</td></tr> <tr><td>eric-sec-access-mgmt-0</td><td>0/1</td><td>Init:0/1</td><td>0</td><td>142m</td></tr> <tr><td>eric-sec-access-mgmt-account-manager-29199300-798q9</td><td>1/1</td><td>Running</td><td>0</td><td>62m</td></tr> <tr><td>eric-sec-access-mgmt-account-manager-29199300-r18gg</td><td>0/1</td><td>Error</td><td>0</td><td>129m</td></tr> <tr><td>eric-sec-access-mgmt-account-manager-29199300-r5wifh</td><td>0/1</td><td>Unknown</td><td>0</td><td>2h17m</td></tr> </tbody> </table>					NAME	READY	STATUS	RESTARTS	AGE	eric-cm-mediator-db-pg-0	2/2	Running	52 (47s ago)	26d	eric-ctrl-bro-0	0/1	Running	18 (6m31s ago)	142m	eric-data-coordinator-zk-0	1/1	Running	0	26d	eric-data-distributed-coordinator-ed-0	1/1	Running	0	26d	eric-data-message-bus-kf-0	0/1	Init:0/1	0	142m	eric-data-object-storage-mn-0	0/2	Init:0/1	21 (2m45s ago)	142m	eric-data-search-engine-data-0	1/3	Running	2 (41m ago)	142m	eric-data-search-engine-master-0	1/3	Running	10 (7m7s ago)	142m	eric-fh-alarm-handler-db-pg-0	2/2	Running	52 (49s ago)	26d	eric-lm-combined-server-db-pg-0	2/2	Running	52 (25s ago)	26d	eric-log-shipper-nxqzb	1/2	Running	9 (7m13s ago)	142m	eric-mesh-controller-6bb4499545-19ck7	1/1	Running	0	26d	eric-odca-isp-event-monitor-db-pg-0	1/2	CrashLoopBackOff	53 (91s ago)	162m	eric-pcf-dms-1-admin-mgr-0	2/2	Running	0	26d	eric-pcf-dms-1-locator-0	4/4	Running	0	26d	eric-pcf-dms-1-server-0	3/3	Running	0	26d	eric-pcf-kvdb-supervisor-0	0/4	Init:CrashLoopBackOff	32 (77s ago)	142m	eric-pm-server-0	3/4	CrashLoopBackOff	31 (3m39s ago)	142m	eric-sec-access-mgmt-0	0/1	Init:0/1	0	142m	eric-sec-access-mgmt-account-manager-29199300-798q9	1/1	Running	0	62m	eric-sec-access-mgmt-account-manager-29199300-r18gg	0/1	Error	0	129m	eric-sec-access-mgmt-account-manager-29199300-r5wifh	0/1	Unknown	0	2h17m
NAME	READY	STATUS	RESTARTS	AGE																																																																																																																			
eric-cm-mediator-db-pg-0	2/2	Running	52 (47s ago)	26d																																																																																																																			
eric-ctrl-bro-0	0/1	Running	18 (6m31s ago)	142m																																																																																																																			
eric-data-coordinator-zk-0	1/1	Running	0	26d																																																																																																																			
eric-data-distributed-coordinator-ed-0	1/1	Running	0	26d																																																																																																																			
eric-data-message-bus-kf-0	0/1	Init:0/1	0	142m																																																																																																																			
eric-data-object-storage-mn-0	0/2	Init:0/1	21 (2m45s ago)	142m																																																																																																																			
eric-data-search-engine-data-0	1/3	Running	2 (41m ago)	142m																																																																																																																			
eric-data-search-engine-master-0	1/3	Running	10 (7m7s ago)	142m																																																																																																																			
eric-fh-alarm-handler-db-pg-0	2/2	Running	52 (49s ago)	26d																																																																																																																			
eric-lm-combined-server-db-pg-0	2/2	Running	52 (25s ago)	26d																																																																																																																			
eric-log-shipper-nxqzb	1/2	Running	9 (7m13s ago)	142m																																																																																																																			
eric-mesh-controller-6bb4499545-19ck7	1/1	Running	0	26d																																																																																																																			
eric-odca-isp-event-monitor-db-pg-0	1/2	CrashLoopBackOff	53 (91s ago)	162m																																																																																																																			
eric-pcf-dms-1-admin-mgr-0	2/2	Running	0	26d																																																																																																																			
eric-pcf-dms-1-locator-0	4/4	Running	0	26d																																																																																																																			
eric-pcf-dms-1-server-0	3/3	Running	0	26d																																																																																																																			
eric-pcf-kvdb-supervisor-0	0/4	Init:CrashLoopBackOff	32 (77s ago)	142m																																																																																																																			
eric-pm-server-0	3/4	CrashLoopBackOff	31 (3m39s ago)	142m																																																																																																																			
eric-sec-access-mgmt-0	0/1	Init:0/1	0	142m																																																																																																																			
eric-sec-access-mgmt-account-manager-29199300-798q9	1/1	Running	0	62m																																																																																																																			
eric-sec-access-mgmt-account-manager-29199300-r18gg	0/1	Error	0	129m																																																																																																																			
eric-sec-access-mgmt-account-manager-29199300-r5wifh	0/1	Unknown	0	2h17m																																																																																																																			

CCSM:

NAME	READY	STATUS	RESTARTS	AGE
eric-cm-mediator-key-init-4xmqn	0/1	Completed	0	26d
eric-ctrl-bro-0	1/1	Running	0	26d
eric-data-coordinator-zk-0	1/1	Running	0	26d
eric-data-distributed-coordinator-ed-0	1/1	Running	0	26d
eric-data-document-database-pg-0	1/2	Running	22 (29s ago)	158m
eric-data-document-database-pg-ah-0	1/2	Running	24 (3m59s ago)	158m
eric-data-document-database-pg-lm-0	1/2	Running	24 (4m ago)	158m
eric-data-message-bus-kf-0	0/2	Init:0/1	0	158m
eric-data-object-storage-mn-0	0/2	Init:0/1	23 (6m13s ago)	158m
eric-data-search-engine-data-0	1/3	Running	3 (8m23s ago)	158m
eric-data-search-engine-master-0	1/3	Running	12 (7m8s ago)	158m
eric-ingressgw-ausf-traffic-g7xzm	1/1	Running	0	26d
eric-ingressgw-epc-soap-traffic-5z5fs	1/1	Running	0	26d
eric-ingressgw-hss-epc-traffic-8d5tb	1/1	Running	0	26d
eric-ingressgw-udm-traffic-f9zvw	1/1	Running	0	26d
eric-log-shipper-fw8cp	1/1	Running	0	26d
eric-mesh-controller-864cc458b4-mkxgw	1/1	Running	0	26d
eric-nrf-agent-init-cm-tqwzg	0/1	Completed	0	26d
eric-nrf-agent-pm-job-loader-ppqgj	0/1	Completed	0	26d
eric-pm-server-0	3/4	CrashLoopBackOff	36 (3m22s ago)	159m
eric-sec-key-management-job-92wfh	0/1	Completed	0	26d
eric-sec-key-management-wini-0	0/2	Init:0/2	10 (6m15s ago)	158m

Initial observation indicate, ADP pods like eric-odca-isp-event-monitor-db-pg-0, eric-pm-server-0 etc are complaining for certificate verification/ missing certificate.

See below:

eric-odca-isp-event-monitor-db-pg-0\_eric-odca-isp-event-monitor-db-pg

```
{"version": "1.2.0", "timestamp": "2025-07-08T14:18:07.808-07:00", "severity": "INFO", "service_id": "eric-odca-isp-event-monitor-db-pg", "message": "catch psycopg2.Error: connection failed: SSL error: certificate verify failed", "metadata": {"container_name": "eric-odca-isp-event-monitor-db-pg"}, "extra_data": {"file": "__init__.py", "line": "438"}}
```

eric-pm-server-0\_eric-pm-exporter

```
{"version": "1.0.0", "timestamp": "2025-07-08T11:54:26.363-07:00", "severity": "error", "service_id": "eric-pm-server", "message": "http: TLS handshake error from [::1]:52260: tls: no certificates configured", "metadata": {"container_name": "eric-pm-exporter", "pod_name": "eric-pm-server-0", "namespace": "ep5g"}}
```

application pods like eric-pcf-dms-1-locator-0\_eric-pcf-dms-1-locator-monitor are failed due to dependency on other ADP pods to come up and not all application pods are started by itself.

Question1: How does after power on certificates are missing for ADP pods?

Question2: Is this known issue in UCC 1.1?

attached adp logs.

[logs\\_ep5g\\_2025-07-08-14-14-40.tgz](#)

[logs\\_ccsm\\_2025-07-08-14-18-34.tgz](#)

#### Comments

Comment by [Zhigang Han](#) [2025-07-14]

Hi Rajan,

As we discussed from the team, We will close the ticket.

Thanks,

BR/Zhigang

Comment by Rajan Rajeshprasad Gupta [ 2025-07-14 ]

Thanks Alex.

I confirm that I can see the steps clearly outlined in the new installation guide and that it is well-structured

Comment by Alexander Malikov [ 2025-07-14 ]

Hello Rajan Rajeshprasad Gupta,

I added following instructions to update reboot workaround script into the installation guide. Please confirm that solution is acceptable:



Best regards,

Alex

Comment by Zhigang Han [ 2025-07-11 ]

Hi Alex,

There is a procedure which has been tested by Rajan. Could you check the fix from the design side? We need to update the installation instruction in CPI.

Thanks,

BR/Zhigang

Comment by Rajan Rajeshprasad Gupta [ 2025-07-10 ]

Team, Tested and Feedback Received:

Option2 by changing parameter in reboot-workaround script and ccd reboot.

Sharing steps:

1. find location of workaround script in ccd

```
find / -type f -name ucc-reboot-workaround.sh 2>/dev/null2
```

2. edit with vi editor

```
sudo vi /usr/local/bin/ucc-reboot-workaround.sh
```

3. Change POD\_COUNT\_FOR\_SCALE\_OUT to 25 (originally 15) and save it.

```
#!/bin/bash

#script version: 1.0.1
#Revision Info
# - monitoring loop after ep5g scale-out
# - changed POD_COUNT_FOR_SCALE_OUT from 10 to 15
# - moved dp pod deletion after ep5g monitoring loop
# - changed the filter of dp pod deletion after ep5g scale out monitoring
# - added date printout at start and stop of script

# print the date+time of reboot script start
date

NAMESPACE="ccsm"
NAMESPACE2="ep5g"
MAX_WAIT_SECONDS=1800
CHECK_INTERVAL=40
POD_COUNT_FOR_SCALE_OUT=15 → 25
MAX_ITERATIONS=3
```

4. reboot UCC CCC

```
sudo reboot
```

wait for pod to come up. It takes normal time as that is taken by UCC server to power on.

Next step:

As discussed during call with colleagues, Please go ahead to update CPI installation guide and Troubleshooting document to avoid issues for UCC project deliveries.

Comment by Rajan Rajeshprasad Gupta [ 2025-07-09 ]

Update:

Based on feedback on email for reported issue in InV.

attached MOP planned to be executed for Tmo.

will share feedback after execution.

MOP-UCC\_PLM-257\_MANA Tmo (Manaul PCX and CCSM).txt

[UCC\_PLM-256] MANA Vz [ UCC 1.1 GA ] : Documentation II : Typo in helm software link Created: 2025-07-08 Updated: 2025-07-15 Resolved: 2025-07-15

Status:	Done
Project:	UCC_PLM
Component/s:	None
Affects Version/s:	UCC Appliance 1.0.1-rc1
Fix Version/s:	None

Type:	Bug	Priority:	Low
Reporter:	Rajan Rajeshprasad Gupta	Assignee:	Alexander Malikov
Resolution:	Closed	Votes:	0
Labels:	None		
Remaining Estimate:	Not Specified		
Time Spent:	Not Specified		
Original Estimate:	Not Specified		

Attachments:	
Team/s:	UCC_XFT2
Found in Build:	UCC 1.1
Requirement Status:	UCC Appliance 0.2.1 - UNCOVERED

#### Description

Hello,

It was noticed. Helm 3.17.0 link is incorrect and pointed to 3.13.0.

Please correct.

Product Name	Version	Download Link
Helm	V3.8.1	<a href="https://get.helm.sh/helm-v3.8.1-linux-amd64.tar.gz">helm-v3.8.1-linux-amd64.tar.gz</a>
Helm	V3.11.3	<a href="https://get.helm.sh/helm-v3.11.3-linux-amd64.tar.gz">helm-v3.11.3-linux-amd64.tar.gz</a>
helmfile	0.156.0	<a href="https://get.helm.sh/helm-v3.15.0-linux-amd64.tar.gz">helmfile-0.156.0-linux-amd64.tar.gz</a>
Helm	V3.13.0	<a href="https://get.helm.sh/helm-v3.13.0-linux-amd64.tar.gz">helm-v3.13.0-linux-amd64.tar.gz</a>
Helm	V3.17.0	<a href="https://get.helm.sh/helm-v3.17.0-linux-amd64.tar.gz">helm-v3.17.0-linux-amd64.tar.gz</a>
Helm	V3.16.4	<a href="https://get.helm.sh/helm-v3.16.4-linux-amd64.tar.gz">helm-v3.16.4-linux-amd64.tar.gz</a>

Table 6 3PP software

#### Comments

Comment by Alexander Malikov [ 2025-07-14 ]

Hello Rajan Rajeshprasad Gupta,

Link was updated and fix will be included in the next version of CPI. Please check it.

Best regards,  
Alex

Comment by Zhigang Han [ 2025-07-08 ]

Hi Rajan,

Yes you are right. It is a known issue. I have assigned the ticket to xft2 team. We will update it.

Thanks,  
BR/Zhigang

Comment by [Rajan Rajeshprasad Gupta](#) [ 2025-07-08 ]  
Correct link : <https://get.helm.sh/helm-v3.17.0-linux-amd64.tar.gz>

[UCC\_PLM-255] **MANA Vz [ UCC 1.1 GA ] : SC software is needed although feature\_sm\_sepp=false** Created: 2025-07-08 Updated: 2025-07-09 Resolved: 2025-07-08

Status:	Rejected
Project:	<a href="#">UCC_PLM</a>
Component/s:	None
Affects Version/s:	<a href="#">UCC Appliance 1.1.0</a>
Fix Version/s:	None

Type:	Bug	Priority:	Medium
Reporter:	<a href="#">Rajan Rajeshprasad Gupta</a>	Assignee:	<a href="#">Reema Sidhwani</a>
Resolution:	Rejected	Votes:	0
Labels:	None		
Remaining Estimate:	Not Specified		
Time Spent:	Not Specified		
Original Estimate:	Not Specified		

Attachments:	<a href="#">CNAT_batch_install_20250708093431.log</a>	<a href="#">Image-load issue due to SC software.txt</a>
Team/s:	UCC_PLM	
Found in Build:	UCC 1.1	
Requirement Status:	UCC Appliance 0.2.1 - UNCOVERED	

#### Description

Hello,  
Feedback from colleagues indicates that VZ does not have a value pack for SC, which means they do not have the software available in the Software Gateway.

They have set in CIQ

`feature_sm_sepp false`

however, we still need to download the SC software manually; otherwise, CNAT will not onboard any images for CCDB.

Please help to verify.

#### Comments

Comment by [Soner Mus](#) [ 2025-07-08 ]

Hello [Zhigang Han](#)

Could you please elaborate your request a bit ? - "PLM believes we need to check both parameters (CCPC and SC) in UCC softwares"

The interaction between CNAT, UCC Configuration, and the LLD works as follows:

- Parameters are defined in the LLD-CIQ site-global section as key-value pairs.
- CNAT reads these parameters during processing.
- When rendering Jinja2 templates, CNAT substitutes each key with its corresponding value to generate output files (e.g., JSON, YAML, XML, or plain text). These files are then used during Day0 or Day1 operations.

Please refer to the following diagram for a brief overview.



The problem that is faced is not a CNAT issue, as you may see the related "config/templates/batch/vnf-images-onboard.yaml.jinja2" template is designed to check only the `nodeName=="ccdb"` so it is not checking if the `feature_sm_sepp=="true"` or `feature_sm_sepp=="false"`. So CNAT will try to take action to onboard the SC csar file.

**Existing:**

```
{% if nodeName=="ccdb" %}
- {{ config_dir }}/config/{{ nodeName }}/sc/vnf-images-sepp.yaml
{% endif %}
```

To.be (to remove the exception that you are facing); [Mats Persson](#) and [Alexander Malikov](#) can comment more.

```
{% if nodeName=="ccdb" and feature_sm_sepp=="true" %}
- {{ config_dir }}/config/{{ nodeName }}/sc/vnf-images-sepp.yaml
{% endif %}
```

BR;

Soner

Comment by [Zhigang Han](#) [ 2025-07-08 ]

Hi Rajan,

as we discussed, PLM will reject the ticket. If customer wants the partial deployment, please raise a new requirement ticket.

Thanks,

BR/Zhigang

Comment by [Mats Persson](#) [ 2025-07-08 ]

Yes, regardless of the value pack ordered for UCC, all software components, including CCPC and SC, are available for the customer's target group to download.

..and yes, despite above, if for some reason the SW is not available for customer download, a ticket should be raised to UCC PLM to investigate why that is the case..

Comment by [Rajan Rajeshprasad Gupta](#) [ 2025-07-08 ]

Thank you [Mats Persson](#)

I can see SC ticket in verizon target group.

Question for clarification.

1. Does this mean that regardless of the value pack ordered for UCC, all software components, including CCPC and SC, are available for the customer's target group to download?
2. If any of the software not available for customer download, Ticket should be raised to PLM?

If the answer to both questions is yes, we should document this clearly to inform the CU who assists us with software downloads.

Comment by [Mats Persson](#) [ 2025-07-08 ]

For UCC 1.1 there has been no requirement to only do a partial SW download for SW components related to optional features. UCC 1.1 SW installation assume all SW components must be available for onboarding. The "feature switch" for SEPP is only concerning the actual installation and configuration of mobility functionality. A new requirement needs to be issued to also support the optionality in SW onboarding for SC CNF if SEPP / mobility functionality is not ordered or disabled by the SEPP "feature switch".

However, as the ticket also mentions, customer access to the SC SWGW ticket has not been enabled (for Verizon in this case). This was a mistake and oversight in the UCC 1.1 release activities that just now has been corrected by the UCC Release Mgmt team together with SC PDG.

Comment by [Zhigang Han](#) [ 2025-07-08 ]

Hi Soner,

In UCC 1.1 LLD, we introduce two new parameters:

features		
feature_traffic_management	feature_tm_pcf	true
feature_secure_mobility	feature_sm_sepp	true

PLM believes we need to check both parameters (CCPC and SC) in UCC softwares.

Thanks,

BR/Zhigang

Comment by [Soner Mus](#) [ 2025-07-08 ]

Hello [Rajan Rajeshprasad Gupta](#)

Cnat is executing the statements from the templates. This has to be substituted in the config/templates/batch/vnf-images-onboard.yaml.jinja2 as you also pointed. In case feature\_sm\_sepp=false, statements related to the SC has to be removed, otherwise CNAT will try to execute. From my understanding this is applicable both for Application and Appliance.

Can you comment once more the lines that you will purpose to remove - colors are not visible? , Mats Persson and/or Alexander Malikov may also comment around your suggestion.

Thanks

Comment by Rajan Rajeshprasad Gupta [ 2025-07-08 ]

Hello Soner Mus

Fyi, PFA logs for CNAT simulated issue in PLM lab.

SC Flag in site-global:

```
uccvariant: appliance
uplink_oam_cidr: 214.14.210.67/31
uplink_oam_gateway: 214.14.210.66
uplink_oam_ip_address: 214.14.210.67
oam_cidr: 10.92.238.0/25
external_cidr: 10.92.238.192/27
dns_domainName: deac.ericsson.se
nameserver1: 10.87.5.142
nameserver2: 10.87.5.142
ntp_server1: 10.22.36.5
ntp_server2: 10.22.36.5
timezone: Etc/UTC
emm_ip: 10.237.5.144
emm_snmppv2_ip: 10.237.5.147
feature_tm_pcf: 'true'
feature_sm_sepp: 'false'
```

Image loading failed:

```
2025/07/08 09:34:36 INFO [MainProcess] [vnflcm.install.batch_install:193]: 'cnom-ccdb' is in the installation queue
2025/07/08 09:34:36 INFO [MainProcess] [vnf.vnf.__init__:38]: VNF info file: /home/egptrjn/ucc/deacucc1/ucc1.1.rc2/config/ccdb/sc/vnf-images-sepp.yaml
2025/07/08 09:34:36 DEBUG [MainProcess] [vnf.vnf._load_vnf_info:123]: This is pipeline mode VNF info file, no need upgrade to pipeline.
2025/07/08 09:34:36 DEBUG [MainProcess] [vnf.vnf._load_vnf_info:128]: Loading VNF info file /home/egptrjn/ucc/deacucc1/ucc1.1.rc2/config/ccdb/sc/vnf-images-sepp.yaml
2025/07/08 09:34:36 DEBUG [MainProcess] [utils.misc.load_config_yaml:160]: Yaml file: /home/egptrjn/ucc/deacucc1/ucc1.1.rc2/config/ccdb/sc/vnf-images-sepp.yaml
2025/07/08 09:34:36 ERROR [MainProcess] [utils.misc.validate:151]: Invalid configuration of vnflcm.csar-file: '/data2/software/software_UCC1.1/SC/ERIC-SC-CXP_904_4189_1_R17A_97.csar' is not of type 'file'
2025/07/08 09:34:36 ERROR [MainProcess] [utils.misc.load_config_yaml:185]: Failed to validate the yaml config. The yaml content was:
vnflcm:
  orchestrator: helm
  vnfInstanceName: sc-ccdb
  vnfProductName: Signaling_Controller
  csar-file: /data2/software/software_UCC1.1/SC/ERIC-SC-CXP_904_4189_1_R17A_97.csar
  namespace: sc
  timeout: 3600
  values-file: values.yaml
  helm-binary: helm
  vnfId: ''
  pipeline:
    - module: push-images-to-registry
      cleanup: false
      remote: common
```

attached complete logs for cnat.

[CNAT\\_batch\\_install\\_20250708093431.log](#)

[Image-load issue due to SC software.txt](#)

I think,

we should suggest temporary work-around to modify "vnf-images-onboard.yaml"

Like below, remove highlighted red lines. Is it enough?

```

batch-size: 3

vnf-info-files:
- /home/egptrjn/ucc/deacucc1/ucc1.1.rc2/config/ccdb/ccdm/vnf-images-ccdm.yaml
- /home/egptrjn/ucc/deacucc1/ucc1.1.rc2/config/ccdb/ccsm/vnf-images-ccsm.yaml
- /home/egptrjn/ucc/deacucc1/ucc1.1.rc2/config/ccdb/ccrc/vnf-images-ccrc.yaml
- /home/egptrjn/ucc/deacucc1/ucc1.1.rc2/config/ccdb/pcx/vnf-images-pcc.yaml
- /home/egptrjn/ucc/deacucc1/ucc1.1.rc2/config/ccdb/pcx/vnf-images-pcg.yaml
- /home/egptrjn/ucc/deacucc1/ucc1.1.rc2/config/ccdb/pcx/vnf-images-ccpc.yaml
- /home/egptrjn/ucc/deacucc1/ucc1.1.rc2/config/ccdb/cnom/vnf-images-cnom.yaml
- /home/egptrjn/ucc/deacucc1/ucc1.1.rc2/config/ccdb/sc/vnf-images-sepp.yaml

cfggen-info-files:

```

/home/egptrjn/ucc/deacucc1/ucc1.1.rc2/config/ccdb/ccdm/cfggen.yaml

Comment by [Rajan Rajeshprasad Gupta](#) [ 2025-07-08 ]

Hello Soner Mus

I will have to wait till colleagues from MANA comes back for working today night.

I will try to simulate case in PLM LAB server B & share you cnat logs.

Comment by [Soner Mus](#) [ 2025-07-08 ]

Hello [Rajan Rajeshprasad Gupta](#)

Is it possible to share the problematic scenario cnat log file ?

Our initial suspicion is, config/templates/batch/vnf-images-onboard.yaml.jinja2 file doesn't contains logic for the SC. But after the log file we can proceed more.

Thanks

Comment by [Frank Peveling](#) [ 2025-07-08 ]

Question:

you miss this SW, right?

SC 1.16 T-160852 CXS1010872-1.16.0.zip ERIC-SC-CXP\_904\_4189\_1\_R17A\_97.csar

Why has VZ no access to this SW?

What is the plan?

feature\_sm\_sepp = false, OK, but do you plan to go for a SC at all?

Current deployment way is to have the complete SW available and control features via setting or licenses.

/Frank

[UCC\_PLM-254] MELA Telf [ UCC 1.0 CP1 ] : NSA is not working Created: 2025-07-07 Updated: 2025-07-24 Resolved: 2025-07-24

Status:	Done
Project:	<a href="#">UCC_PLM</a>
Component/s:	None
Affects Version/s:	<a href="#">UCC Appliance 1.0.0-rc1</a>
Fix Version/s:	<a href="#">ucc appliance 1.2.0</a>

Type:	Bug	Priority:	Medium
Reporter:	<a href="#">Rajan Rajeshprasad Gupta</a>	Assignee:	<a href="#">Alvaro Martin</a>
Resolution:	Closed	Votes:	0
Labels:	None		
Remaining Estimate:	Not Specified		
Time Spent:	Not Specified		
Original Estimate:	Not Specified		

Other Assignees:	Quang-Thanh Nguyen
Sprint:	UCC XFT2 Sprint 12
Team/s:	UCC_XFT2

<b>Found in Build:</b>	UCC 1.0 CP1
<b>Requirement Status:</b>	UCC Appliance 0.2.1 - UNCOVERED

#### Description

Hello,

Refer ticket [UCCSUPPORT-49](#) NSA is not working - eTeamProject Alpha

#### Summary:

real gNB is not allowing split bearer userplane (5G NSA) for qci=5, as qci 5 is dedicated for ims signaling.

UCC has default configuration for 4G in HSS as below which Indicated qci=5 is used for data-service:

```
hssepc eps-apn-configuration 11
apn-name internet
ambr-max-dl 41943040
ambr-max-dl-ext 400000000
ambr-max-ul 20971520
ambr-max-ul-ext 400000000
apn-oi-replacement mmc010.mcc315.gprs
can-be-deleted true
bearer-charging-chars 1
pdn-type ipv4
qos-profile-arp 1
qos-profile-arp-preemption-capability disabled
qos-profile-arp-preemption-vulnerability disabled
qos-profile-qci 5
vp1mn-allowed false
iwk5gs-indicator subscribed
```

This is not correct and can create issues for customers who do not do qci=5 configuration on radio for split bearer.

as qci=5 is dedicated for ims signalling and not used for data-services.

Recommendation to use in UCC. qci=9 and arp=2 for data/5g nsa.

```
hssepc eps-apn-configuration 11
apn-name internet
ambr-max-dl 41943040
ambr-max-dl-ext 400000000
ambr-max-ul 20971520
ambr-max-ul-ext 400000000
apn-oi-replacement mmc010.mcc315.gprs
can-be-deleted true
bearer-charging-chars 1
pdn-type ipv4
qos-profile-arp 2
qos-profile-arp-preemption-capability disabled
qos-profile-arp-preemption-vulnerability disabled
qos-profile-qci 9
vp1mn-allowed false
iwk5gs-indicator subscribed
```

Please update cnat generated configuration for ccsm-hss.

So customer can use NSA without raising ticket to us.

#### Comments

Comment by [Alvaro Martin](#) [ 2025-07-24 ]

New config is updated in CCSM 1.15 for UCC1.2 and it's already pushed to working branch [UCC-196\\_Appliance\\_CNF\\_SW\\_uplift](#)

Comment by [S. Chandrasekar](#) [ 2025-07-08 ]

Hi [Alexander Malikov](#) , [Rajan Rajeshprasad Gupta](#)

As discussed with Rajan, We agree to change the default profile, QCI value to 9 and arp to 2, Also in the installation instructions, We can add the statement , default profile given in the config is just example, It needs to be modified or additional profile according to customer requirement to be created.

BR/Chandrasekar

Comment by [Zhigang Han](#) [ 2025-07-07 ]

hi team,

I do see this table:

#### QCI to 5QI Mapping (Reference from 3GPP TS 23.501 & TS 23.203):

QCI	Service Type	5QI (Mapped)	Resource Type	Typical Use Case
1	Conversational Voice	1	GBR	VoLTE

2	Conversational Video (Live)	2	GBR	Video call
3	Real-time gaming	3	GBR	Online gaming
4	Buffered video streaming	4	GBR	Streaming (YouTube, etc.)
5	IMS Signaling	5	Non-GBR	SIP signaling
6	TCP-based services (low latency)	6	Non-GBR	Web access, file downloads
7	Similar to QCI 6 with diff. perf	7	Non-GBR	Similar to QCI 6
8/9	Default Bearer (Internet)	8 or 9	Non-GBR	Best effort / default traffic

Thanks,

BR/Zhigang

Comment by [Alexander Malikov](#) [ 2025-07-07 ]

@Quang-Thanh Nguyen, could you please check this ticket from 3GPP point of view if that's correct or not?

[Alvaro Martin](#), I guess if the statement from customer is correct than we need to update HSS configuration.

Best regards?

Alex

Comment by [Zhigang Han](#) [ 2025-07-07 ]

Hi Alexander,

as we discussed from the team, If we support 5G NSA split bearer, I do see there is a need to update our cnat script to generate the correct configuration for ccsm.

Thanks,

BR/Zhigang

[UCC\_PLM-253] [UCC MELA : 1.1 GA: CCSM ticket is not accessible from any customer ID in software gateway](#) Created: 2025-07-02 Updated: 2025-07-06 Resolved: 2025-07-06

Status:	Done
Project:	<a href="#">UCC_PLM</a>
Component/s:	None
Affects Version/s:	<a href="#">UCC Appliance 1.1.0</a>
Fix Version/s:	None

Type:	Bug	Priority:	High
Reporter:	<a href="#">Rajan Rajeshprasad Gupta</a>	Assignee:	<a href="#">Reema Sidhwani</a>
Resolution:	Closed	Votes:	0
Labels:	None		
Remaining Estimate:	Not Specified		
Time Spent:	Not Specified		
Original Estimate:	Not Specified		

Attachments:	<input type="checkbox"/> High Problem 2025-06-13_9 (External) CCSM_ Compatibility Issue with Service Mesh 17 or higher.msg	
Found in Build:	<a href="#">UCC 1.1 GA</a>	
Requirement Status:	<a href="#">UCC Appliance 0.2.1 - UNCOVERED</a>	

#### Description

Hello,

It was come to notice, Colleagues planning to deploy UCC 1.1 GA.

They are unable to access software gateway ticket for CCSM 1.14 EP1 which is part of UCC 1.1 GA.

Everyone is getting ""Unauthorized""

<https://swgw.ericsson.net/enovia/tvc-action/SWGObjectUrl?type=SWG+Ticket&rev=1&name=T-162101>

As understood reason:

There was a Gols message impacting CCSM1.14 EP1 so might be that its not accessible anymore.  
Recommended Action: We recommend upgrading to CCSM 1.14 EP3 or CCSM 1.15, both of which include the fix for this issue.

attached Gols message.

[High Problem 2025-06-13\\_9 \(External\) CCSM\\_Compatibility Issue with Service Mesh 17 or higher.msg](#)

Question1: Which software of CCSM should be used for UCC 1.1 GA deliveries?

Note: CCSM 1.14 EP3: and CCSM 1.15: is accessible.

CCSM 1.15:

<https://swgw.ericsson.net/enovia/tvc-action/SWGObjectUrl?type=SWG+Ticket&rev=1&name=T-165655>

CCSM 1.14 EP3:

<https://swgw.ericsson.net/enovia/tvc-action/SWGObjectUrl?type=SWG+Ticket&rev=1&name=T-165881>

Question2: If we start using other software, There is mandatory change required on imageloading and other files, Is UCC planning to give updated config files?

Please let us know feedback as early as possible to avoid delay in downloading software for delivery.

#### Comments

Comment by Rajan Rajeshprasad Gupta [ 2025-07-04 ]

Thank you Reema!

I have verified for verizon and Ericsson GMBH. I can see it now.

Trust, It will be available for all UCC customers. We will see based on case by case delivery.

The screenshot shows the SW Gateway interface. At the top, there's a header with the SW Gateway logo and a download icon. Below the header, the word "Home" is visible. On the left, there's a sidebar with a minus sign icon and a ticket ID "T-162101". To the right of the sidebar, detailed ticket information is displayed:

- Header:** CCSM 1.14 EP1 (highlighted in yellow)
- Start Date:** Jul 04, 2025
- Description:** CCSM 1.14 EP1 (CSAR 1.37.9+2) Automatic Distribution
- Expiry Date:** Jul 05, 2026
- Ticket Url:** <https://swgw.ericsson.net/enovia/tvc-action/SWGObjectUrl?type=SWG+Ticket&rev=1&name=T-165655>

Below this, there are three buttons: "Download", "Delivery Report", and "Release Documents". Under the "Download" button, a sub-instruction says "Expand Target Group and select Deliverable[s] to Download and Push". A "Download" button with a green arrow icon is shown, along with dropdown menus for target groups and deliverables. A cursor is hovering over the "Target Group Name" dropdown menu. A table below lists target groups:

Target Group ID	Target Group Name	Product Number	Version	Description
948400	VERIZON COMMUNICATIONS INC.			
962353	ERICSSON GMBH			

Comment by Reema Sidhwani [ 2025-07-04 ]

Issue should be resolved now. Please check.

Comment by Rajan Rajeshprasad Gupta [ 2025-07-04 ]

Thank you Reema

Mohit Tomar - Please keep track and use as soon as available for Verizon.

Comment by Reema Sidhwani [ 2025-07-04 ]

Hi Rajan, the configuration manager of CCSM was informed and requested to give access to the blocked SWGW for 1.14 EP1 already on Wednesday. I have sent a reminder

Comment by Rajan Rajeshprasad Gupta [ 2025-07-04 ]

Hello Team

Please update.

2 Teams are waiting for this.

MELA: Team for UCC installation

MANA: Verizon team for UCC 1.1 re-install.

We need to share feedback asap.

+Jossy Pallan

[UCC\_PLM-252] UCC MANA : ucc-ccpc-prov script does not allow to attach dataplan with length>15 Created: 2025-06-25 Updated: 2025-09-22 Resolved: 2025-07-18

Status:	Done
Project:	UCC_PLM
Component/s:	None
Affects Version/s:	UCC Appliance 1.0.1-rc1
Fix Version/s:	None

Type:	Bug	Priority:	Medium
Reporter:	Rajan Rajeshprasad Gupta	Assignee:	Sherif Farag F
Resolution:	Closed	Votes:	0
Labels:	UCC-CCPC-PROV		
Remaining Estimate:	0h		
Time Spent:	8h		
Original Estimate:	8h		

Attachments:	
Sprint:	UCC XFT3 Sprint 12
Epic Link:	Coding Activity 1.2
Team/s:	UCC_XFT2, UCC_XFT3
Found in Build:	UCC 1.1 RC2
Requirement Status:	UCC Appliance 0.2.1 - UNCOVERED

#### Description

Hello,

MANA colleagues are currently testing the QoS use case with UCC.

During the configuration of custom CCPC policies, it was discovered that the ucc-ccpc-prov script does not allow attaching a dataplan with a length greater than 15.

This limitation is not documented anywhere in the UCC documentation, and there is no information available regarding this restriction.

See below:

```
ericsson@fe1-sfs:~/campus_ucc/software/ccpc-prov-binary$ ./ucc-ccpc-prov PUT 31041000000002 1 dataplan_128kbps_qci6
```

```
/__/ /__/ /__/ /__/  
/ / \ / / \ / / \ /  
\ / \ / / \ / / \ /
```

© Ericsson AB 2024.

No part of this configuration file may be distributed to 3rd parties without the written permission of the copyright owner.

The contents of this configuration file are subject to revision without notice due to continued progress in methodology, design and manufacturing. Ericsson shall have no liability for any error or damage of any kind resulting from the use of this configuration file.

Error: DataPlan should be a string 3-15 characters, number and - is allowed

ucc-ccpc-prov.py - 1.0.1

See below dataplan is already created and exist in cccp internal DB.

```
ericsson@fe1-sfs:~/campus_ucc/software/ccpc-prov-binary$ ./ucc-ccpc-prov PUT 310410000000002 1 OTT-dataplan
/ _/ / _/ / _/ / _/
/ / \ / \ / \ / \ /
\ _/ \ _/ \ / \ _/
© Ericsson AB 2024.
No part of this configuration file may be distributed to 3rd parties without the written permission of the copyright owner.
The contents of this configuration file are subject to revision without notice due to continued progress in methodology,
design and manufacturing. Ericsson shall have no liability for any error or damage of any kind resulting from the use of this configuration file.2025-06-25
01:06:34,973 - INFO - UCC-CCPT-PROV version: 1.0.1
2025-06-25 01:06:34,974 - INFO - Operation: PUT
--
--
2025-06-25 01:06:37,949 - DEBUG - Starting new HTTPS connection (1): prov-pcx-jucca.ericsson.se:443
2025-06-25 01:06:37,961 - DEBUG - https://prov-pcx-jucca.ericsson.se:443 "GET /ccpc-provisioning/v1/dataplans HTTP/11" 200 64
2025-06-25 01:06:37,961 - INFO - DATA PLANS Retrieved: 200 b'{"ids": ["dataplan_128kbps_qci6", "MCS-dataplan", "OTT-dataplan"]}'"
2025-06-25 01:06:37,962 - INFO -
{
    "ids": [
        "dataplan_128kbps_qci6",
        "MCS-dataplan",
        "OTT-dataplan"
    ]
}
```

Request from ticket.

1. If there is valid reasons, To document any such limitation to avoid re-work during project delivery
2. Improvement to allow dataplan string length 30

## Comments

Comment by [Sherif Farag F](#) [2025-07-18]

Hello Rajan Rajeshprasad Gupta

This new requirements and enhancements are included on ccpc-prov tool (*—ucc-ccpc-prov-1.04 onwards*), the latest ccpc-prov tool binary can be found at:

<https://arm.sero.gic.ericsson.se/artifactory/proj-ucc-ccpc-prov-release-generic-local/releases/1.0.4-ucc-ccpc-prov-tool-release.tar.gz>

Br, Sherif//

Comment by [Soner Mus](#) [2025-07-09]

Hello Alexander Malikov

Thanks for the comment, per example in the original issue (dataplan\_128kbps\_qci6 --> 21 chars). Let Us put the control for;

- Total digit: 30
- Includes Only
  - Lowercase letters (a–z)
  - Uppercase letters (A–Z)
  - Numbers (0–9)
  - Special characters (e.g., underscore \_ hyphen -)

We will implement this in the CCPC Prov tool like this. Thanks for your kind help.

Thanks

Comment by [Alexander Malikov](#) [2025-07-09]

Hello Soner,

We use REST API for CCPC provisioning. Body is json based. For simplification we can stay that in UCC we can support only following characters:

- Lowercase letters (a–z)
- Uppercase letters (A–Z)
- Numbers (0–9)
- Special characters (e.g., underscore \_ hyphen - and ".")  
If you think we need to add more I don't have any strong opinion on that.

Best regards,  
Alex.

Comment by [Soner Mus](#) [2025-07-09]

Hello Alexander Malikov

Thanks for the input. Just to clarify, when you mention that fields like profileid, rulename, dataplanName, and policyName should be "3–15 characters," could you please cor

Specifically, are the following accepted:

- Lowercase letters (a–z)
- Uppercase letters (A–Z)
- Numbers (0–9)
- Special characters (e.g., underscore \_ hyphen -, etc.)

Please let me know the exact rules so we can implement the proper validation in the CCPC provisioning tool.

Thanks

Comment by [Alexander Malikov](#) [ 2025-07-09 ]

Soner Mus, Gonzalo Poveda and Rajan Rajeshprasad Gupta, can we agree on this?  
profileid, string 3-15 characters  
rulename, string 3-15 characters  
dataplanName, string 3-15 characters  
policyName, string 3-15 characters

If everybody ok. Soner Mus could you please check and update CCPC provisioning tool and I will update Installation guide.

Comment by [Soner Mus](#) [ 2025-07-09 ]

Hello Alexander Malikov

Could you please help the rule that needs to be applied in order to validate the naming ?

Thanks

Comment by [Soner Mus](#) [ 2025-07-01 ]

Hello Alexander Malikov,

In the CCPC Provisioning tool, it is technically possible to remove the validation control. However, from our perspective, there should still be a mechanism in place to validate

For example, since this information needs to be stored in a database for persistence, constraints such as a maximum character limit should be enforced.

BR;

Comment by [Frank Peveling](#) [ 2025-07-01 ]

Hello,

is there something needed to trigger the CPI update?

This Jira is about parameter "dataplan",

whats about other parameters like QOS profileid, rulename and policyName?

I would put some lines in Software Installation Guide, chapter 16 PVF Prov... under Prerequisites.

- Parameter nameing convention:

```
profileid, string ? characters
rulename, string ? characters
dataplanName, string 3-15 characters
policyName, string ? characters
```

and 16.1 step 4.4 Datapaln Definitions:

Where:

<Dataplans > is the value defined for parameter dataplanName (string 3-15 characters).

Greetings,

Frank

Comment by [Alexander Malikov](#) [ 2025-06-30 ]

Hello,

It's hardcoded in CCPC provisioning tool code:

```
if parser.parse_args().operation == "PUT" and not is_valid_string(parser.parse_args().data_plan_name):
    parser.error(f"DataPlan should be a string 3-15 characters, number and - is allowed \nuucc-ccpc-prov.py - {__version__}\n")
```

```
def is_valid_string(input_string):
    pattern = r'^[a-zA-Z0-9-]{3,15}$'
    if re.match(pattern, input_string):
        return True
    return False
```

We can update it in CPI as well in UCC 1.2

Best regards,

Alex

Comment by [Frank Peveling](#) [ 2025-06-27 ]

Possible solutions:

Easy way: Document the requirements in CPI:

DataPlan should be a string 3-15 characters, number and - is allowed

Long-run: UCC should follow mainly the application parameter requirements.

Means here form CCPC minimum 1 character ...

ucc@plm-jumphost:~/software/dist\$ ./ucc-ccpc-prov --help

...

positional arguments:

...  
data\_plan\_name The name of the data plan is required for operation=PUT only

Comment by Frank Peveling [2025-06-27]

CCPC seems to have a less restrictive requirement, it only need minimum 1 character.

Error: DataPlan should be a string 3-15 characters, number and - is allowed

This restriction seems to be defined by UCC and not inherit by CCPC.

Means it's up to UCC to document this requirement.

Comment by Frank Peveling [2025-06-27]

## Ultra Compact Core (UCC) 1.1

eventTriggers

Filters

Libraries

- Ultra Compact Core (UCC) 1.1
- Cloud Core Data-Storage Manager (CCDM) 1.13 EP1
- Cloud Core Policy Controller (CCPC) 1.16 EP1
- Cloud Core Resource Controller (CCRC) 1.17
- Cloud Core Subscription Manager (CCSM) 1.14 EP1
- Cloud Native CNOM 2.2
- Ericsson Cloud Container Distribution 2.31.1
- Ericsson R6000 24 Q4
- Packet Core Controller (PCC) 1.34
- Packet Core Controller (PCC) 1.34 (CP), FOSS
- Packet Core Gateway (PCG) 1.26
- Packet Core Gateway (PCG) 1.26 (EP), FOSS
- Signaling Controller (SC) 1.16
- Ericsson Dynamic Activation (EDA) 2.20

Cloud Core Policy Controller (CCPC) 1.16 EP1

Contents

- Cloud Core Policy Controller (CCPC) ...
  - Library Overview
  - Product Overview
  - Planning
  - Site Engineering
  - Installation
  - Initial Configuration
  - Operation and Maintenance
  - Interface
    - REST API Specification
    - CCPC Provisioning API
      - Rules
      - Policies
      - Profiles
      - Dataplans
      - Locators
      - SharedDataplans
      - UsageAccumulators
      - Subscribers
      - Contents
      - Operator-specific-infos
      - Entities
      - FlexibleDiameter

REQUEST

PATH PARAMETER

REQUEST BODY

EXAMPLE

OBJECT

A dataplan is eq  
the same service  
{  
    dataplanName:  
  
        description:  
        defaultPrice:  
  
        globalScope:  
        staticQual:

[UCC_PLM-251] TMO: UCC 1.1 # AMF complaints for "CertM Certificate Not Available"	
Created: 2025-06-12 Updated: 2025-06-13 Resolved: 2025-06-13	
Status:	Rejected
Project:	UCC_PLM
Component/s:	None
Affects Version/s:	UCC Appliance 1.0.0-rc2
Fix Version/s:	None

Type:	Bug	Priority:	Medium
Reporter:	Rajan Rajeshprasad Gupta	Assignee:	Zhigang Han
Resolution:	Rejected	Votes:	0
Labels:	None		
Remaining Estimate:	Not Specified		
Time Spent:	Not Specified		
Original Estimate:	Not Specified		

Attachments:	<input type="checkbox"/> itc_06122025_1.pcapng	<input type="checkbox"/> logs_ep5g_2025-06-12-08-05-16.tgz
Team/s:	UCC_PLM	
Found in Build:	UCC 1.1 RC2	
Requirement Status:	UCC Appliance 0.2.1 - UNCOVERED	

#### Description

Hello,  
got complaints for T-mo, during their first SA call.  
AMF could not register into NRF and its complaints as alarm

```
certMCertificateNotAvailable
  active-severity      Critical
  service-name         eric-pc-mm-controller
  event-type           ProcessingErrorAlarm
  expires              34
  source               /mm/cm_cert_manager/23
  specific-problem    CertM Certificate Not Available
  probable-cause       100505
  major-type           193
  minor-type           4239786207
  last-event-time      2025-06-10T21:38:39.837391 PDT
  additional_text       The certificate SERVER is signed on unavailable picking failure of secunc service
```

Also alarm for nrf\_mngt is timeout.

as a result, AMF reject UEsession with cc:20(congestion).

I checked with tmo colleagues, how was ca.crt is generated, they confirm it is self signed and, all other nodes like SMF,UDM etc are properly registered into NRF only AMF complains for nrf-management service connection.

attached ADP.logs\_ep5g\_2025-06-12-08-05-16.tgz

[itc\\_06122025\\_1.pcapng](#)

#### Comments

Comment by [Zhigang Han](#) [ 2025-06-13 ]

Hi Rajan,

Thank you so much for the update! I will reject the ticket from my side.

Thanks,

BR/Zhigang

Comment by [Rajan Rajeshprasad Gupta](#) [ 2025-06-13 ]

Hello Sam,

lets close this ticket.

I got message from tmo colleagues, after generated new CAs and redeployed PCX.

With PKCS #8 ca.key, they can see in the AMF certificate manager certificate is valid.

```
trusted-certificate ca.crt
certificate-state valid
certificate-content C=SE,ST=Stockholm,L=Stockholm,O=Ericsson,OU=ucc,CN=UCC
version            3(0x2)
serial-number      6C5FB0774E970B769E45EA283E66D034C225729B
signature-algorithm sha256WithRSAEncryption
issuer             C=SE,ST=Stockholm,L=Stockholm,O=Ericsson,OU=ucc,CN=UCC
valid-from         2025-06-12T18:01:52+00:00
valid-to           2035-06-10T18:01:52+00:00
public-key         "30 82 01 22 30 0d 06 09 2a 86 48 86 f7 0d 01 01 05 00 03 82 01 0f 00 30 82 01 0a 02 82 01 01 00 c2 a0 b5 a5 10 da 45 98 a0 91 08 63 80
05 90 bf f2 79 92 b9 41 71 4d 0c 99 2c 18 13 d9 cc c4 9b 10 1a be 53 ee 13 65 3c 2c ee 42 a2 dd 22 db 2d 64 8d 20 c0 de 70 3f b1 87 ea a9 73 7c ad 12 ea c0 44 3a
9b 76 dc 7c 9a d3 19 6b ae 5f 3b 98 b8 d9 92 ac aa a2 f3 e3 31 65 90 5a 93 8f 28 b9 3b b7 0b 7b 82 3b f4 ca 7a 20 71 ef 2e 26 e4 df 93 ab 75 5d de e4 c8 bd 1b ef
e6 ba 09 55 2a 82 bb 19 e2 24 97 18 f3 d7 55 5b ad ae 8f fd 23 e9 1c 26 5d f3 81 a9 97 ad 54 a5 e9 37 4b 13 65 85 ec 23 17 60 19 5d 48 f4 89 91 ca 88 a1 20 4e 26
7a 8f ad 65 1e 5d 98 f2 26 c3 20 65 1d f3 87 37 1b d1 f4 ea 9e bf 3a 41 d9 08 97 2e c9 94 f8 1f cd 06 34 7a 3f 3e 24 12 af 6e 0e 21 e2 d4 0a bc fa a7 ef 4d 49 e3
6a 06 69 b1 53 1d 15 26 80 f8 3d 48 79 e4 30 d7 06 69 2d 80 a0 e1 07 8a b5 27 3f 02 03 01 00 01 "
public-key-algorithm rsaEncryption
key-usage          ""
extension-content  [ "X509v3 Subject Key Identifier: 6E:FC:D1:95:30:9E:69:D8:4F:C0:B6:4E:53:A4:AC:8C:FC:8A:F1:48" "X509v3 Authority Key Identifier:
keyid:6E:FC:D1:95:30:9E:69:D8:4F:C0:B6:4E:53:A4:AC:8C:FC:8A:F1:48" "X509v3 Basic Constraints: CA:TRUE" ]
```

Issue is no more noticed.

Comment by [Zhigang Han](#) [ 2025-06-12 ]

Hi Rajan,

Matthew contacted me for these certificate issues. He thinks the script he used to create the wrong certificates. I gave him the script to generate the certificate files when he planned to deploy UCC 1.0 CP1, however I told him the script has not been tested on UCC 1.1 deployment. I believe the script generates the wrong format of certificate files which caused the issue. Could you help him to redo chapter 9 with certificate and redeploy the CNFs?

Thanks,

BR/Zhigang

Comment by [Rajan Rajeshprasad Gupta](#) [ 2025-06-12 ]

Pod logs indicate:

```
{"version":"1.0.0","severity":"info","service_id":"eric-pc-mm-controller","timestamp":"2025-06-12T08:08:36.182-07:00","extra_data":{"pc_mm_real_timestamp":"2025-06-12T08:08:36.176-07:00","pc_mm_stream":"Erlang::Global"},"message":":=ERROR REPORT==== 12-Jun-2025::08:08:36.176058 ===\r\nError in process <0.14818.0> on node 'e_Erlang_Global_pm1_63_2@192.168.1.87' with exit value:\r\n{badmatch,[error,read_ca_certificate_error]},\r\n  [{http_tls_lib,get_credential_options,2,\r\n    [{file,\"http\\/http_tls_lib.erl\"},\r\n     {line,100}]}],\r\n   [{http_tls_lib,get_tls_options,1,\r\n     [{file,\"http\\/http_tls_lib.erl\"},\r\n      {line,53}]}],\r\n    [{sbi_client_conn_owner,create_tls_opts,1,\r\n      [{file,\"http\\/sbi_client\\sbi_client_conn_owner.erl\"},\r\n       {line,856}]}],\r\n     [{sbi_client_conn_owner,create_http_options_help,3,\r\n       [{file,\"http\\/sbi_client\\sbi_client_conn_owner.erl\"},\r\n        {line,856}]}],\r\n      [{sbi_client_conn_owner,create_http_options,2,\r\n        [{file,\"http\\/sbi_client\\sbi_client_conn_owner.erl\"},\r\n         {line,733}]}],\r\n          [{sbi_client_conn_owner,start_gun_owner_process,2,\r\n            [{file,\"http\\/sbi_client\\sbi_client_conn_owner.erl\"},\r\n             {line,211}]}]}\r\n\r\n"}]
```

```
{"version":"1.0.0","severity":"info","service_id":"eric-pc-mm-controller","timestamp":"2025-06-12T08:08:40.400-07:00","extra_data":{},"pc_mm_stream":"Erlang::Global"},"message":":=ERROR REPORT==== 12-Jun-2025::08:08:40.399658 ===\r\nncm_cert_manager:provider_get_cert: CredId = \"ca.crt\", CredType = trusted_certificate\r\nReason: KCopsResultCredErrorCredentialIdMissing\r\nDescription:\"ERROR -308 - The Credential Id is missing\"; ErrorCode=-308\r\n\r\n"}
```

[UCC\_PLM-250] MANA TMO: UCC 1.1 # mm checkpoint failed with "Application error: swm\_object\_store\_na " Created: 2025-06-11 Updated: 2025-06-12 Resolved: 2025-06-12

Status:	Done
---------	------

<b>Project:</b>	UCC_PLM
<b>Component/s:</b>	None
<b>Affects Version/s:</b>	UCC Appliance 1.0.0-rc2
<b>Fix Version/s:</b>	None

<b>Type:</b>	Bug	<b>Priority:</b>	Medium
<b>Reporter:</b>	Rajan Rajeshprasad Gupta	<b>Assignee:</b>	Alexander Malikov
<b>Resolution:</b>	Closed	<b>Votes:</b>	0
<b>Labels:</b>	None		
<b>Remaining Estimate:</b>	Not Specified		
<b>Time Spent:</b>	Not Specified		
<b>Original Estimate:</b>	Not Specified		

<b>Attachments:</b>	<a href="#">cpuchange-pod.txt</a>	<a href="#">logs_ep5g_2025-06-10-22-34-54.tgz</a>	<a href="#">Screenshot-1.png</a>	<a href="#">tmo_ucc_1.1_lld.xlsx</a>
<b>Team/s:</b>	UCC_XFT2			
<b>Found in Build:</b>	UCC 1.1 RC2			
<b>Requirement Status:</b>	UCC Appliance 0.2.1 - UNCOVERED			

### Description

Hello,  
I have received complaints for TMO colleagues, UCC 1.1 deployment for PCX is failed as mm checkpoint failed with "Application error: swm\_object\_store\_na ".  
See logs as below:

```
system_admin@pcx-ccda#mm checkpoint name LicensesOK
Error:Failed to execute action checkpoint, message: Failed: Application error: swm_object_store_na.

system_admin@pcx-ccda#mm checkpoint-list
return-value
WARNING: Failed to update ListOfSoftwareConfigurations, listing may be incorrect.

container (001-00-87), 2024-12-12 18:34, InstalledActive
```

After asking for ADP logs to understand reason why checkpoint is failing as there is no OSMN pod created for storing checkpoint logs.

further checking, It comes to notice that OSMN pod which is statefulset is not reflecting in pod status and statefulset is failing due to configuration.

logs as below:

Events:				
Type	Reason	Age	From	Message
----	-----	----	-----	-----
Normal	SuccessfulDelete	50m	statefulset-controller	delete Pod eric-data-object-storage-mn-0 in StatefulSet eric-data-object-storage-mn successful
Warning	FailedCreate	11m (x20 over 50m)	statefulset-controller	create Pod eric-data-object-storage-mn-0 in StatefulSet eric-data-object-storage-mn failed error: Pod "eric-data-object-storage-mn-0" is invalid: [spec.containers[0].resources.limits[cpu]: Invalid value: cpu": name part must consist of alphanumeric characters, '-', '_' or '.', and must start and end with an alphanumeric character (e.g. 'MyName', or 'my.name', or '123-abc', regex used for validation is '([A-Za-z0-9][A-Za-z0-9_.]*?[A-Za-z0-9])'), spec.containers[0].resources.limits[cpu]: Invalid value: cpu": must be a standard resource for containers, spec.containers[0].resources.requests[cpu]: Invalid value: cpu": name part must consist of alphanumeric characters, '-', '_' or '.', and must start and end with an alphanumeric character (e.g. 'MyName', or 'my.name', or '123-abc', regex used for validation is '([A-Za-z0-9][A-Za-z0-9_.]*?[A-Za-z0-9])', spec.containers[0].resources.requests[cpu]: Invalid value: cpu": must be a standard resource for containers]

attached ADP logs and lld.

[logs\\_ep5g\\_2025-06-10-22-34-54.tgz](#)

[tmo\\_ucc\\_1.1\\_lld.xlsx](#)

It is not clear what can have made such configuration failure of pod definition which is not expected to happen.

I requested to re-deploy PCX to see if problem notice again (as we cant delete OSMN as pod itself is not creating )

### Comments

Comment by [Zhigang Han](#) [2025-06-11]

Hi Rajan,

We will update UCC 1.1 installation instruction. If you agree on the fix, please let us know if we could close the ticket.

Thanks,

BR/Zhigang

Comment by [Rajan Rajeshprasad Gupta](#) [ 2025-06-11 ]

Hello Alex,

Tested. Below CLI works. Lets update in II.

```
kubectl -n ep5g patch sts eric-data-object-storage-mn \
--type='json' \
-p='[
{"op": "replace", "path": "/spec/template/spec/containers/0/resources/limits/cpu", "value": "700m"}]
```

2 times CPU changes from 700 to 600 and finally 700 works.

logs attached.

[cpuchange-pod.txt](#)

Comment by [Alexander Malikov](#) [ 2025-06-11 ]

So it should looks like this in Installation guide:



Comment by [Alexander Malikov](#) [ 2025-06-11 ]

Hello,

We are looking to update II with this command :

```
"kubectl -n ep5g patch sts eric-data-object-storage-mn \
--type='json' \
-p='[
{"op": "replace", "path": "/spec/template/spec/containers/0/resources/limits/cpu", "value": "700m"}]
```

]"

Please confirm that it works and we will update Installation guide.

Best regards,

Alex

Comment by [Rajan Rajeshprasad Gupta](#) [ 2025-06-11 ]

Thank you.

Shared feedback to avoid typo and do change by "kubectl edit sts eric-data-object-storage-mn -n ep5g" instead of patch command.

Will update once get feedback on late evening or tomorrow.

Comment by [Frank Peveling](#) [ 2025-06-11 ]

Hello,

I look always in the lastest II form this link:

[https://ericsson.sharepoint.com/:x/r/sites/UltraCompactCoreUCC/Shared%20Documents/General/DEV-DOCUMENTS-WORKDIR/UCC%201.1/Ericsson Ultra Compact Core - Appliance - Software Installation Guide - new.docx](https://ericsson.sharepoint.com/:x/r/sites/UltraCompactCoreUCC/Shared%20Documents/General/DEV-DOCUMENTS-WORKDIR/UCC%201.1/Ericsson%20Ultra%20Compact%20Core%20-%20Appliance%20-%20Software%20Installation%20Guide%20-%20new.docx)

This morning it had the "revision" in the footer of the document, Rev.:J 2025-05--06.

Comment by [Rajan Rajeshprasad Gupta](#) [ 2025-06-11 ]

Thank you for information.

hello [Frank Peveling](#) , I could not see In the Installation Guide, revision PJ17, which I'm currently referencing, which Installation Instructions (II) are you referring to?

```
kubectl -n ep5g patch sts eric-data-object-storage-mn --type='json' \
-p='[
{"op": "replace", "path": "/spec/template/spec/containers/0/resources/limits/cpu", "value": "700m"}]
```

your argument seems to correct, as I see there is time difference between normal pod and OSMN up status .[ OSMN pods are 20-30min behind other pods in time]

Comment by [Frank Peveling](#) [ 2025-06-11 ]

Maybe that was the trigger for the problem:

Copy paste from SW II:

```
kubectl -n ep5g patch sts eric-data-object-storage-mn --type='json' \
-p='[{"op": "replace", "path": "/spec/template/spec/containers/0/resources/limits/cpu", "value": "700m"}]
'
```

But it should be:

```
kubectl -n ep5g patch sts eric-data-object-storage-mn --type='json' \
-p='[{"op": "replace", "path": <here a NL> "/spec/template/spec/containers/0/resources/limits/cpu", "value": "700m"}]
'
```

Comment by [Frank Peveling](#) [2025-06-11]

I expect that something went wrong at the end of chapter 14.5 of SW Installation Guide  
by increasing the above mentioned value:

8. PCX eric-data-object-storage-mn pod may have high CPU utilization from time to time.

It is needed to increase the CPU limit from 500m to 700m using the patch command below. This has to be applied in both CCDs:

```
export USER=eccd
export CLUSTER=ccda
```

```
ssh -o ServerAliveInterval=60 \
$USER@$(cat $config_dir/config/templates/site-global-ucc.yaml \
yq eval \
'.network.$CLUSTER.ccd.ccd_oam.ipassignment .ccd_control_plane_external_ip' -)
```

```
kubectl -n ep5g patch sts eric-data-object-storage-mn --type='json' \
-p='[{"op": "replace", "path": "/spec/template/spec/containers/0/resources/limits/cpu", "value": "700m"}]'
```

Expected result: "statefulset.apps/eric-data-object-storage-mn patched"

Comment by [Frank Peveling](#) [2025-06-11]

OK,

error: FailedCreate .... Pod eric-data-object-storage-mn-0...

... Invalid value: cpu": name part must consist of alphanumeric characters, '-' '\_' or ':'.

Found that in the attached logs describe/STATEFULSETS/eric-data-object-storage-mn.txt:

Name: eric-data-object-storage-mn

Namespace: ep5g

Containers:

eric-data-object-storage-mn:

Limits:

cpu: 500m

cpu": 700m

ephemeral-storage: 4Gi

memory: 8Gi

Requests:

cpu: 50m

ephemeral-storage: 256Mi

memory: 8Gi

I guess there was an attempt to increase the CPU limit for the storage handler that failed.

The attempt left the invalid yaml and the pod creation failed by that.

Are logs available from this resource alteration attempt?

Greeting,

Frank

<b>Status:</b>	Rejected
<b>Project:</b>	UCC_PLM
<b>Component/s:</b>	None
<b>Affects Version/s:</b>	UCC Appliance 1.1.0
<b>Fix Version/s:</b>	None

<b>Type:</b>	Bug	<b>Priority:</b>	Low
<b>Reporter:</b>	Bengt-Dirk Heye	<b>Assignee:</b>	Zhigang Han
<b>Resolution:</b>	Rejected	<b>Votes:</b>	0
<b>Labels:</b>	None		
<b>Remaining Estimate:</b>	Not Specified		
<b>Time Spent:</b>	Not Specified		
<b>Original Estimate:</b>	Not Specified		

<b>Attachments:</b>	<a href="#">TC-TA11-MCN-1105_hSEPP_eric-sepp-worker-fb94664b8-6tz2_20250512.txt</a>	<a href="#">TC-TA11-MCN-1105-topology_hiding_roaming_registration_20250512.txt</a>	<a href="#">TC-TA11-MCN-1105_vSEPP_eric-sepp-worker-84f8c6b56-slm48_20250512.txt</a>
<b>Team/s:</b>	UCC_PLM		
<b>Severity_qmt:</b>	3- Medium		
<b>Found in Build:</b>	LFD1, SC 1.16		
<b>Requirement Status:</b>	UCC Appliance 0.2.1 - UNCOVERED		

#### Description

When reviewing the logs for the SC worker, we have observed that the vSEPP received sensitive topology information as part of the hSMF discovery response.

smfInfo: pgwFqdn: topon.s5.pgw-pcx-ucc1b.nodes.epc.mnc099.mcc244.3gppnetwork.org  
smfInfo: pgwFqdn: topon.s5.pgw-pcx-ucc1b.nodes.epc.mnc099.mcc244.3gppnetwork.org

This pgwFqdn also reveals topology information about two ucc systems (ucc1a, ucc1b), that it might be a dual mode system (pgw-pcx/epc) ...

```

nfInstances:
- fqdn: ATAB1J2502CZEF6FQD7X0B6A7VMOXSNYQ.5gc.mnc099.mcc244.3gppnetwork.org
  locality: cda
  nfInstanceId: d67766fc-210f-4ecf-858f-000000b1c1d1
  nfServices:
    - fqdn: ATAB1J2502CZEF6FQD7X0B6A7VMOXSNYQ.5gc.mnc099.mcc244.3gppnetwork.org
      ipEndPoints:
        - port: 443
      nfServiceStatus: REGISTERED
      scheme: https
    serviceInstanceId: nsmf-pdusession.d67766fc-210f-4ecf-858f-000000b1c1d1
    serviceName: nsmf-pdusession
    supportedFeatures: "24"
    versions:
      - apiFullVersion: 1.2.3
        apiVersionInUri: v1
  nfStatus: REGISTERED
  nfType: SMF
  plmnList:
    - mcc: "244"
      mnc: "99"
  priority: 1
  rNccnfc:

```

#### Comments

Comment by [Zhigang Han](#) [ 2025-05-23 ]

Hi Bengt,

I will reject the ticket from PLM side. Could you open the ticket from XFT Jira? Here is the XFT Jira link:

<https://eteamproject-alpha.internal.ericsson.com/issues/?jql=project%20%3D%20%22UCC%20XFT%22%20and%20issuetype%20%3D%20Bug>

Thanks,

BR/Zhigang

[UCC_PLM-247] UCC 1.0 MELA : MCC/MNC input in the LLD template comment correction <small>Created: 2025-04-25 Updated: 2025-06-03 Resolved: 2025-06-03</small>			
Status:	Done		
Project:	<a href="#">UCC_PLM</a>		
Component/s:	None		
Affects Version/s:	<a href="#">UCC Appliance 1.1.0</a>		
Fix Version/s:	None		

Type:	Bug	Priority:	Medium
Reporter:	<a href="#">Rajan Rajeshprasad Gupta</a>	Assignee:	<a href="#">Alexander Malikov</a>
Resolution:	Closed	Votes:	0
Labels:	UCC_Appliance_1.1.0		
Remaining Estimate:	Not Specified		
Time Spent:	Not Specified		
Original Estimate:	Not Specified		

Attachments:	
Team/s:	UCC_XFT2
Found in Build:	UCC Appliance 1.1.0-drop.1
Requirement Status:	UCC Appliance 0.2.1 - UNCOVERED

#### Description

Hello,

Feedback from colleagues from MELA.

The comment says that MCC and MNC should be 3 digits:

1	Home PLMN					
2	mcc	mcc	244		MCC	
3	mnc	mnc	099		MNC	
4			2440990000000000			

But it's not entirely clear that if you have a 2 digit MNC (which we have in The Netherlands) that a leading zero is required.

Since we have SIMs with IMSI range 204961xxxx, the engineer thought the MNC was 961.

Maybe it's good to change the comment for the mnc to:

Suggestion to updated LLD comments:

"MNC should be 2 or 3 digits. In case of the mnc is 2 digits a leading zero is required"

#### Comments

Comment by [Alexander Malikov](#) [ 2025-06-03 ]

It was fixed in the UCC 1.1 LFD2 LLD template

Comment by [Zhigang Han](#) [ 2025-04-25 ]

Hi Rajan,

I agree with you if we could have the clear description to help the engineer to fill up LLD easily. I am not sure if this is a bug for our LLD or it is just an improvement from our side. I will assign the ticket to XFT2 team because XFT2 team mainly is responsible for LLD and Let us wait for the design's answer.

Thanks,

BR/Zhigang

[UCC\_PLM-231] UCC MCN: [UCC 1.1 ] To correct message-data regex Created: 2025-04-10 Updated: 2025-04-24 Resolved: 2025-04-24

Status:	Done
Project:	UCC_PLM
Component/s:	None
Affects Version/s:	None
Fix Version/s:	None

Type:	Bug	Priority:	Medium
Reporter:	Rajan Rajeshprasad Gupta	Assignee:	Andrei Mihalcea
Resolution:	Closed	Votes:	0
Labels:	None		
Remaining Estimate:	Not Specified		
Time Spent:	Not Specified		
Original Estimate:	Not Specified		

Sprint:	UCC XFT2 Sprint 8, UCC XFT2 Sprint 9
Team/s:	UCC_XFT2
Found in Build:	UCC Appliance 1.1.0-drop.1
Requirement Status:	UCC Appliance 0.2.1 - UNCOVERED

#### Description

Hello,

During testing, we observed that SEPP was unable to select NFpool despite the presence of a routing rule. It was determined that the default regex available in UCC SEPP is ineffective, and therefore, a new and updated regex needs to be added to ensure correct NFpool selection in message-data

See available message-data regex in UCC:

```
message-data target_apiroot_data
header      3gpp-sbi-target-apiRoot
extractor-regex "^(P<nf>\w+)-.*\..5gc\.mnc(P<mnc>\d+)\.mcc(P<mcc>\d+)"
```

See Results from debug logs: nothing as captured as desired.

```
{"version": "1.1.0", "timestamp": "2025-04-09T13:59:22.677+00:00", "severity": "debug", "service_id": "eric-sepp-worker", "message": "Variables:\nproto: null\nversion: null\nnf: null\nmnc: null\nmcc: null\nnf_type: null\ntarget_nf_type: null", "metadata": {"proc_id": "13", "ul_id": ""}, "extra_data": {"location": {"src_file": "source/extensions/filters/http/eric_proxy/filter.cc", "src_line": "790"}, "thread_info": {"thread_id": "93"}, "stream_id": "6414708886805233601", "connection_id": "1683"}}
```

Correct message-data regex in UCC:

```
message-data target_apiroot_data
header      3gpp-sbi-target-apiRoot
extractor-regex "^(?:https://)?(?:P<nf>[^-]+)-.*\..5gc\.mnc(?:P<mnc>\d+)\.mcc(?:P<mcc>\d+)"
```

See Results from debug logs: as captured as desired.

```
{"version": "1.1.0", "timestamp": "2025-04-09T15:32:32.820+00:00", "severity": "debug", "service_id": "eric-sepp-worker", "message": "Variables:\nnf: udm\nmnc: 099\nmcc: 244\nproto: null\nversion: null\ntarget_nf_type: null", "metadata": {"proc_id": "13", "ul_id": ""}, "extra_data": {"location": {"src_file": "source/extensions/filters/http/eric_proxy/filter.cc", "src_line": "790"}, "thread_info": {"thread_id": "94"}, "stream_id": "17581332398250896692", "connection_id": "4241"}}
```

To correct UCC day1 files

#### Comments

Comment by Andrei Mihalcea [ 2025-04-16 ]

Hi ,

Regex was correct in Day1 config and pushed in GIT for next Drop/LFD .

```
"^(?:https://)?(?:P<nf>[^-]+)-.*\..5gc\.mnc(?:P<mnc>\d+)\.mcc(?:P<mcc>\d+)"
```

Best Regards,  
Andrei

[UCC_PLM-229] UCC MCN: [UCC 1.1] 400//UNSPECIFIED_MSG_FAILURE\" ,\"detail\" ,\"route_not_found	
Status:	Done
Project:	UCC_PLM
Component/s:	None
Affects Version/s:	None
Fix Version/s:	None

Type:	Bug	Priority:	Medium
Reporter:	Rajan Rajeshprasad Gupta	Assignee:	Andrei Mihalcea
Resolution:	Closed	Votes:	0
Labels:	None		
Remaining Estimate:	Not Specified		
Time Spent:	Not Specified		
Original Estimate:	Not Specified		

<b>Sprint:</b>	UCC XFT2 Sprint 8, UCC XFT2 Sprint 9
<b>Team/s:</b>	UCC_XFT2
<b>Found in Build:</b>	UCC Appliance 1.1.0-drop.1
<b>Requirement Status:</b>	UCC Appliance 0.2.1 - UNCOVERED

## Description

Hello,

```
{"version":"1.1.0","timestamp":"2025-04-08T13:12:29.795+00:00","severity":"trace","service_id":"eric-sepp-worker","message": "new response body is set:{\"cause\":\\\"UNS\n\"proc_id\":\"12\",\"ul_id\":\"\"},\"extra_data\":{\"location\":{\"src_file\":\"source/extensions/filters/http/eric_proxy/filter.cc\",\"src_line\":674}},"thread_info\":{\"thread_id\":4}
```

It is also notice from logs, AUSF discovery message as below;

After decoding encoded PLMN coming as part of AUSF discovery, we see as below;

After URI decoding:target-plmn-list=[{"mcc": "244", "mnc": "99"}]&requester-plmn-list=[{"mcc": "240", "mnc": "81"}, {"mcc": "460", "mnc": "31"}, {"mcc": "262", "mnc": "72"}, {"mcc": "242", "mnc": "11"}]

Which indicate MNC received as "99" instead of configured MNC in routing-case as "099" so none of the routing rule match.

Fix: To add additional rule without zero.

```
sepp-function nf-instance ucc1-sepp
routing-case routing_from_external
  message-data-ref [ apiRoot_data proto_from_path ]
  routing-rule psepp_to_nfNRF_preferred2
    condition "var.proto=='nrrf-disc' and var.mnc=='99' and var.mcc=='244'"
    routing-action nrf_pool_pref
      action-route-preferred from-target-api-root-header
      action-route-preferred failover-profile-ref fop_ext
      action-route-preferred target-nf-pool nf-pool-ref nrf_pool
  !
!
```

Question1: Should we update configuration for routing rule by considering with and without zero MNC?

Question2: Should we keep only without zero routing rule?

## Comments

Comment by Andrei Mihalcea [ 2025-04-10 ]

Hi guys,

This case should be closed is not applicable what is here. The SEPP Routing was completely changed in the last Day1 config that was installed in MCN on 9th April. There was a problem also for the new routing config in the "regex" used but was updated and new TT was opened for this :

[https://eteamproject-alpha.internal.ericsson.com/browse/UCC\\_PLM-231](https://eteamproject-alpha.internal.ericsson.com/browse/UCC_PLM-231)

Cheers,

Andrei,

Comment by Andrei Mihalcea [ 2025-04-09 ]

Hi Rajan,

It's strange the behavior that you mention, because it shouldn't matter if it's receiving MNC "099" or "99" because the MNC used used in condition, meaning tge "var.mnc" is extracted from the header (3gpp-Sbi-target-apiRoot) using this regex ("(https?://)?.\*5gc\.mnc(?:P<mnc>\d+)\.mcc(?:P<mcc>\d+)") and basically this regex will extract always with "0", meaning like this "099" because is extracting from FQDN and FQDN is always with "099".

Again, don't understand why is fixed after you made this correction however I would say that you need to put the latest Day1, as mentioned last week, the Day1 for SEPP is in full process of refinement and configuration mentioned above was changed in Day1.

I will inform also by e-mail to be everybody aware.

Thank you,

Andrei,

[UCC\_PLM-226] UCC MCN: [UCC 1.1 ] SEPP does not registered into NRF Created: 2025-04-03 Updated: 2025-04-10 Resolved: 2025-04-10

Status:	Rejected
Project:	<a href="#">UCC_PLM</a>
Component/s:	None
Affects Version/s:	None
Fix Version/s:	None

Type:	Bug	Priority:	Medium
Reporter:	<a href="#">Rajan Rajeshprasad Gupta</a>	Assignee:	<a href="#">Andrei Mihalcea</a>
Resolution:	Rejected	Votes:	0
Labels:	None		
Remaining Estimate:	Not Specified		
Time Spent:	Not Specified		
Original Estimate:	Not Specified		

Sprint:	UCC XFT2 Sprint 8
Team/s:	UCC_XFT2
Found in Build:	UCC Appliance 1.1.0-drop.1
Requirement Status:	UCC Appliance 0.2.1 - UNCOVERED

## Description

Hello,

During testing, we discovered that while N32-C is active, SEPP is not registered with NRF. Upon analysis, we found that the NRF management configuration required to trigger SEPP registration with NRF was missing.

Configuration added to make it work. Lets add in standard UCC SC config to avoid issue.

```
sepp-admin@sepp-ucc(config)#sepp-function nf-instance ucc1-sepp
sepp-admin@sepp-ucc(config-nf-instance-ucc1-sepp)# nrf-service nf-management nrf-group-ref [ nrf-ucc1 ]
```

```
sepp-admin@sepp-ucc(config-nf-instance-ucc1-sepp)#commit  
Commit complete.
```

After that, we can see SEPP is getting registered into NRF.

Metrics query

```
sepp-admin@sepp-ucc#metrics-query | in nrf  
  "nrf_endpoint_failovers_created",  
  "nrf_endpoint_failovers_total",  
  "nrf_failovers_created",  
  "nrf_failovers_total",  
  "nrf_in_answers_created",  
  "nrf_in_answers_total",  
  "nrf_out_requests_created",  
  "nrf_out_requests_total",  
sepp-admin@sepp-ucc#metrics-query "nrf_in_answers_total"  
{  
  "nrf_in_answers_total": 0
```

Also direct from NRF:

```
* Connection #0 to host nrf-ccrc-ucc1b.5gc.mnc099.mcc244.3gppnetwork.org left intact  
{  
  "ipv4Addresses": [  
    "172.16.3.76"  
  ],  
  "nfInstanceId": "ef8b9906-a379-4f19-977c-7dc7247225f9",  
  "load": 0,  
  "fqdn": "seppint-sc-ucc1b.5gc.mnc099.mcc244.3gppnetwork.org",  
  "nfStatus": "REGISTERED",  
  "nfType": "SEPP",  
  "seppInfo": {  
    "connectors": []
```

## Comments

Comment by Andrei Mihalcea [2025-04-10]

Hi Rajan,

SEPP shouldn't be registered in NRF, this is not a requirement for UCC Project. The last Day1 is cleaned-up for the SEPP -> NRF Registration things. Before there were some leftovers but now it should be clean.

Cheers,

Andrei,

[UCC\_PLM-225] UCC MCN: [UCC 1.1] N32-c down with status code: 503, title: Service Unavailable Created: 2025-04-02 Updated: 2025-04-07 Resolved: 2025-04-07

Status:	Done
Project:	UCC_PLM

<b>Component/s:</b>	None
<b>Affects Version/s:</b>	None
<b>Fix Version/s:</b>	None

<b>Type:</b>	Bug	<b>Priority:</b>	Medium
<b>Reporter:</b>	Rajan Rajeshprasad Gupta	<b>Assignee:</b>	Andrei Mihalcea
<b>Resolution:</b>	Closed	<b>Votes:</b>	0
<b>Labels:</b>	None		
<b>Remaining Estimate:</b>	Not Specified		
<b>Time Spent:</b>	Not Specified		
<b>Original Estimate:</b>	Not Specified		

<b>Attachments:</b>	day1_sepp-config.txt.jinja2	image-2025-04-02-23-54-05-521.png	image-2025-04-03-19-35-02-391.png	
	logs_sc_2025-04-02-14-13-34.tgz	mcn-ucc-sepp-03-04-2025.txt	mnc-gic-sepp-03-04-2025.txt	ucc-sepp1.pcap
<b>Team/s:</b>	UCC_XFT2			
<b>Found in Build:</b>	UCC Appliance 1.1.0-drop.1			
<b>Requirement Status:</b>	UCC Appliance 0.2.1 - UNCOVERED			

### Description

Hello,

After doing connectivity for SEPP roaming testing.

We started roaming testing, we observed N32-c down with status code: 503, title: Service Unavailable.

we see status of n32-c as below

```
sepp-admin@sepp-ucc#show sepp-function nf-instance ucc1-sepp external-network externalNetwork roaming-partner rp1
roaming-partner rp1
n32-c
  security-negotiation-data deacucc2-sepp1
    last-update 2025-04-02T16:57:03.688+00:00
    operational-state
      value faulty
      reason "status code: 503, title: Service Unavailable"
```

We also see alarm on sepp as below

```
SeppSecurityCapabilityNegotiationFailure
  active-severity Critical
  service-name ericsson-sepp
  event-type CommunicationsAlarm
  expires 3541
  source sepp-instance=deacucc2-sepp1,roaming-partner=rp1,hsepp.5gc.mnc081.mcc240.3gppnetwork.org:443
  specific-problem SEPP, Security Capability Negotiation Failure
  probable-cause 158
  major-type 193
  minor-type 12124174
  last-event-time 2025-04-02T12:01:02.212000 UTC
  additional +out status code: 503 title: Service Unavailable
```

While we see counters for number of n32-c negotiation failure, counter keep on increasing.

```
sepp-admin@sepp-ucc#metrics-query n32c_in_responses_failure_total
{
  "data": {
    "result": [
      {
        "value": 1
      }
    ]
  }
}
```

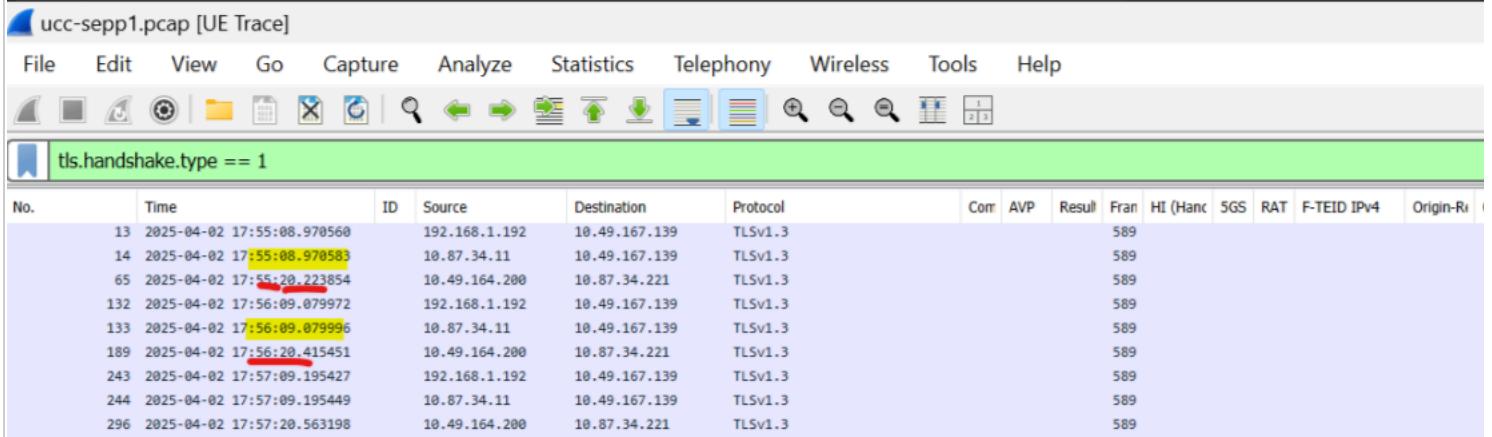
```

"metric": {
    "__name__": "n32c_in_responses_failure_total",
    "app": "eric-sepp-manager",
    "app_kubernetes_io_instance": "sc-ccdb-6",
    "app_kubernetes_io_managed_by": "Helm",
    "app_kubernetes_io_name": "eric-sepp",
}

```

We could not see tcpdump pcap as it is encrypted.

however, from tcpdump on worker, it is clear tcp sync is working fine on TLS 1.3. n32-c negotiation is happening exactly in 60second by each sepp. attached PCAP.



Same error is visible in sepp-manager logs

```

{"version":"1.1.0","timestamp":"2025-04-02T12:15:07.701Z","service_id":"eric-sepp-manager","severity":"warning","message":"seppmgr[7]||vert.x-eventloop-thread-0||c.e.Unavailable"}
{"version":"1.1.0","timestamp":"2025-04-02T12:15:07.705Z","service_id":"eric-sepp-manager","severity":"info","message":"seppmgr[7]||vert.x-eventloop-thread-0||c.e.sc.\\"faultName\\"\\"SeppSecurityCapabilityNegotiationFailure\\"",\\"serviceName\\"\\"ericsson-sepp\\"",\\"faultyResource\\"\\"sepp-instance=deacucc2-sepp1,roaming-partner=rp1,hsepp.5gc.mnc081.mcc240.3gppnetwork.org:443\"\\",\\\"severity\\"\\"Critical\"\\",\\\"description\\"\\"status code: 503, title: Service Unavailable\\\",\\\"createdAt\\"\\"2025-04-02T12:15:07.705Z\\\"\\\"FullRDN\\"\\"nf=sepp-instance=ucc1-sepp,static-sepp-instance-data=MCN-GIC-sepp,static-sepp-instance=deacucc2-sepp1,hsepp.5gc.mnc081.mcc240.3gppnetwork.partner=rp1\\\"\\\"}}"
{"version":"1.1.0","timestamp":"2025-04-02T12:15:07.706Z","service_id":"eric-sepp-manager","severity":"warning","message":"seppmgr[7]||vert.x-eventloop-thread-0||c.e.n32c request handshake to remote sepp: deacucc2-sepp1 with reason:Exchange Capability operation failed with reason: status code: 503, title: Service Unavailable"}
{"version":"1.1.0","timestamp":"2025-04-02T12:15:07.706Z","service_id":"eric-sepp-manager","severity":"info","message":"seppmgr[7]||vert.x-eventloop-thread-0||c.e.sc.\\"faultName\\"\\"SeppSecurityCapabilityNegotiationFailure\\"",\\"serviceName\\"\\"ericsson-sepp\\"",\\"faultyResource\\"\\"sepp-instance=deacucc2-sepp1,roaming-partner=rp1,hsepp.5gc.mnc081.mcc240.3gppnetwork.org:443\"\\",\\\"severity\\"\\"Critical\"\\",\\\"description\\"\\"status code: 503, title: Service Unavailable\\\",\\\"createdAt\\"\\"2025-04-02T12:15:07.706Z\\\"\\\"FullRDN\\"\\"nf=sepp-instance,ucc1-sepp,static-sepp-instance-data=MCN-GIC-sepp,static-sepp-instance=deacucc2-sepp1,hsepp.5gc.mnc081.mcc240.3gppnetwork.partner=rp1\\\"\\\"}}"
{"version":"1.1.0","timestamp":"2025-04-02T12:15:07.706Z","service_id":"eric-sepp-manager","severity":"warning","message":"seppmgr[7]||vert.x-eventloop-thread-0||c.e.n32c request handshake to remote sepp: deacucc2-sepp1 with reason:Exchange Capability operation failed with reason: status code: 503, title: Service Unavailable"}
{"version":"1.1.0","timestamp":"2025-04-02T12:15:33.116Z","service_id":"eric-sepp-manager","severity":"info","message":"seppmgr[7]||vert.x-eventloop-thread-0||c.e.a.e[\\"name\\"\\"n32c_in_responses_failure_total\\"\\",\\\"instances\\"\":[{\\"name\\"\\"[nf, nf_instance, roaming_partner, error_body]\\"=[sepp, deacucc2-sepp1, rp1, status_code: 503, \\"name\\"\\"n32c_out_requests_total\\"\\",\\\"instances\\"\:[{\\"name\\"\\"[nf, nf_instance, roaming_partner, method, path]\\"=[sepp, deacucc2-sepp1, rp1, POST, /n32c-handshake/v1

```

503 error indicate to me permanent failure. Could you help to check if there is mistake in configuration which is causing error or other and a way to fix it?

attached ADP logs.[logs\\_sc\\_2025-04-02-14-13-34.tgz](#)

## Comments

Comment by [Rajan Rajeshprasad Gupta](#) [2025-04-07]

Hello Meryam, Please close. this is fixed.

Comment by [Meryam Nachi](#) [2025-04-07]

Hi Rajan, should we close this ticket?

Comment by [Andrei Mihalcea](#) [2025-04-03]

Hi Rajan,

Nice, well done! One is solved 😊.....the next one to come 😊.

Just for your information, I've made some more updates in the Day1 config, but we still have to review them tomorrow and then I can provide you the last Day1 Jinja.

Cheers,

Andrei,

Comment by [Rajan Rajeshprasad Gupta](#) [ 2025-04-03 ]

Hello Andrei,

This problem is solved by correcting certificate mapping in GIC SEPP.

Logs where not giving information if problem was with UCC or GIC.

One page summary fix attached.

## SEPP-05 :n32-c gives 503 service unavailable[2/2]

Background:

N32-c didn't come up and getting into fault state. See alarm and status.

After correcting certificate part, See active state print

```
sepp-admin@sepp-ucc#show sepp-function nf-instance ucc1-sepp external-network externalNetwork roaming-partner rp1
Thu Apr 3 12:23:06.826 UTC+00:00
roaming-partner rp1
n32-c
security-negotiation-data deacucc2-sepp1
last-update 2025-04-03T12:23:02.841+00:00
operational-state
value active
security-capability TLS
supports-target-aproot true
received-plmn-id 244 50
```

N32-c Active Link

```
sepp-admin@sepp-ucc#show sepp
Thu Apr 3 12:49:22.212 UTC+00:00
sepp-function
nf-instance ucc1-sepp
external-network externalNetwork
roaming-partner rp1
in-request-screening-case-ref caseReqInRP
topology-hiding-ref [ topology_hiding_amf topology_hiding_topology_hiding_udm ]
out-response-screening-case-ref caseRespOutRP
domain-name [ *5gc.mmc081.mcc240.3gppnetwork.org
trusted-cert-in-list-ref trustcertlist-int-in-out
trusted-cert-out-list-ref trustcertlist-int-in-out
supports-target-aproot true
topology-hiding-with-admin-state tphFqdnMapping
admin-state active
!
topology-hiding-with-admin-state tphFqdnScrambling
admin-state active
scrambling-key TAB1
activation-date 2025-03-06T14:50:31.456449+06:00
!
!
```

N32-c Active Link

```
sepp-admin@sepp-ucc#show running-config sepp-function nf-instance
roaming-partner rp1
sepp-function nf-instance ucc1-sepp
external-network externalNetwork
roaming-partner rp1
in-request-screening-case-ref caseReqInRP
topology-hiding-ref [ topology_hiding_amf topology_hiding_topology_hiding_udm ]
out-response-screening-case-ref caseRespOutRP
domain-name [ *5gc.mmc081.mcc240.3gppnetwork.org
trusted-cert-in-list-ref trustcertlist-int-in-out
trusted-cert-out-list-ref trustcertlist-int-in-out
supports-target-aproot true
topology-hiding-with-admin-state tphFqdnMapping
admin-state active
!
topology-hiding-with-admin-state tphFqdnScrambling
admin-state active
scrambling-key TAB1
activation-date 2025-03-06T14:50:31.456449+06:00
!
!
```

Issue Fix:

Added to GIC CA into the truststore: sc-traf-root-ca-list1

[ 4 parameters are used during negotiation: TLS SAN, OwnPLMN and TargetedPLMN. All should be correctly configured to allow N32-C negotiation work

Comment by [Andrei Mihalcea](#) [ 2025-04-03 ]

Hi Rajan,

As we are in process of cleaning-up the day1 config for SEPP, I've made several modification in SEPP config. I've tested in my side and looks okey, meaning that installation try one more installation with this Day1 Jinja and let me know if it's something changed ? If we still have the same errors we will check after that.

Thank you,

Andrei,

Comment by [Rajan Rajeshprasad Gupta](#) [ 2025-04-03 ]

configuration attached for both SEPP.

UCC : SC 1.16 [mcn-ucc-sepp-03-04-2025.txt](#)

GIC : SC 1.14 [mnc-gic-sepp-03-04-2025.txt](#)

[UCC\_PLM-223] UCC MCN: [UCC 1.1 day1 ] SEPP hardcoded PLMN for own and RP Created: 2025-03-27 Updated: 2025-04-24 Resolved: 2025-04-24

Status:	Done
Project:	<a href="#">UCC_PLM</a>
Component/s:	None
Affects Version/s:	None
Fix Version/s:	None

Type:	Bug	Priority:	Medium
Reporter:	<a href="#">Rajan Rajeshprasad Gupta</a>	Assignee:	<a href="#">Andrei Mihalcea</a>
Resolution:	Closed	Votes:	0
Labels:	None		
Remaining Estimate:	Not Specified		
Time Spent:	Not Specified		
Original Estimate:	Not Specified		

Attachments:				
Sprint:	UCC XFT2 Sprint 8, UCC XFT2 Sprint 9			
Team/s:	UCC_XFT2			
Found in Build:	UCC Appliance 1.1.0-drop.1			
Requirement Status:	UCC Appliance 0.2.1 - UNCOVERED			

#### Description

Hello,

The MCN team has updated the LLD for Visited PLMN and Own PLMN. However, following deployment, we observed that the RP PLMN and Own PLMN configurations were incorrectly injected into the SEPP.

#### LLD information updated:

Visited PLMN		
Visited mcc	visited_mcc	244
Visited mnc	visited_mnc	050

#### Configuration in SEPP node:

```

sepp-admin@sepp-ucc#show running-config | in -a 5 -b 5 098
4561- firewall-profile-ref      firewall-profile-rp1
4562- roaming-partner rp1
4563- in-request-screening-case-ref caseReqInRP
4564- topology-hiding-ref      [ topology_hiding_amf topology_hiding_ausf topology_hiding_nrf topology_hiding_smf topology_hiding_udm ]
4565- out-response-screening-case-ref caseRespOutRP
4566: domain-name          [*sepp.5gc.mnc098.mcc243.3gppnetwork.org ]
4567- trusted-cert-in-list-ref trustcertlist-int-in-out
4568- trusted-cert-out-list-ref trustcertlist-int-in-out
4569- supports-target-apiroot   true
4570- topology-hiding-with-admin-state tphFqdnMapping
4571- admin-state active
-
4835- static-nf-instance-data deacucc2-sepp
4836- static-nf-instance deacucc2-sepp1
4837- nf-type sepp
4838- static-nf-service default
4839- address scheme https
4840: address fqdn seppext-deacucc2b.5gc.mnc098.mcc243.3gppnetwork.org
4841- address multiple-ip-endpoint 1
4842- port    443
4843- ipv4-address [ 8.8.4.8 ]
4844- !

```

4845- !  
sepp-admin@sepp-ucc#

The same issue applies to Own PLMN. As a result, the CA certificate will not match, and N32 will not be operational for RP. To avoid reconfiguration, both RP PLMN and Own PLMN should be accurately applied from the LLD.

#### Comments

Comment by Rajan Rajeshprasad Gupta [ 2025-04-24 ]

To be verified on SDU readiness testing once lab is available. Closing based on already available feedback.

Comment by Andrei Mihalcea [ 2025-04-08 ]

Hey Rajan,

1. First thing, we don't have anymore "visite\_mcc" and "visited\_mnc" parameters in LLD, we are using like below :

routing_inaicator	routing_inaicator	v
Visited PLMN		
Visited1 PLMN name	visited1_name	
Visited1 mcc	visited1_mcc	
Visited1 mnc	visited1_mnc	
Visited1 Domain	visited1_domain	
Visited1 SEPP FQDN	visited1_sepp_fqdn	
Visited1 SEPP IPv4	visited1_sepp_ipv4	
Visited2 PLMN name	visited2_name	
Visited2 mcc	visited2_mcc	
Visited2 mnc	visited2_mnc	
Visited2 Domain	visited2_domain	
Visited2 SEPP FQDN	visited2_sepp_fqdn	
Visited2 SEPP IPv4	visited2_sepp_ipv4	
Visited3 PI MN name	visited3_name	

2. Second point, in the configuration parts where you mentioned the wrong FQDNs we have already the parametrization, so NO hard coded values we have anymore :

```
{% if visited1_name is defined and visited1_name != None %}  
#! Definition for RoamingPartner 1  
static-sepp-instance-data {{ visited1_name }}-sepp  
static-sepp-instance {{ visited1_name }}-sepp1  
  nf-type sepp  
    address scheme https  
    address fqdn {{ visited1_sepp_fqdn }}  
    address multiple-ip-endpoint 1  
      port        443  
      ipv4-address [ {{ visited1_sepp_ipv4 }} ]  
    !  
  !  
!  
{% endif %}
```

```
{% if visited1_name is defined and visited1_name != None %}  
#! Definition for RoamingPartner 1  
roaming-partner {{ visited1_name }}  
  topology-hiding-ref      [ topology_hiding_amf topology_hiding_ausf topology_hiding_nrf topology_hiding_smf topology_hiding_udm ]  
  domain-name               [ *.{ {{ visited1_domain }} } ]  
  supports-target-apiroot   true  
  topology-hiding-with-admin-state tphFqdnMapping  
  admin-state active  
!
```

Maybe you are using some old files.

Cheers,

Andrei,

[UCC\_PLM-218] UCC MCN: [UCC 1.1 day1 ] SEPP missing n32-c configuration for roaming partner Created: 2025-03-24 Updated: 2025-04-24 Resolved: 2025-04-24

<b>Status:</b>	Done
<b>Project:</b>	<a href="#">UCC_PLM</a>
<b>Component/s:</b>	None
<b>Affects Version/s:</b>	None
<b>Fix Version/s:</b>	None

<b>Type:</b>	Bug	<b>Priority:</b>	Medium
<b>Reporter:</b>	<a href="#">Rajan Rajeshprasad Gupta</a>	<b>Assignee:</b>	<a href="#">Andrei Mihalcea</a>
<b>Resolution:</b>	Closed	<b>Votes:</b>	0
<b>Labels:</b>	None		
<b>Remaining Estimate:</b>	Not Specified		
<b>Time Spent:</b>	Not Specified		
<b>Original Estimate:</b>	Not Specified		

<b>Attachments:</b>		
<b>Sprint:</b>	UCC XFT2 Sprint 7, UCC XFT2 Sprint 8, UCC XFT2 Sprint 9	
<b>Team/s:</b>	UCC_XFT2	
<b>Found in Build:</b>	UCC Appliance 1.1.0-drop.1	
<b>Requirement Status:</b>	UCC Appliance 0.2.1 - UNCOVERED	

#### Description

Hello,

SEPP Day1 configuration generated for SEPP roaming partner as below;

```

external-network externalNetwork
service-address-ref      externalplmn
in-request-screening-case-ref   caseReqInRP
routing-case-ref          routing_from_external
out-response-screening-case-ref  caseRespOutRP
global-ingress-rate-limit-profile-ref [ global_rate_limit_profile_1 ]
firewall-profile-ref       firewall-profile-rp1
roaming-partner rp1
in-request-screening-case-ref  caseReqInRP
topology-hiding-ref        [ topology_hiding_amf topology_hiding_ausf topology_hiding_nrf topology_hiding_smf topology_hiding_udm ]
out-response-screening-case-ref caseRespOutRP
domain-name                [ *.sepp.5gc.mnc098.mcc243.3gppnetwork.org ]
trusted-cert-in-list-ref    trustcertlist-int-in-out
trusted-cert-out-list-ref   trustcertlist-int-in-out
supports-target-apiroot    true
topology-hiding-with-admin-state tphFqdnMapping
admin-state active
!
topology-hiding-with-admin-state tphFqdnScrambling
admin-state active
scrambling-key TAB1
activation-date 2025-03-06T14:50:31.456449+06:00
!
```

The configuration for enabling the N32-c interface between SEPPs is not included. The attached document highlights the missing N32-c configuration in yellow.

```

expert@sc-testnode#show running-config | sepp-function nf-instance instance_1 external-network externalNetwork
external-network externalNetwork
service-address-ref vpn_external
routing-case-ref routing_from_external
roaming-partner RP_BE
comment "Trusted roaming partner in PLMN 206-33 (RP-BE)"
routing-case-ref routing_from_external
domain-name [ *.region1.sepp.5gc.mnc033.mcc206.3gppnetwork.org ]
trusted-certificate-list sc-traf-root-ca-list2
supports-target-apiroot negotiated
topology-hiding-with-admin-state th_fqdn_map_1
admin-state graceful-activation
!
n32-c enabled true
n32-c nf-pool-ref sepp_RP_BE_pool
n32-c allow-plmn primary-id-mcc 206
n32-c allow-plmn primary-id-mnc 033
!
roaming-partner RP_SE
comment "Trusted roaming partner in PLMN 240-60 (RP-SE)"
routing-case-ref routing_from_external
domain-name [ *.region1.sepp.5gc.mnc060.mcc240.3gppnetwork.org ]
trusted-certificate-list sc-traf-root-ca-list2
supports-target-apiroot negotiated
topology-hiding-with-admin-state th_fqdn_map_1
admin-state graceful-activation
!
n32-c enabled true
n32-c nf-pool-ref sepp_RP_SE_pool
n32-c allow-plmn primary-id-mcc 240
n32-c allow-plmn primary-id-mnc 060
!

```

If not explicitly configured, the N32-c interface will be disabled by default. Refer to the Yang default values for more information.

YANG Model

Schema Node	<input type="checkbox"/> Hide leafs	Config true	Type list	Cardinality	Description
topology-hiding-ref					Reference to a defined topology hiding profile for external network.
roaming-partner		true	list		Definition of a roaming partner of this SEPP instance
name					Place for comment: to messages coming...
comment					is applied when...
firewall-profile-ref					it is applied when...
in-request-screening-case-ref					requests originate...
out-response-screening-case-ref					from the 3gpp-S...
routing-case-ref					ce to the install...
supports-target-apiroot					ce to the install...
trusted-cert-in-list-ref					tificate group d...
trusted-cert-out-list-ref					
trusted-certificate-list					
user-label					
n32-c					
enabled					Procedure be...
nf-pool-ref					r disable N32-c ..
allow-plmn					artner.
security-negotiation-data					N IDs of the roa...
domain-name					dshake proced...
global-ingress-rate-limit-profile-ref					ociated with. T...
topology-hiding-ref					le
subscriber-identifier					e for Pseudo Se...

**enabled**

A switch that allows the operator to enable or disable N32-c support for the roaming partner

Type: boolean

Config: true

**Default Value:** false

Constraint: N32-C functionality must be enabled first

Status: preliminary

Path: /sepp-function/nf-instance/external-network/roaming-partner/n32-c/enable

Full Path: /scsepp:sepp-function/scsepp:nf-instance/scsepp:external-network/scsepp:roaming-partner/scsepp:n32-c/scsepp:enabled

Module: ericsson-sepp

Comment by Andrei Mihalcea [ 2025-03-25 ]

Hi Rajan,

Thank you for raising this thing. Indeed, that configuration was missing. I've updated the Jinja Templates and pushed in GIT and soon will be merged in branch : UCC\_Appliance\_Sprint\_7

I've also tested and looks okey.

Thank you,

Andrei,

[UCC\_PLM-217] [UCC MCN: \[UCC 1.1\] SC incorrect vtap feature activation](#) Created: 2025-03-24 Updated: 2025-03-28 Resolved: 2025-03-25

Status:	Rejected
Project:	<a href="#">UCC_PLM</a>
Component/s:	None
Affects Version/s:	None
Fix Version/s:	None

Type:	Bug	Priority:	Medium
Reporter:	<a href="#">Rajan Rajeshprasad Gupta</a>	Assignee:	<a href="#">Andrei Mihalcea</a>
Resolution:	Rejected	Votes:	0
Labels:	None		
Remaining Estimate:	Not Specified		
Time Spent:	Not Specified		
Original Estimate:	Not Specified		

Attachments:	Enabled vTAP Lite SEPP.png 2025-03-25-16-19-02-937.png	image-2025-03-24-22-52-14-263.png	image-2025-03-25-16-07-42-099.png	image-2025-03-25-16-19-25-587.png	RE_question for vTAP support.msg
Sprint:	UCC XFT2 Sprint 7				
Team/s:	UCC_XFT2				
Found in Build:	UCC Appliance 1.1.0-drop.1				
Requirement Status:	UCC Appliance 0.2.1 - UNCOVERED				

#### Description

Hello,

SEPP has 2 vtap features.

1st - vtap light [ This does not required vtap consumer ]

2nd - vtap PVBT[ This does requires vtap consumer ]

Unfortunately, sc configuration has config for vtap PVBT which is useless as UCC customer will not have vTAP Consumers to decode pcaps.

vtap light is ideal vtap configuration which only requires sftp to store and decode pcap during roaming partners troubleshooting.

vTap light = Bulk tracing = vTap agent [ all 3 names are for same function ]

More info about vtap lite:

[https://calstore.internal.ericsson.com/elex?LI=600/LZN7940001/2\\*&FB=4\\_0\\_0&FN=2\\_15451-CSH109710\\_1-V1Uen.\\*.html&HT=owm1572421742059&DT=SC+Troubleshooting+Guideline](https://calstore.internal.ericsson.com/elex?LI=600/LZN7940001/2*&FB=4_0_0&FN=2_15451-CSH109710_1-V1Uen.*.html&HT=owm1572421742059&DT=SC+Troubleshooting+Guideline)

[https://calstore.internal.ericsson.com/elex?LI=600/LZN7940001/2\\*&FB=4\\_0\\_0&FN=1\\_1551-CSH109710\\_1-V1Uen.\\*.html&HT=xhj1634311204821&DT=Product+Overview](https://calstore.internal.ericsson.com/elex?LI=600/LZN7940001/2*&FB=4_0_0&FN=1_1551-CSH109710_1-V1Uen.*.html&HT=xhj1634311204821&DT=Product+Overview)

I checked helm get values of UCC 1.1 for sepp. I confirm, ucc 1.1 is using default helm chart values which has tapagent configured as false.

Function Area	Service	Parameter Name	Functionality	Mandatory	Description	Value
Signaling Controller	Security Edge Protection Proxy	eric-sepp.tapagent.manager.enabled	Feature Activation	No	Enables the vTAP agent in the SEPP manager pod.	Default: false
Signaling Controller	Security Edge Protection Proxy	eric-sepp.tapagent.worker.enabled	Feature Activation	No	Enables the vTAP agent in the SEPP worker pod.	Default: false

Please activate day0 configuration for sc for vtap light.

eric-sepp.tapagent.manager.enabled = true

eric-sepp.tapagent.worker.enabled = true

It means we can control the start and stop of vTAP lite through config map settings. Therefore, we can enable the vTAP lite feature from day 0 using Helm parameters, and activate it via the config map whenever packet capture is needed. Once the capture is complete, we can disable vTAP lite by reverting the config map settings.

Steps 4 and 5 can be used to toggle vTAP lite on or off as needed.

## Steps for vTAP Light activation

1# Day0 activation [ always keep true; eric-sepp.tapagent.worker.enabled=true ]

2# sftp secret creation [ always keep created for sftp of pcap ]

3# Create configmap for vTap light [ with false; "TAP\_ENABLED": false ]

4# Start vTap light by editing configmap[ enable by true ; "TAP\_ENABLED": true]

5# Stop vTAP light by editing configmap [ disable by false; "TAP\_ENABLED": false ]

6# View vTAP files in SFTP folder

### Comments

Comment by Andrei Mihalcea [ 2025-03-25 ]

Hi Rajan,

After discussing with you I've made one more try and for the moment looks okey.

So, I've enabled in day0 (values.yaml) the following 2 parameters (picture attached as well):

```

tapagent:
manager:
enabled: 'true'
worker:
enabled: 'true'

```

After this thing I've created the secret and CM that are mentioned in CPI and then all the PODs went UP and cnat pipeline installation was successful. I've created the secret PODs to come UP in order to insert the Day1 configurations (picture below when I have created the CM and Secret in CCD).

```

TEST SUITE: None
2025/03/25 13:42:19 INFO: /tmp/tmpzm7ufz_k/Definitions/OtherTemplates/eric-dsc-1.16.0-2-h2980dd2.tgz
2025/03/25 13:42:19 INFO: additional_values_flag: True
2025/03/25 13:42:19 INFO: No additional values file found.
2025/03/25 13:42:19 INFO: Skipping helm chart '/tmp/tmpzm7ufz_k/Definitions/OtherTemplates/eric-dsc-1.16.0-2-h2980dd2.tgz'
2025/03/25 13:42:19 INFO: Pipeline job 'step-4' succeeded
2025/03/25 13:42:19 INFO: Running pipeline job with timeout 3600 seconds
2025/03/25 13:42:19 INFO: ==> Running pipeline job 'step-5' using module 'verify-pod-running'
2025/03/25 13:42:19 INFO: Waiting for all Pods in Running status. (Ignoring: ['eric-sepp-worker'])
2025/03/25 13:42:19 WARNING: 14 Pods are not in Running status. Continue waiting
2025/03/25 13:42:50 WARNING: 9 Pods are not in Running status. Continue waiting
2025/03/25 13:43:22 WARNING: 8 Pods are not in Running status. Continue waiting
2025/03/25 13:43:53 WARNING: 5 Pods are not in Running status. Continue waiting
2025/03/25 13:44:25 WARNING: 3 Pods are not in Running status. Continue waiting
2025/03/25 13:44:56 WARNING: 2 Pods are not in Running status. Continue waiting
2025/03/25 13:45:28 WARNING: 2 Pods are not in Running status. Continue waiting
2025/03/25 13:45:59 WARNING: 1 Pods are not in Running status. Continue waiting
2025/03/25 13:46:20 INFO: All Pods are in Running status
2025/03/25 13:46:20 INFO: Pipeline job 'step-5' succeeded
2025/03/25 13:46:20 INFO: Running pipeline job with timeout 3600 seconds
2025/03/25 13:46:20 INFO: ==> Running pipeline job 'step-6' using module 'sleep'
2025/03/25 13:46:20 INFO: Wait 60 seconds to continue
2025/03/25 13:47:20 INFO: Pipeline job 'step-6' succeeded
2025/03/25 13:47:20 INFO: Running pipeline job with timeout 3600 seconds
2025/03/25 13:47:20 INFO: ==> Running pipeline job 'step-7' using module 'load-cmvp-user-config'
2025/03/25 13:47:20 INFO: Loading CMVP config from file: /home/eanimia/ucc-prod-dev/config/ccdb/sc/day1_security_sepp_users
2025/03/25 13:47:20 INFO: Opening a connection to 10.92.233.107:22
2025/03/25 13:47:25 INFO: Loaded configuration
2025/03/25 13:47:25 INFO: Pipeline job 'step-7' succeeded
2025/03/25 13:47:25 INFO: Pipeline job completed successfully after 3600 seconds

```

Below how I have created the CM and Secret :

## 1. Secret Creation

```

cat >> sftpConfig.json << EOF
[

{   "host": "localhost",    "sftpPort": 22,    "username": "udmuser1",    "password": "password1",    "uploadDir": "upload"  }

,

{   "host": "10.87.5.142",    "sftpPort": 22,    "username": "eanimia",    "password": "xxxxxxxxxx",    "uploadDir": "/home/eanimia/vTAP"  }

]
EOF

```

```
kubectl create secret generic sftp-server-config --from-file=sftpConfig.json -o yaml -n sc
```

## 2. CM Creation :

```
vi tap_config.json
```

insert the following content

```

[
{   "ServiceName": "eric-sepp-manager",    "TAP_ENABLED": false,    "TracingMode": "sftp",    "TAP_INT": "eth0",    "NF_TYPE": "sepp",    "TAI"
,

{   "ServiceName": "eric-sepp-worker",    "TAP_ENABLED": false,    "TracingMode": "sftp",    "TAP_INT": "eth0",    "NF_TYPE": "sepp",    "TAP_I
]
```

```
kubectl create -n sc cm eric-sc-tap-config --from-file tap_config.json
```

**NOTEs :**

1. As is mentioned in CPI, the TAP\_FILTER IP is the POD IP that can be found even by POD describe even by "kubectl get endpoints -n sc | grep worker" and "kubectl get end
2. TAP\_ENABLED should be put on TRUE when Traces wants to be collected
3. After any modification in this configmap it should be waited 1 min or something for the config to be taken. It can be checked in pod log (as is shown below) when the co
4. Also in SEPP CLI we should enable the vTAP :

```
sepp-function nf-instance deacucc3-sepp vtap enabled true
```

**Outputs :**

```
kubectl logs -n sc eric-sepp-worker-748998f98c-m6v97
```

```
[{"with server: 10.87.5.142"} {"version": "0.2.0", "timestamp": "2025-03-25T14:01:47.865527", "severity": "info", "service_id": "tap-agent", "metadata": {"function": "tap-agent"}, "h server 10.87.5.142 success."}] Start ssh authorization [{"version": "0.2.0", "timestamp": "2025-03-25T14:01:48.645055", "severity": "debug", "service_id": "tap-agent", "metadata": {"function": "tap-agent"}, "h server 10.87.5.142 success."}]
```

```
eanimia@ubuntu-jumphost2:~/vTAP$ ls -l
total 0
-rw-r--r-- 1 eanimia ucc 0 Mar 25 14:02 eric-sepp-manager-5bc69b7bd7-6zqsb-2025-03-25T14-02-07.pcap
-rw-r--r-- 1 eanimia ucc 0 Mar 25 14:01 eric-sepp-worker-748998f98c-m6v97-2025-03-25T14-01-48.pcap
eanimia@ubuntu-jumphost2:~/vTAP$
```

That's all, looks like is working.

Cheers,

Andrei,

---

Comment by [Rajan Rajeshprasad Gupta](#) [ 2025-03-25 ]

Thank you Andrei.

---

Comment by [Andrei Mihalcea](#) [ 2025-03-25 ]

Hi Rajan,

I've started to work on this case but in the meantime we found out that none of the vTAP type are in scope of the UCC in this moment (e-mail attached).

Anyway, I've made a quick test and looks that is not enough just to enable those 2 parameters, I think are also needed some certificates plus other stuffs. Also I'm not sure if sepp.tapagent.manager.enabled or we need also the eric-sepp.vtap.enabled (I would say that this one is for PVTB but not clear) and eric-sepp.tapcollector.worker.enabled (t

Anyway, for the moment looks that we will park this thing.

Cheers,

Andrei,

---

[\[UCC\\_PLM-215\] UCC MCN: \[UCC 1.1 \] ISP deployment not allowed in the default namespace.](#) Created: 2025-03-21 Updated: 2025-04-01 Resolved: 2025-04-01

Status:	Done
Project:	<a href="#">UCC_PLM</a>
Component/s:	None
Affects Version/s:	<a href="#">UCC Appliance 1.1.0</a>
Fix Version/s:	None

Type:	Bug	Priority:	Low
Reporter:	Houssem Marzouguia	Assignee:	Hector Caballero Rodriguez
Resolution:	Closed	Votes:	0
Labels:	None		

<b>Remaining Estimate:</b>	Not Specified
<b>Time Spent:</b>	Not Specified
<b>Original Estimate:</b>	Not Specified

<b>Issue Links:</b>	<b>Association</b>		
	Associates with	<a href="#">UCCXFT-843</a>	UCC1.1 drop2 - Fail to install ISP po...
<b>Sprint:</b>	UCC XFT4 Sprint 8		Done
<b>Epic Link:</b>	ISP tool UCC 1.1		
<b>Team/s:</b>	UCC_XFT4		
<b>Found in Build:</b>	UCC Appliance 1.1 - drop 1		
<b>Requirement Status:</b>	UCC Appliance 0.2.1 - UNCOVERED		

#### Description

<p>Hi,</p> <p>during the installation of the UCC 1.1 on MCN lab, we faced the below issue the installation of the ISP pod on the default namespace.</p> <p>the deployment of the ISP pod was failing due to the below error.</p> <p>disallow-k8s-default-namespace:  validate-podcontroller-namespace: 'validation error: Using "default" namespace  is not allowed for pod controllers. rule validate-podcontroller-namespace failed  at path /metadata/namespace/'</p> <p>the deployment was refused on the default namespace due the policy named "disallow-k8s-default-namespace" which prevents deploying resources into the default namespace.</p> <p>As a workaround, I've edited the policy by changing the validationFailureAction from <b>enforce</b> to <b>audit</b>.</p> <p>As a result the ISP POD was successfully installed on the default namespace.</p> <pre>eccd@ucc-ccdb:~&gt; kubectl get pods -n default NAME          READY   STATUS    RESTARTS   AGE ucc-isp-deployment-5f65bb764b-zqzh4  1/1     Running   0          23h</pre> <p>Could you please the workaround ? and check how to avoid the manual update of the policy?</p>
---

#### Comments

Comment by <a href="#">Hector Caballero Rodriguez</a> [ 2025-03-26 ]
Version <a href="#">0.0.192</a> fixes this issue as ISP is now deployed to the <i>ucc-isp</i> namespace.
Comment by <a href="#">Zhigang Han</a> [ 2025-03-21 ]
Hi Hector,
Quick update:
PLM also checked with I&V team about the issue. Here is the answer from I&V team:
we have the same problem with installing ISP in STC labs during UCC1.1 LFD1 deployment
Thanks,
BR/Zhigang
Comment by <a href="#">Soner Mus</a> [ 2025-03-21 ]
Hello,
Sorry for the confusion, assigned to the correct team.
Thanks
Comment by <a href="#">Meryam Nachi</a> [ 2025-03-21 ]
Hi, I am assigning the ticket to <a href="#">Soner Mus</a> as he is responsible for ISP.
Br, Meryam
Comment by <a href="#">Zhigang Han</a> [ 2025-03-21 ]
Hi Houssem,

as we discussed, the issue is only for UCC 1.1. I just checked UCC 1.0 CP1 system. We donot have any policy under the default namespace. I have assigned the ticket to the design.

Thanks,

BR/Zhigang

Comment by Houssem Marzouguia [ 2025-03-21 ]

adding the policy which is causing the failure:

```
eccc@ucc-ccdb:~> kubectl get policy disallow-k8s-default-namespace -n default -o yaml
apiVersion: kyverno.io/v1
kind: Policy
metadata:
  annotations:
    ccd.ericsson.com/last-applied-configuration: {"apiVersion":"kyverno.io/v1","kind":"Policy","metadata":{"annotations":{"ccd/addon":"kyverno","ericsson.ccd.workload.io/management":"True","pod-policies.kyverno.io/autogen-controllers":"none","policies.kyverno.io/category":"Multi-Tenancy","policies.kyverno.io/description":"Kubernetes Namespaces are an optional feature that provide a way to segment and isolate cluster resources across multiple applications and users. As a best practice, workloads should be isolated with Namespaces. Namespaces should be required and the default (empty) Namespace should not be used. This policy validates that Pods specify a Namespace name other than `default`. Rule auto-generation is disabled here due to Pod controllers need to specify the `namespace` field under the top-level `metadata` object and not at the Pod template level."}, "policies.kyverno.io/minversion":"1.6.0","policies.kyverno.io/severity":"medium","policies.kyverno.io/subject":"Pod","policies.kyverno.io/title":"Disallow Default Namespace"}}
    "name": "disallow-k8s-default-namespace",
    "namespace": "default",
    "spec": {
      "background": false,
      "rules": [
        {
          "match": {
            "any": [
              {
                "resources": {
                  "kinds": ["Pod"]
                }
              }
            ]
          },
          "name": "validate-pod-namespace"
        }
      ],
      "validate": {
        "message": "Using 'default' namespace is not allowed for pods."
      }
    }
  }
  "ccd/addon": "kyverno"
  "ericsson.ccd.workload.io/management": "True"
  "pod-policies.kyverno.io/autogen-controllers": "none"
  "policies.kyverno.io/category": "Multi-Tenancy"
  "policies.kyverno.io/description": "Kubernetes Namespaces are an optional feature that provide a way to segment and isolate cluster resources across multiple applications and users. As a best practice, workloads should be isolated with Namespaces. Namespaces should be required and the default (empty) Namespace should not be used. This policy validates that Pods specify a Namespace name other than `default`. Rule auto-generation is disabled here due to Pod controllers need to specify the `namespace` field under the top-level `metadata` object and not at the Pod template level."
  "policies.kyverno.io/minversion": "1.6.0"
  "policies.kyverno.io/severity": "medium"
  "policies.kyverno.io/subject": "Pod"
  "policies.kyverno.io/title": "Disallow Default Namespace"
  "creationTimestamp": "2025-03-17T15:42:49Z"
  "generation": 2
  "name": "disallow-k8s-default-namespace"
  "namespace": "default"
  "resourceVersion": "2455043"
  "uid": "28a2e42e-9cec-4a45-ba5d-69cecd31059f"
spec:
  admission: true
  background: false
  emitWarning: false
  rules:
  - match:
    any:
    - resources:
      kinds:
      - Pod
    name: validate-pod-namespace
    skipBackgroundRequests: true
    validate:
      allowExistingViolations: true
      message: Using 'default' namespace is not allowed for pods.
      pattern:
        metadata:
          namespace: '!default'
    - match:
      any:
```

```

- resources:
  kinds:
    - DaemonSet
    - Deployment
    - Job
    - ReplicaSet
    - ReplicationController
    - StatefulSet
    - CronJob
name: validate-podcontroller-namespace
skipBackgroundRequests: true
validate:
allowExistingViolations: true
message: Using 'default' namespace is not allowed for pod controllers.
pattern:
metadata:
  namespace: '!default'
validationFailureAction: Audit
status:
autogen: {}
conditions:
- lastTransitionTime: "2025-03-17T16:00:27Z"
  message: Ready
  reason: Succeeded
  status: "True"
  type: Ready
rulecount:
  generate: 0
  mutate: 0
  validate: 2
  verifyimages: 0
validatingadmissionpolicy:
  generated: false
  message: ""

```

<a href="#">[UCC_PLM-214] MANA BAH+Tmo :Redundant routing-indicator in AUSF leads to Profile A/B discovery failure for actual UEs</a>	
Created: 2025-03-19 Updated: 2025-04-24	
<b>Status:</b>	Done
<b>Project:</b>	<a href="#">UCC_PLM</a>
<b>Component/s:</b>	None
<b>Affects Version/s:</b>	None
<b>Fix Version/s:</b>	None

<b>Type:</b>	Bug	<b>Priority:</b>	Medium
<b>Reporter:</b>	<a href="#">Rajan Rajeshprasad Gupta</a>	<b>Assignee:</b>	<a href="#">Alvaro Martin</a>
<b>Resolution:</b>	Closed	<b>Votes:</b>	0
<b>Labels:</b>	None		
<b>Remaining Estimate:</b>	Not Specified		
<b>Time Spent:</b>	Not Specified		
<b>Original Estimate:</b>	Not Specified		

<b>Attachments:</b>	 BAH-ProfileA-Ok(Identity-response#553,554)-16-08-2024.pcap.pcapng 2025-03-19-18-39-15-269.png	 image-2025-03-19-18-37-35-505.png	 image-
<b>Sprint:</b>	UCC XFT2 Sprint 8, UCC XFT2 Sprint 9		
<b>Team/s:</b>	UCC_XFT2		
<b>Found in Build:</b>	UCC 1.0		
<b>Requirement Status:</b>	UCC Appliance 0.2.1 - UNCOVERED		

#### Description

Hello,

The default AUSF configuration within UCC statically sets the routing indicator to '0.' See details below:

```
ausf nf-profile ausf-info routing-indicator [ 0 ]
```

When working with real devices such as Cradlepoint or Samsung, the UE sent the routing indicator as '0000,' while AUSF was configured with '0.' This mismatch prevented successful AUSF discovery via NRF, which responded with 200 OK without AUSF information.

This is leading to failure of AUSF and 5G SA registration.

**Current work-around added for both BAH and Tmo :**

```
show run ausf nf-profile ausf-info| in routing-indicator
```

```
config; no ausf nf-profile ausf-info routing-indicator ; commit;
```

I recommend removing the redundant routing-indicator configuration in AUSF to prevent discovery failures for Profile A and Profile B SUCI for real UE based on device behavior for new UCC deliveries.

**Comments**

---

Comment by [Alvaro Martin](#) [ 2025-04-08 ]

For UCC1.1 I have added a new variable in LLD to define the routing indicator as it's a customer defined parameter. Then in CCSM configuration, the routing indicator will be defined by this variable. This is already pushed to integration branch in UCC1.1

---

Comment by [Zhigang Han](#) [ 2025-03-19 ]

Hi Rajan,

It is the configuration mismatching case for me. Other customers are ok with the configuration, however we ran into the trouble with TMO. I have assigned the ticket to the TMO team.

If the customer should not update the default configuration, it should count as a bug because our configuration didnot cover all the cases.

Thanks,

BR/Zhigang

---

Comment by [Rajan Rajeshprasad Gupta](#) [ 2025-03-19 ]

Attached is the working PCAP file after the fix. Previously, when mTLS was enabled, UETrace did not capture any data and ITC contained encrypted information that couldn't be decrypted.

BAH-ProfileA-Ok(Identity-response#553,554)-16-08-2024.pcap.pcapng [UE Trace]

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/>

Time	ID	Source	Destination	Protocol	Com	AVP	Result	Fran	HI (Hand)	5GS	RAT	F-TEID	IPv4	Origin-R	O
550 2024-08-16 19:34:22.458000		UE		NAS-5GS/NAS...				123	in...						
551 2024-08-16 19:34:22.459000			UE	NAS-5GS						43					
552 2024-08-16 19:34:22.459000				NGAP/NAS-5GS						62					
553 2024-08-16 19:34:22.573000				NGAP/NAS-5GS						146					
554 2024-08-16 19:34:22.573000		UE		NAS-5GS						104					
555 2024-08-16 19:34:22.573000			10.136.160.217	172.16.5.112	HTTP2					555					
556 2024-08-16 19:34:22.575000			172.16.5.112	10.136.160.217	HTTP2/JSON					979					
557 2024-08-16 19:34:22.592000			10.136.160.217	172.16.5.108	HTTP2/JSON					369					
558 2024-08-16 19:34:22.610000			172.16.5.108	10.136.160.217	HTTP2/JSON					720					

< Frame 554: 104 bytes on wire (832 bits), 104 bytes captured (832 bits) on interface unknown, id 0

> EXPORTED\_PDU

Non-Access-Stratum 5GS (NAS)PDU

- Security protected NAS 5GS message
  - Extended protocol discriminator: 5G mobility management messages (126)
    - 0000 .... = Spare Half Octet: 0
    - .... 0001 = Security header type: Integrity protected (1)
    - Message authentication code: 0x061b4005
    - Sequence number: 79
- Plain NAS 5GS Message
  - Extended protocol discriminator: 5G mobility management messages (126)
    - 0000 .... = Spare Half Octet: 0
    - .... 0000 = Security header type: Plain NAS message, not security protected (0)
    - Message type: Identity response (0x5c)
- 5GS mobile identity
  - Length: 53
    - 0... .... = Spare: 0
    - .000 .... = SUPI format: IMSI (0)
    - .... 0... = Spare: 0
    - .... .001 = Type of identity: SUCI (1)
    - Mobile Country Code (MCC): United States (315)
    - Mobile Network Code (MNC): Unknown (010)
    - Routing indicator: 0000
      - .... 0001 = Protection scheme Id: ECIES scheme profile A (1)
    - Home network public key identifier: 4

> Scheme output: 4030a4eb8419cac94c977669d274bb7bfed459065921ea24520a130ab3d52b5f01f4b9a3c7025808fe834093d2

BAH-ProfileA-Ok(Identity-response#553,554)-16-08-2024.pcap.pcapng [UE Trace]

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/>

Protocol	Com	AVP	Result	Fran	HI (Hand)	5GS	RAT	F-TEID	IPv4	Origin-R	Orig	Dest	Type	Info
NAS-5GS/NAS...				123		in...							5G...	Registration request
NAS-5GS						43							SU...	Identity request
NGAP/NAS-5GS						62							SU...	DownlinkNASTransport, Identity request
NGAP/NAS-5GS						146							SU...	UplinkNASTransport, Identity response
NAS-5GS						104							SU...	Identity response
HTTP2						555							HEADERS[181]: GET /nrrf-disc/v1/nf-instances?service-names=nausf-auth	
HTTP2/JSON						979							HEADERS[181]: 200 OK, DATA[181], JSON (application/json)	
HTTP2/JSON						369							HEADERS[1]: POST /nausf-auth/v1/ue-authentications, DATA[1], JSON (application/json)	
HTTP2/JSON						720							HEADERS[1]: 201 Created, DATA[1], JSON (application/json)	
...	...	...	...	...	...	...	...	...	...	...	...	...	...	...

... Stream: HEADERS, Stream ID: 181, Length 501, GET /nrrf-disc/v1/nf-instances?service-names=nausf-auth&target-nf-type=AUSF&requester-nf-type=AMF&requester-nf-instance-fqdn=pcc-bahucc01b

Length: 501  
Type: HEADERS (1)  
Flags: 0x05, End Headers, End Stream  
0... .... .... .... .... .... = Reserved: 0x0  
.000 0000 0000 0000 0000 1011 0101 = Stream Identifier: 181  
[Pad Length: 0]  
Header Block Fragment [...]: 86447fb3022f6e6e72662d646973632f76312f6e662d696e7374616e6365733f736572766963652d6e616d65733d6e617573662d6175746826746172676574  
[Header Length: 581]  
[Header Count: 5]  
Header: :scheme: http  
Header: :path: /nrrf-disc/v1/nf-instances?service-names=nausf-auth&target-nf-type=AUSF&requester-nf-type=AMF&requester-nf-instance-fqdn=pcc-bahucc01b.amf.5gc.mnc01  
Name Length: 5  
Name: :path  
Value Length: 434  
Value [...]: /nrrf-disc/v1/nf-instances?service-names=nausf-auth&target-nf-type=AUSF&requester-nf-type=AMF&requester-nf-instance-fqdn=pcc-bahucc01b.amf.5gc.mnc01  
:path [...]: /nrrf-disc/v1/nf-instances?service-names=nausf-auth&target-nf-type=AUSF&requester-nf-type=AMF&requester-nf-instance-fqdn=pcc-bahucc01b.amf.5gc.mnc01  
Request URI Path: /nrrf-disc/v1/nf-instances  
Request URI Query [...]: service-names=nausf-auth&target-nf-type=AUSF&requester-nf-type=AMF&requester-nf-instance-fqdn=pcc-bahucc01b.amf.5gc.mnc01  
Request URI Query Parameter: service-names=nausf-auth  
Request URI Query Parameter: target-nf-type=AUSF  
Request URI Query Parameter: requester-nf-type=AMF  
Request URI Query Parameter: requester-nf-instance-fqdn=pcc-bahucc01b.amf.5gc.mnc010.mcc315.3gppnetwork.org  
Request URI Query Parameter: requester-nf-instance-id=d67766fc-210f-4ecf-858f-000000a1c1d2  
Request URI Query Parameter: target-pimn-list=%5B%7B%22mcc%22%3A%22315%22%2C%22mnc%22%3A%222010%22%7D%5D  
Request URI Query Parameter: requester-pimn-list=%5B%7B%22mcc%22%3A%22315%22%2C%22mnc%22%3A%222010%22%7D%5D  
Request URI Query Parameter: routing-indicator=0000  
Request URI Query Parameter: preferred-locality=ccdb  
[Unescaped [...]: /nrrf-disc/v1/nf-instances?service-names=nausf-auth&target-nf-type=AUSF&requester-nf-type=AMF&requester-nf-instance-fqdn=pcc-bahucc01b.amf.5gc.mnc01  
Representation: Literal Header Field with Incremental Indexing - Indexed Name  
Index: 4  
Header: :method: GET  
Header: :authority: nrf-ccrc-bahucc01b.5gc.mnc010.mcc315.3gppnetwork.org:443  
Header: content-length: 0  
[Response in frame: 556]  
[Full request URI [...]: http://nrf-ccrc-bahucc01b.5gc.mnc010.mcc315.3gppnetwork.org:443/nrrf-disc/v1/nf-instances?service-names=nausf-auth&target-nf-type=AUSF&requester-nf-type=AMF&requester-nf-instance-fqdn=pcc-bahucc01b.amf.5gc.mnc010.mcc315.3gppnetwork.org:443]

BAH-ProfileA-Ok(Identity-response#553,554)-16-08-2024.pcap.pcapng

[UCC\_PLM-213] Firmware upload failed because wrong jumphost port is used Created: 2025-03-18 Updated: 2025-04-17 Resolved: 2025-03-21

Status:	Done
Project:	UCC_PLM

<b>Component/s:</b>	None
<b>Affects Version/s:</b>	None
<b>Fix Version/s:</b>	None

<b>Type:</b>	Bug	<b>Priority:</b>	Low
<b>Reporter:</b>	<a href="#">Bengt-Dirk Heye</a>	<b>Assignee:</b>	Unassigned
<b>Resolution:</b>	Closed	<b>Votes:</b>	0
<b>Labels:</b>	None		
<b>Remaining Estimate:</b>	Not Specified		
<b>Time Spent:</b>	Not Specified		
<b>Original Estimate:</b>	Not Specified		

<b>Attachments:</b>	 CNAT_install_ccd_None_20250312155809.log	 image-2025-03-18-11-49-54-179.png
<b>Team/s:</b>	UCC_XFT3	
<b>Workaround:</b>	Temporarily we added port 8080 in our apache2 configuration: Listen 8080 (in port.config) <VirtualHost *:80 *:8080> (in sites-available/000-default.conf)	
<b>Found in Build:</b>	UCC 1.1 LFD1, CNAT Version: dev-development-bec8be21	
<b>Requirement Status:</b>	UCC Appliance 0.2.1 - UNCOVERED	

### Description

In the Site Data tab of our LLD document we specified:

```
jump host server IP      jumphost_ip      10.87.39.40
Web server http port    webserver_port   80
```

and this IP with port 80 is actually used, e.g., during CCD installation:

```
2025/03/13 00:22:20 INFO [orchestrator.ccdadm.install:144]: config_drive_image_url: http://10.87.39.40:80/config-drive-ucc1b.img
```

However, when triggering the firmware upgrade with cnat:

```
cnat --install --no-cfggen --vnf-info vnf-server.yaml --no-env-file
```

the script:

```
pipeline/server_configuration_firmware_upgrade.py
```

is executed and leads to the below Error:

```
2025/03/12 15:58:52 ERROR [utils.redfish.upload_firmware:458]: Error in upload_firmware: Firmware upload failed after 5.08 seconds. Task State: Exception, Messages: [{"MessageArgs": ["http://10.87.39.40:8080/26_41_1"], "MessageId": "Base.1.18.CouldNotEstablishConnection"}]
```

The executed script has the port 8080 hardcoded:

```
158:     else:
159:         base_url = f"http://{jumphost_ip}:8080"
```

Port 8080 is not in use in our webhost.

### Comments

Comment by [Zhigang Han](#) [2025-03-18]

Hi there,

when we prepared for the jumphost, there was one file to set the value of the port on the jumphost:

```
/etc/apache2/sites-available/000-default.conf
```

```
stcucc3@seroious08732:~$ more /etc/apache2/sites-available/000-default.conf
<VirtualHost *:8080>
    # The ServerName directive sets the re
    # the server uses to identify itself.
    # redirection URLs. In the context of
    # specifies what hostname must appear
    # match this virtual host. For the def
    # value is not decisive as it is used
    # However, you must set it for any fur
    #  
#ServerName www.example.com

    ServerAdmin webmaster@localhost
    DocumentRoot /local/software-ucc1.1/CCD/

    # Available loglevels: trace8, ..., tr
    # error, crit, alert, emerg.
    # It is also possible to configure the
    # modules, e.g.
    #LogLevel info ssl:warn

    ErrorLog ${APACHE_LOG_DIR}/error.log
    CustomLog ${APACHE_LOG_DIR}/access.log

    # For most configuration files from co
    # enabled or disabled at a global leve
    # include a line for only one particul
    # following line enables the CGI confi
    # after it has been globally disabled
    #Include conf-available/serve-cgi-bin.
</VirtualHost>
```

Make sure LLD is matching the port setting from /etc/apache2/sites-available/000-default.conf port value.

I have assigned the ticket to the design. I believe we need to update UCC 1.1.0 II which we need to have this checking information in chapter 7 jumphost preparation.

Thanks,  
BR/Zhigang

[UCC_PLM-212] UCC MCN: [UCC 1.1 ] CCD installation failed	
<b>Status:</b>	Rejected
<b>Project:</b>	<a href="#">UCC_PLM</a>
<b>Component/s:</b>	None
<b>Affects Version/s:</b>	<a href="#">UCC Application 1.1.0</a> , <a href="#">UCC Appliance 1.1.0</a>
<b>Fix Version/s:</b>	None

<b>Type:</b>	Bug	<b>Priority:</b>	Medium
<b>Reporter:</b>	<a href="#">Houssem Marzouqua</a>	<b>Assignee:</b>	<a href="#">Meryam Nachi</a>
<b>Resolution:</b>	Rejected	<b>Votes:</b>	0
<b>Labels:</b>	None		
<b>Remaining Estimate:</b>	Not Specified		
<b>Time Spent:</b>	Not Specified		
<b>Original Estimate:</b>	Not Specified		

<b>Attachments:</b>	<a href="#"> CNAT_install_ccd_None_20250314105618.log</a>	<a href="#"> journalctl-logs.txt</a>
<b>Team/s:</b>	<a href="#">UCC_XFT2</a>	
<b>Severity_qmt:</b>	2- High	
<b>Found in Build:</b>	<a href="#">UCC Appliance 1.1</a>	
<b>Requirement Status:</b>	<a href="#">UCC Appliance 0.2.1 - UNCOVERED</a>	

#### Description

hello,

we are deploying UCC1.1 in our MCN lab and CCD installation is failing.

please find below the error:

```
home/ecccd/.kube/config: No such file or directoryscp: /home/ecccd/.kube/config: No such file or directoryscp: /home/ecccd/.kube/config: No such file or directoryERROR: This is not the first error, check the logs for "WARNING: #1"
```

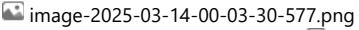
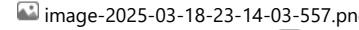
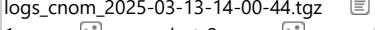
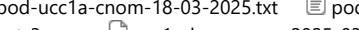
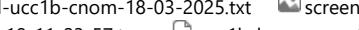
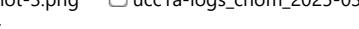
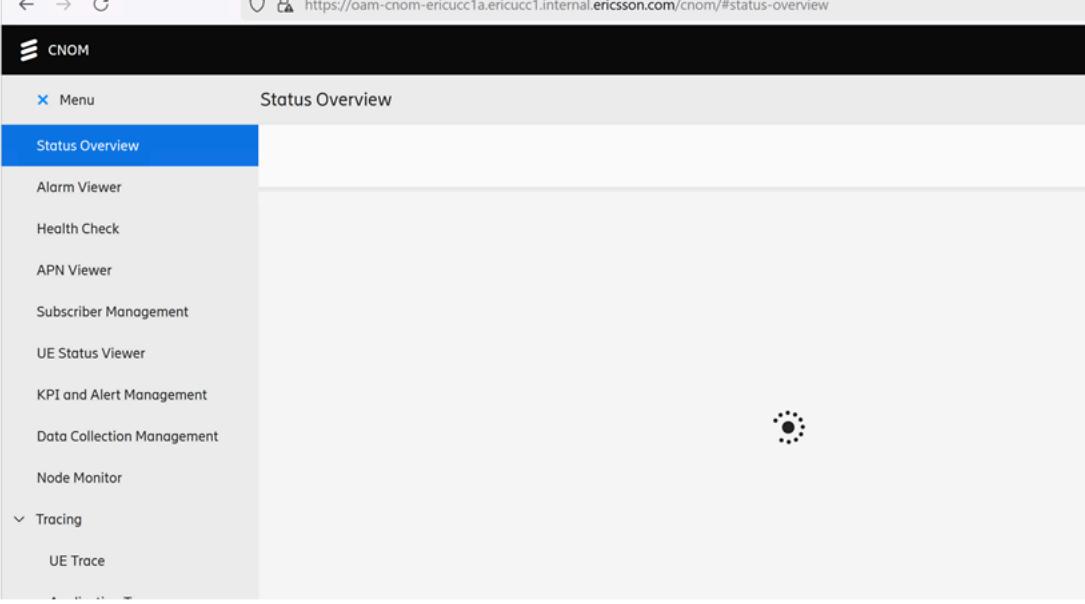
please attached cnat logs.

thanks, Br,

Houssem.

#### Comments

Comment by <a href="#">Houssem Marzouqua</a> [ 2025-03-17 ]
Hi Zhigang,
the issue was in the environment of our lab.
please close/reject the ticket.
Thanks.
Houssem.
Comment by <a href="#">Zhigang Han</a> [ 2025-03-14 ]
Hi Houssem,
as we discussed from our call, once you confirmed the solution from the design team, you will update the ticket from your side.
According to Houssem, the issue is related to use the wrong certificates during the deployment.
As we agreed on, I have lowered the priority from high to medium level.
Thanks,
BR/Zhigang

[UCC_PLM-211] MANA Vz : Too slow cnom/not working <small>Created: 2025-03-13 Updated: 2025-05-09 Resolved: 2025-05-09</small>						
<b>Status:</b>	Done					
<b>Project:</b>	<a href="#">UCC_PLM</a>					
<b>Component/s:</b>	None					
<b>Affects Version/s:</b>	None					
<b>Fix Version/s:</b>	None					
<b>Type:</b>	Bug	<b>Priority:</b>	Low			
<b>Reporter:</b>	<a href="#">Rajan Rajeshprasad Gupta</a>	<b>Assignee:</b>	<a href="#">Christos Delis (EXT)</a>			
<b>Resolution:</b>	Closed	<b>Votes:</b>	0			
<b>Labels:</b>	None					
<b>Remaining Estimate:</b>	4h					
<b>Time Spent:</b>	Not Specified					
<b>Original Estimate:</b>	4h					
<b>Attachments:</b>	           					
<b>Sprint:</b>	UCC XFT3 Sprint 7, UCC XFT3 Sprint 8, UCC XFT3 Sprint 9					
<b>Team/s:</b>	UCC_XFT3					
<b>Found in Build:</b>	UCC 1.0.CP1					
<b>Requirement Status:</b>	UCC Appliance 0.2.1 - UNCOVERED					
<b>Description</b>						
<p>Hello,</p> <p>cnom are running slow and take forever to refresh and load a page.</p> <p>This issue seems to be getting worse in the past few days, clear cache does not help.</p>						
						

The screenshot shows a browser window with the URL <https://oam-cnom-ericucc1a.ericucc1.internal.ericsson.com/cnom/#status-overview>. The title bar says "CNOM". The left sidebar has a blue header "Status Overview" and a list of modules: Alarm Viewer, Health Check, APN Viewer, Subscriber Management, UE Status Viewer, KPI and Alert Management, Data Collection Management, Node Monitor, Tracing, UE Trace, and Application Trace. The main content area has a red warning icon and the text "App not found" followed by "Failed to dynamically import 'StatusOverview'. Details: Unable to resolve specifier 'StatusOverview.js' imported from https://oam-cnom-ericucc1a.ericucc1.internal.ericsson.com/cnom/node\_modules/@eui/container/index.js".

Q1: Is this a known bug?

Q2: What steps can be taken to ensure CNOM functions normally?

Initial analysis indicate pod "eric-data-object-storage-mn-0" is restarting in high number due to OOM.

```
eccd@ucc-ccda:~> kubectl get pod -n cnom
NAME                               READY   STATUS    RESTARTS   AGE
eric-cm-mediator-869586b989-nbl5p      1/1    Running   11 (6d ago)   106d
eric-cm-mediator-db-pg-0            3/3    Running   33 (6d ago)   106d
eric-cm-mediator-db-pg-bragent-9789dfc4d-hm4wv  3/3    Running   33 (6d ago)   106d
eric-cm-mediator-key-init-x56jw     0/1    Completed  0          106d
eric-cm-mediator-notifier-589fb46d94-mk7hr  1/1    Running   11 (6d ago)   106d
eric-cnom-data-ingester-6dcbc55cd8-58l19  2/2    Running   22 (6d ago)   106d
eric-cnom-document-database-mg-7bb89d9985-zsptf  2/2    Running   22 (6d ago)   106d
eric-cnom-document-database-mg-bragent-64cb9d4969-zvkm2  2/2    Running   22 (6d ago)   106d
eric-cnom-server-57bd4447c-fztq8       2/2    Running   22 (6d ago)   106d
eric-cnom-stream-receiver-66bf486f69-jbh8m     2/2    Running   33 (6d ago)   106d
eric-ctrl-bro-7fc4ccfcf8-cfzcq      1/1    Running   11 (6d ago)   106d
eric-data-distributed-coordinator-ed-0    2/2    Running   22 (6d ago)   106d
eric-data-distributed-coordinator-ed-agent-c658d6778-dtwg2  2/2    Running   22 (6d ago)   106d
eric-data-key-value-database-rd-6f777d855f-qtzv5  1/1    Running   12 (6d ago)   106d
eric-data-key-value-database-rd-operand-dtrp7    2/2    Running   22 (6d ago)   106d
eric-data-key-value-database-rd-operand-n5sp4    2/2    Running   22 (6d ago)   106d
eric-data-object-storage-mn-0        2/2    Running   421 (8m43s ago) 106d
eric-data-object-storage-mn-mgt-78dfb5c758-rcsb6  3/3    Running   33 (6d ago)   106d
eric-sec-certm-75f478cf68-jrtx2      1/1    Running   11          106d
eric-sec-key-management-job-jli9l-dc6m9      0/1    Completed  0          106d
eric-sec-key-management-main-0        3/3    Running   33 (6d ago)   106d
eric-sec-sip-tls-main-766496558c-jkxjk  3/3    Running   33 (6d ago)   106d
eric-sec-sip-tls-main-766496558c-wqzsp  3/3    Running   33 (6d ago)   106d
eric-tm-ingress-controller-cr-contour-v1-dc5f9c58d-c4r9v  2/2    Running   22 (6d ago)   106d
eric-tm-ingress-controller-cr-contour-v1-dc5f9c58d-p5k5m  2/2    Running   22 (6d ago)   106d
eric-tm-ingress-controller-cr-envoy-ml9vc     2/2    Running   22 (6d ago)   106d
eccc@ucc-ccda:~> ./collect_adp_logs.sh cnom
```

Attached ADP logs and Pod logs.

[logs\\_cnom\\_2025-03-13-14-00-44.tgz](#)

## Comments

Comment by Christos Delis (EXT) [2025-05-09]

Hello Zhigang Han,

No there is no update on top of this ticket.

We have added a note for the Retention Time on Installation Guide.

We could close the ticket.

BRs,  
Christos

Comment by [Zhigang Han](#) [ 2025-05-08 ]

Hi Christos,

Do we have any update for this ticket? Could we close this ticket?

Thanks,

BR/Zhigang

Comment by [Christos Delis \(EXT\)](#) [ 2025-04-04 ]

Hello [Zhigang Han](#),

Yes, could be a good option to include it on our troubleshooting guide, but i think in order to prevent this issue maybe is better to have it as a note in our Installation Guide Let me discuss it further with the Program and will let you know.

Thanks in advance.

BRs,  
Christos.

Comment by [Zhigang Han](#) [ 2025-04-03 ]

hi Christos,

Maybe we could have one chapter as troubleshooting guide. In this chapter, we could add some known issues and add the note for this cnom retention parameter update. I troubleshoot chapter in our installation guide when they face the issue.

Thanks,

BR/Zhigang

Comment by [Christos Delis \(EXT\)](#) [ 2025-04-03 ]

Hello [Zhigang Han](#),

I made a Note (Recommendation) on our Installation Guide on Section 17, where information for Local OAM is described, as it shown on below figure:



What do you think on this approach?

Thank you in advance.

Brs,  
Christos

Comment by [Zhigang Han](#) [ 2025-04-02 ]

Hi Christos,

I think at this point, we could add post-installation procedure as the suggestion to update the retention configuration in the deployment instruction as you mentioned.

Thanks,

BR/Zhigang

Comment by [Christos Delis \(EXT\)](#) [ 2025-04-02 ]

Hello [Rajan Rajeshprasad Gupta](#),

Unfortunately, there is no way to implement automatically via deployment those settings as those can be done only via GUI.

As long as you are observing this behavior, i think maybe the best option is to include this procedure as default settings in our Installation and Integrated Local Manager

BRs,  
Christos

Comment by [Rajan Rajeshprasad Gupta](#) [ 2025-04-02 ]

Hello Christos Delis (EXT)

Thank you for feedback on work-around. I reduce priority to low for ticket.

I am concerned about starting UCC deployment, as we are experiencing OSMN crashes despite having minimal production traffic on CNOM.

Once UCC customers begin running committed traffic of 3,000-5,000 UEs and utilize UEtrace, their CNOM systems may crash.

Is there a way to set the default retention of CNOM data to the lowest setting to prevent complaints?

eg.

FM and PM KPI = 24 hours

PM counters = 24 Hours

UEtrace data = 2 Hours

Continuous UE trace = 10minutes

Automatic data collection hours = 24 hours

Automatic Healthcheck reports =24 hours

Delete manual healthcheck report = on

Delete save UE trace files = on

---

Comment by Christos Delis (EXT) [ 2025-04-02 ]

Hello Rajan Rajeshprasad Gupta,

Thanks.

FYI: by restarting cnom-server pod issue has been resolved in our side.

As CNOM 1 is low prioritized should we close that ticket?

BRs,

Christos

---

Comment by Rajan Rajeshprasad Gupta [ 2025-04-01 ]

Hello Christos Delis (EXT)

Since CNOM Server 2 is functioning properly, Vz is conducting tests on this server. Troubleshooting CNOM Server 1 is a low priority, as we plan to reinstall UCC next month

Sorry, no feedback for suggested option for CNOM server 1 fix as that is low priority now.

---

Comment by Christos Delis (EXT) [ 2025-04-01 ]

Hello Rajan Rajeshprasad Gupta,

In our lab we observed below issue for the first time, as you had already mentioned some time ago.



As we don't have a lot of evidence for the root cause of this issue, do you know if this issue has been resolved?

BRs,

Christos

---

Comment by Christos Delis (EXT) [ 2025-03-24 ]

Hello Rajan Rajeshprasad Gupta

Do you have any updates from the customer related this issue?

BRs,

Christos

---

Comment by Christos Delis (EXT) [ 2025-03-19 ]

Hello Rajan Rajeshprasad Gupta,

No, we have not encounter that issue before.

Have you tried to restart eric-cnom-server on UCC1a where you are getting 504 error?

Please, if you manage to login after the restart of cnom-server, provide the below Retention configurations, as on UCC1b, to check if eric-data-storage-mn-0 will be stable.

BRs,

Christos

---

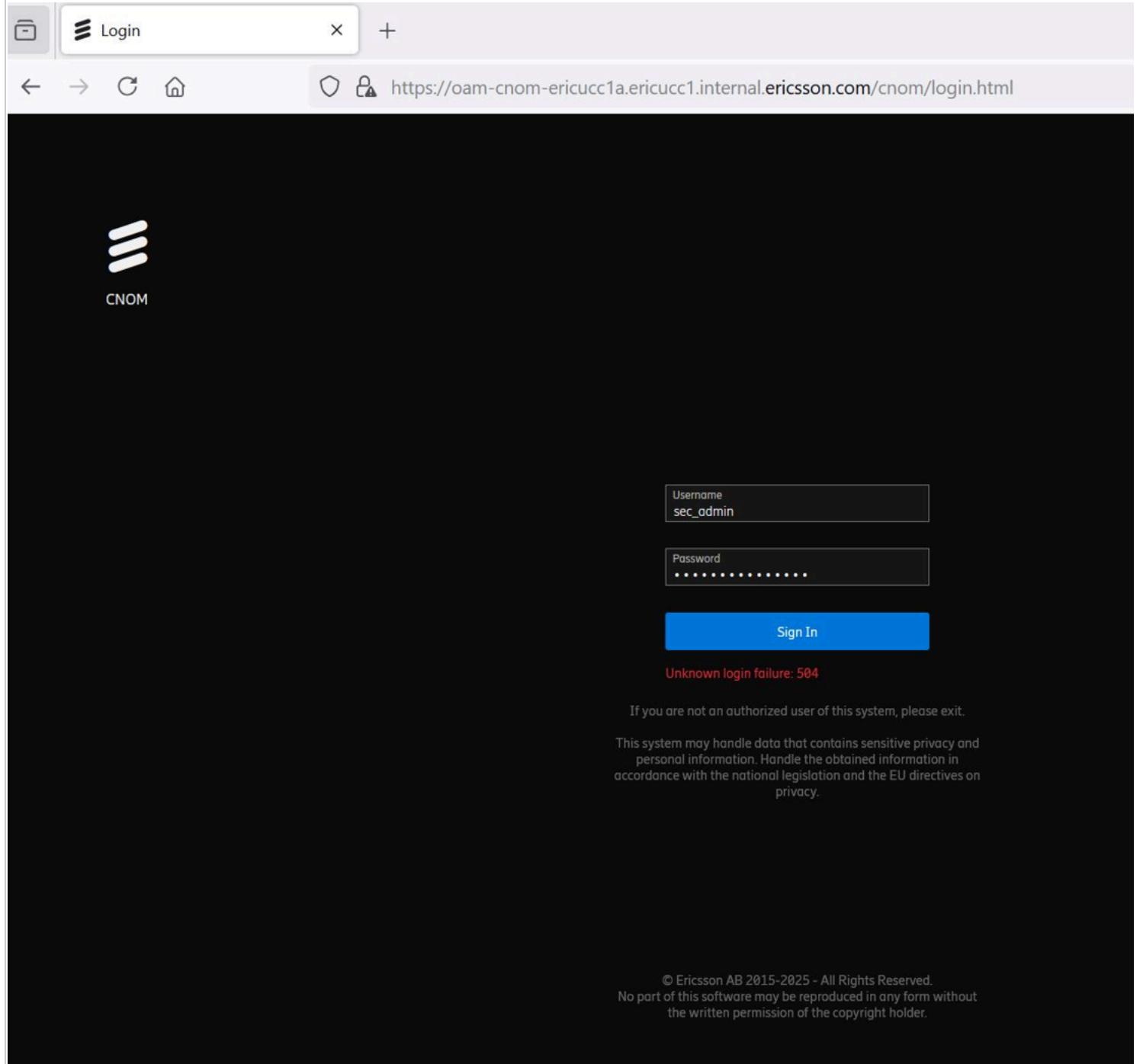
Comment by Rajan Rajeshprasad Gupta [ 2025-03-18 ]

Hello Christos Delis (EXT)

Received feedback from Vz.

CNOM - UCC1B // They have applied log retention as suggested. They will feedback after few days feedback on slowness.

CNOM - UCC1A // Primary site where issue is observed, This CNOM is nomore accessible and we are getting : "Unknown login failure : 504 ".



Did we observed such error in past?

attached adp logs for both UCC1A and UCC1B.

I observed eric-data-object-storage-mn-0 is still restarting in UCC1A CNOM and Stable in UCC1B CNOM

[pod-ucc1a-cnom-18-03-2025.txt](#)

[pod-ucc1b-cnom-18-03-2025.txt](#)

[ucc1a-logs\\_cnom\\_2025-03-18-11-23-57.tgz](#)

[ucc1b-logs\\_cnom\\_2025-03-18-11-19-06.tgz](#)

Comment by [Rajan Rajeshprasad Gupta](#) [2025-03-17]

Thank you.

Requested customer to change default value to as below;

FM and PM KPI = 24 hours

PM counters = 24 Hours

UEtrace data = 2 Hours

Continuous UE trace = 10minutes

Automatic data collection hours = 24 hours

Automatic Healthcheck reports =24 hours

Delete manual healthcheck report = on

Delete save UE trace files = on

Will update once get feedback from them.

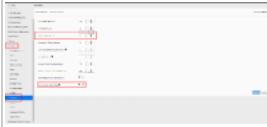
Comment by Christos Delis (EXT) [ 2025-03-17 ]

Hello Rajan Rajeshprasad Gupta,

Regarding your described scenario should be a very possible explanation as we have not observed this situation before.

According CPI, this issue may occur due to the default Retention Time on two parameters "UE Trace Data" and "Delete Saved UE Trace Files", [https://cpistore.internal.ericsson.com/LXA1191071\\_1Uen.X.html&HT=iiu1657861852981&DT=Cloud+Native+CNOM+User+Guide](https://cpistore.internal.ericsson.com/LXA1191071_1Uen.X.html&HT=iiu1657861852981&DT=Cloud+Native+CNOM+User+Guide)

Maybe one first trial could be to reduce that Retention Time lower than 20 hours and Enable Delete Saved UE Trace Files option to delete the old Trace values.



BRs,  
Christos

Comment by Rajan Rajeshprasad Gupta [ 2025-03-17 ]

Hello Christos Delis (EXT)

I am uncertain about the condition that triggered this behavior.

However, I have observed that Verizon is continuously running UE traces on five different UEs, each operating on distinct devices. These devices include UE1 on Cradlepoint, sending signaling messages.

Vz is running throughput test via Iperf and multiple redundancy test-case which they have in their test list.

I suspect, though I am not completely certain, that continuously running UE traces on five devices may be leading to the accumulation of PCAP files, which in turn is causing

Question1: Did we tested Multiple UE trace running on CNOM during load test ? or Stability testing?

Question2: Do you guys think restarting "eric-data-object-storage-mn-0" by kubectl delete can help? I can request to do it?

Question3: Do you guys think re-deployment of CNOM can help? I can request to handover UCC for 2-4 hours to do re-deployment and feedback?

Comment by Christos Delis (EXT) [ 2025-03-17 ]

Hello Rajan Rajeshprasad Gupta,

No is not a known issue. We have never encountered this issue before.

Could you please share under which condition you observed this situation? is CCD memory full?

BRs,  
Christos

Comment by Zhigang Han [ 2025-03-14 ]

Hi Rajan,

one thing from my side:

Most of the data used by Status Overview is stored in Object Store. eric-data-object-storage-mn-0 is definitely for object store. If the database pod is constantly restarting :

eric-data-object-storage-mn-0

2/2 Running 421 (8m43s ago)

Thanks,

BR/Zhigang

Comment by [Zhigang Han](#) [ 2025-03-14 ]

Hi Rajan,

Here is the information about CNOM:

CNOM PDU provides 3+1 flavors:

1. High Capacity cCNOM --> with cENM's "cCNOM BP License"
2. Default Capacity cCNOM --> similar to old days small ENM's vCNOM size
3. Embedded cCNOM --> to be embedded to each CNF product
4. Low Capacity cCNOM --> removed lots of features, redundancies & others to reduce the size to be small enough in order to collocate with other CNFs on CCD-S (current CNOM without ENM)

our UCC CNOM is the flavor number 4. My concern is the resource limitation which is the root cause of the page information loading very slow, however from the logs attached assigned to UCC design team for the further investigation. Let us wait for the answer from UCC design!

Thanks,

BR/Zhigang

Comment by [Zhigang Han](#) [ 2025-03-14 ]

Hi Rajan,

We checked the attached pod logs however unfortunately there is not much useful information from the logs.

We did see one pod has restarted for more than 400 times, however there is no log for the pod from the attached file.

We also checked CPI troubleshoot document there was one case about CNOM server not responding, however the case is not the same as our case:

For our case, CNOM gui is able to open but inside gui, the information was loaded very slowly

For CPI case, CNOM gui is not able to open or not respond properly.

We have assigned the ticket to our UCC design side for the further support.

Thanks,

BR/Zhigang

[UCC\_PLM-210] [UCC MCN: \[UCC 1.1 LLD\] does not see information for SC license requirement](#) Created: 2025-03-12 Updated: 2025-04-24 Resolved: 2025-04-24

Status:	Done
Project:	<a href="#">UCC_PLM</a>
Component/s:	None
Affects Version/s:	None
Fix Version/s:	None

Type:	Bug	Priority:	Medium
Reporter:	<a href="#">Rajan Rajeshprasad Gupta</a>	Assignee:	<a href="#">Adrian Michel</a>
Resolution:	Closed	Votes:	0
Labels:	None		
Remaining Estimate:	Not Specified		
Time Spent:	Not Specified		
Original Estimate:	Not Specified		

Attachments:	
Team/s:	<a href="#">UCC_XFT2</a>
Found in Build:	UCC Appliance 1.1.0-drop.1
Requirement Status:	UCC Appliance 0.2.1 - UNCOVERED

Description

Hello,

While reviewing the UCC 1.1 LLD in preparation for license ordering, I noticed that the "site data" section lacks information on license requirements.

1. Could you confirm if this is an oversight, or if there are indeed no license requirements for SEPP in the context of 5G SA roaming?

2. Additionally, please correct the minor typo related to "cnom"

A	B	C	D	E	F
0 ENM IP FM	enm_snmpv2_ip	10.237.5.147		IPv4	10.
<b>3. CNF Setting</b>					
Description	Variable_Name	Variable_Value	Validation Check	Variable Type	Ex
licensing parameters					
NELS FQDN	nels_fqdn	nels-cnels2.toolserv.gic.ericsson.se		FQDN	
NELS Host IP	nels_ip	10.87.91.167		IPv4	
NELS Port	nels_port	9095		Number	
customerId from license key file	nels_customerid	946060		Number	946
ECCD swlId from license key file	nels_eccd_swltId	STA-ECCD-13		no validation	
CCDM swlId from license key file	nels_ccdm_swltId	STA-CCDM-38		no validation	
CCSM swlId from license key file	nels_ccsm_swltId	STA-CCSM-39		no validation	
CCRC swlId from license key file	nels_ccrc_swltId	STA-CCRC-31		no validation	
CCPC swlId from license key file	nels_ccpc_swltId	STA-CCPC-22		no validation	
CNOM swlId from license key file	nels_cnom_swltId	DEACUCC_DEV_UCC3		no validation	
UCA swlId from license key file	nels_uca_swltId	STA-UCA-4		no validation	
PCC swlId from license key file	nels_pcc_swltId	STA-PCC-30		no validation	
PCG swlId from license key file	nels_pcg_swltId	STA-PCG-33		no validation	
<b>Home PLMN</b>					
mcc	mcc	244		MCC	
mnc	mnc	099		MNC	
supi start interval	supi_start	2449900000000000		Number	
supi end interval	supi_end	2449999999999999		Number	
gpsi start interval	gpsi_start	8608100000000000		Number	
gpsi end interval	gpsi_end	8608199999999999		Number	
<b>Visited PLMN</b>					
Visited mcc	visited_mcc	243		MCC	
Visited mnc	visited_mnc	098		MNC	
<b>APN parameters</b>					
EMBB IP pool	ccda_internet_pool	10.23.0.0/17		IPv4	10.
EMBB IP pool	ccdb_internet_pool	10.23.128.0/17		IPv4	10.
EMBB IP pool IPv6	ccda_internet_poolv6	2a01:23::/49		IPv6	2a0
EMBB IP pool IPv6	ccdb_internet_poolv6	2a01:23:0:8000::/49		IPv6	2a0
IoT IP pool	ccda_iot_pool	10.24.0.0/17		IPv4	10.
IoT IP pool	ccdb_iot_pool	10.24.128.0/17		IPv4	10.
IoT IP pool IPv6	ccda_iot_poolv6	2a01:24::/49		IPv6	2a0

**Site Data**

Comments

Comment by Åsa Preuss [2025-04-24]

Shouldn't this ticket be labeled with Document?

We need it to make statistics.

BR Åsa

Comment by Andrei Mihalcea [2025-03-13]

Hello,

The attached snip was added in Instruction, it's a good thing but I think also the node should raise an alarm if there will be license problem, but indeed, for checking the inventory this is very good.

Cheers,

Andrei,

Comment by Meryam Nachi [2025-03-12]

Andrei Mihalcea : I guess this is a good comment. We can add that to our Installation instruction guide to verify the licenses.

Comment by Rajan Rajeshprasad Gupta [2025-03-12]

Thank you Adrian Michel

I reviewed the CPI for NELS configuration in SC, which adheres to day-1 configuration similar to PCC-MM. It would be beneficial to include an SC health-check using the following two license CLIs in the installation guide.

This addition will help prevent issues related to the absence of a valid license in NELS and eliminate unproductive troubleshooting during roaming testing.

```
show nlm site  
show nlm license-inventory license-key
```

Comment by [Andrei Mihalcea](#) [ 2025-03-12 ]

Hi guys,

During the parametrization for Application, Gonzalo updated also in day0 the proper variable for sc\_swlt ( nels\_sc\_swlt ). Remains only to be added in LLD as well.

Cheers,

Andrei,

Comment by [Meryam Nachi](#) [ 2025-03-12 ]

Hi Rajan ,

Thank you for your feedback.

There is no need to have any extended license with a specific feature. But we still need to have basic license for SC.

We will add a row in the LLD for SC.

[UCC\_PLM-209] **MANA Vz : Powering off UCC Server A doesn't suspend NFs in NRF** Created: 2025-03-11 Updated: 2025-03-11 Resolved: 2025-03-11

Status:	Rejected
Project:	<a href="#">UCC_PLM</a>
Component/s:	None
Affects Version/s:	<a href="#">UCC Appliance 1.0.1</a>
Fix Version/s:	None

Type:	Bug	Priority:	Low
Reporter:	<a href="#">Rajan Rajeshprasad Gupta</a>	Assignee:	<a href="#">Zhigang Han</a>
Resolution:	Rejected	Votes:	0
Labels:	Verizon		
Remaining Estimate:	Not Specified		
Time Spent:	Not Specified		
Original Estimate:	Not Specified		

Attachments:			
Defect code_qmt:	3- Usability		
Detected in phase:	Production		
Team/s:	UCC_PLM		
Severity_qmt:	4-Low/Cosmetic		
Found in Build:	<a href="#">UCC Appliance 1.0.1</a>		
Requirement Status:	UCC Appliance 0.2.1 - UNCOVERED		

#### Description

Hello,

Vz has NF level redundancy test-cases.

While powering off UCC server A, doesn't suspend NFs in NRF.

We were expecting NRF will suspend NFs of Server A as there are no heart-beat messages received from UCC server A NFs.

Note1: There is no impact on call as UE re-attached to UCC Server-B AMF, AMF will start using locality ccdb to select NFs and call will be handled SMF/AUSF/UDM/PCF of Server-B.

Note2: Same behavior is reproducible 10/10 times.

Question: Is this expected behavior of NRF?

Question: In which case, NRF will suspend NFs if NFs goes to down abruptly without responding to heartbeat message?

#### Comments

Comment by [Rajan Rajeshprasad Gupta](#) [ 2025-03-11 ]

Thank you for confirmation Zhigang.

Will feedback to Vz, we can close ticket,

Comment by [Zhigang Han](#) [ 2025-03-11 ]

Hi Rajan,

Question: Is this expected behavior of NRF?

Answer: It is the expected behavior.

*in Availability-First Mode, if one NRF site (referred as site A) in geo-red sites down forever and the NFs registered to NRF-A did not failover to other NRF for some reason, the nf status of these NFs maybe always "REGISTERED" in other NRFs.*

Question: In which case, NRF will suspend NFs if NFs goes to down abruptly without responding to heartbeat message?

Answer: if NRF CCDA is not coming up to update the status of NFs in CCDA, all NFs from CCDA will stay in registered status all the time.

Thanks,

BR/Zhigang

[UCC\_PLM-208] UCC MCN: [UCC 1.1 LLD] smgeored & cregeored in PCX Created: 2025-03-11 Updated: 2025-04-16 Resolved: 2025-04-16

Status:	Done
Project:	<a href="#">UCC_PLM</a>
Component/s:	None
Affects Version/s:	None
Fix Version/s:	None

Type:	Bug	Priority:	Low
Reporter:	<a href="#">Rajan Rajeshprasad Gupta</a>	Assignee:	<a href="#">Meryam Nachi</a>
Resolution:	Closed	Votes:	0
Labels:	None		
Remaining Estimate:	Not Specified		
Time Spent:	Not Specified		
Original Estimate:	Not Specified		

Attachments:	
Team/s:	<a href="#">UCC_XFT2</a>
Found in Build:	UCC Appliance 1.1.0-drop.1
Requirement Status:	UCC Appliance 0.2.1 - UNCOVERED

#### Description

Hello,

Refer to the 1.1 drop2 LLD to begin preparations for MCN installation.

We see smgeored & cregeored in PCX are new VIPs introduced in LLD.

It is not clear what is use for VIPs.

sig_data	172.16.3.97/32	smgeored
	172.16.3.98/32	cregeored
	172.16.3.99/32	ccpc_intersite
	172.16.3.100/32	ccdm_intersite

Please clarify use of this VIPs in LLD as PCC-SM used in 1.0 was ACTIVE-ACTIVE and There is no information if there is change in behavior from 1.1.

#### Comments

Comment by Meryam Nachi [ 2025-04-16 ]

Hi Rajan,

We will take that into consideration for the next release. We are planning to do more cleanups in UCC 1.2.

Comment by Rajan Rajeshprasad Gupta [ 2025-03-11 ]

Thank you, Adrian and Meryam.

Upon rechecking the 1.0 LLD, I found that both parameters are indeed present. They are dummy parameters without any current impact.

Question: Should we remove these dummy parameters in the next LLD release?

Comment by Meryam Nachi [ 2025-03-11 ]

those parameters already exist in 1.0 LLD. They are not newly added.

Screenshot from UCC 1.0 CP1 LLD:

#NAME#	ccg_ingress	#NAME#	#NAME#
172.16.2.97/32	smgeored	172.16.2.97	OK
172.16.2.98/32	cregeored	172.16.2.98	OK
172.16.2.99/32	ccpc_intersite	172.16.2.99	OK
172.16.2.100/32	ccdm_intersite	172.16.2.100	OK

Comment by Adrian-Bogdan Iliescu [ 2025-03-11 ]

There is no change, SMFs are still in active-active mode , there is no SMF geo-red implemented

[UCC\_PLM-207] UCC MCN: [UCC 1.1 LLD] Wrong SWGW ticket for SC Created: 2025-03-10 Updated: 2025-04-24 Resolved: 2025-04-24

Status:	Done
Project:	UCC_PLM
Component/s:	None
Affects Version/s:	UCC Appliance 1.1.0
Fix Version/s:	None

Type:	Bug	Priority:	Low
Reporter:	Houssem Marzouga	Assignee:	Unassigned
Resolution:	Closed	Votes:	0
Labels:	None		
Remaining Estimate:	Not Specified		
Time Spent:	Not Specified		
Original Estimate:	Not Specified		

Attachments:	
Sprint:	UCC XFT2 Sprint 7, UCC XFT2 Sprint 8, UCC XFT2 Sprint 9
Team/s:	UCC_XFT2
Found in Build:	UCC Appliance 1.1.0-drop.1
Requirement Status:	UCC Appliance 0.2.1 - UNCOVERED

#### Description

Hello,

In the UCC1.1 LLD, the SWGW ticket related to SC is T-160854, which references **eric-sc-ucc-values-1.16.0+97**. However, it does not include a reference to the CSAR file.

	UCA (EDA)		1.2 EP1	<a href="#">T-162997</a>	CXP 904 4024	R6B	
	CNOM		2.2	<a href="#">T-</a>	CXF 101 0173/2	R1B	
	CCDM	5GC	1.13	<a href="#">T-161571</a>	CXS 101 1093	1.13.43	
	CCSM	5GC	1.14 EP1	<a href="#">T-161472</a>	CXS 101 844	1.37.9	
Ericsson	CCRC (NRF Only)	5GC	1.17 EP1	<a href="#">T-161598</a>	CXS 101 7716	1.17.6+1	
	SC	5GC	1.16	<a href="#">T-160854</a>	CXP 904 4197	1.16.0	
	PCC	5GC	1.34 CP5	<a href="#">T-161336</a>	CXP 904 1577/1	R64J	
	PCG	5GC	1.26 EP1	<a href="#">T-160884</a>	CXP 904 1656/1	R62C	
	CCPC	5GC	1.16 EP1	<a href="#">T-160434</a>	CXS 101 960	1.16.6	
	PCx (EP5G)	5GC	1.16 EP1	<a href="#">T-159965</a>	CXD 101 086/2	R7B	
					CXP 904 3166/2	R7B	
					CXP 904 3220/2	R7B	

The LLD should be updated to include a reference to the CSAR file, as specified in the MoP, with SWGW ticket [T-160852](#).

Thanks.

Br,

Houssem.

#### Comments

Comment by [Meryam Nachi](#) [ 2025-03-13 ]

Hi Rajan, we have fixed this and will be part of the next Delivery.

#### [UCC\_PLM-206] UCC MCN: [UCC 1.1 II] Does not contains SC Integration in CNOM

Created: 2025-03-07 Updated: 2025-04-24 Resolved: 2025-04-24

Status:	Done
Project:	<a href="#">UCC_PLM</a>
Component/s:	None
Affects Version/s:	None
Fix Version/s:	None

Type:	Bug	Priority:	Medium
Reporter:	<a href="#">Rajan Rajeshprasad Gupta</a>	Assignee:	Unassigned
Resolution:	Closed	Votes:	0
Labels:	None		
Remaining Estimate:	Not Specified		
Time Spent:	Not Specified		
Original Estimate:	Not Specified		

Team/s:	UCC_XFT2
Found in Build:	UCC Appliance 1.1.0-drop.1
Requirement Status:	UCC Appliance 0.2.1 - UNCOVERED

#### Description

Hello,

Refer to the 1.1 drop2 installation guide to begin preparations for 5G SA roaming

We don't see the CNOM steps required to integrate the SC, nor do we see the SC KPIs in CNOM.

Question1: Should SC be excluded from CNOM, or should it be added?

Question2: If SC becomes part of CNOM, do we have KPIs established for it?

#### Comments

Comment by [Rajan Rajeshprasad Gupta](#) [ 2025-03-12 ]

Thank you Andrei Mihalcea

Comment by [Andrei Mihalcea](#) [ 2025-03-12 ]

Hi guys,

CNOM was not done for this drop. Indeed the Embedded CNOM will be used for SC. Our colleague Gonzalo is working on it and will push the needed changes to GIT as soon as are ready.

Thank you,

Andrei,

Comment by [Christos Delis \(EXT\)](#) [ 2025-03-12 ]

[Rajan Rajeshprasad Gupta](#), as far as i know this process is under development.

At the end, FQDN for SC will also be available to connect to embedded CNOM.

Maybe [Meryam Nachi](#) could comment better on that.

Thank you in advance.

Comment by [Rajan Rajeshprasad Gupta](#) [ 2025-03-12 ]

Thank you [Christos Delis \(EXT\)](#)

Follow-up question for embedded CNOM on SC.

1. Similar to how the embedded CNOM on CCRC has an FQDN for login, we have an FQDN for CNOM access. However, I don't see a corresponding FQDN for SC. Is this an omission in the LLD?

eg.

cnom-ccrc-ucc1a.deac.ericsson.se | 10.92.239.70

2. Similar to the embedded CNOM on CCRC, should we include one-page user-guide information in the installation guide to assist with navigating to SC CNOM?

Comment by [Christos Delis \(EXT\)](#) [ 2025-03-12 ]

Good morning [Rajan Rajeshprasad Gupta](#),

According to the feedback that i received from Eric, SC will not be part of CNOM on UCC 1.1.

In this case embedded CNOM on SC will be used.

BRs,

Christos

Comment by [Rajan Rajeshprasad Gupta](#) [ 2025-03-11 ]

Assigned to [Meryam Nachi](#)

She will route to DEV team-member who will look into ticket for 5G SA roaming as part of MCN verification.

Comment by [Adrian Michel](#) [ 2025-03-11 ]

Wrong Adrian, I guess you mean Adrian-Bogdan?!

## [UCC\_PLM-205] UCC MCN: [UCC 1.1 Artefacts] Does not contains folder for SC

Created: 2025-03-07 Updated: 2025-04-16 Resolved: 2025-04-16

Status:	Done
Project:	<a href="#">UCC_PLM</a>
Component/s:	None
Affects Version/s:	None
Fix Version/s:	None

Type:	Bug	Priority:	Medium
Reporter:	<a href="#">Rajan Rajeshprasad Gupta</a>	Assignee:	Unassigned
Resolution:	Closed	Votes:	0
Labels:	None		
Remaining Estimate:	Not Specified		
Time Spent:	Not Specified		
Original Estimate:	Not Specified		

<b>Team/s:</b>	UCC_XFT2
<b>Found in Build:</b>	UCC Appliance 1.1.0-drop.1
<b>Requirement Status:</b>	UCC Appliance 0.2.1 - UNCOVERED

#### Description

Hello,

Refer to the 1.1 drop2 installation guide to begin preparations for 5G SA roaming

Product Name	Version	SWGW ticket	Content
UCC Artefacts	1.1 drop 2	<a href="#">Artifactory link</a>	UCC_Artefacts_-_Configuration_Files.gz

The artifact link for the configuration file is missing the SC configuration in CCDB. Please update the Artifactory link in the II and share the correct link.

#### Comments

Comment by [Rajan Rajeshprasad Gupta](#) [ 2025-03-13 ]

Thank you Meryam Nachi .

Re-tested with the new build, ucc-config-1.1.0-build-33, which now includes the 'sc' folder

Product Name	Version	SWGW ticket	Content
UCC Artefacts	1.1 LFD1	<a href="#">Artifactory link</a>	UCC_Artefacts_-_Configuration_Files.gz

Comment by [Meryam Nachi](#) [ 2025-03-13 ]

Hi Rajan, this is already updated in the II and the delivery page as well.

#### [UCC\_PLM-204] UCC MCN: [UCC 1.1 LLD] roaming PLMN certificate

Created: 2025-03-06 Updated: 2025-04-24 Resolved: 2025-04-24

<b>Status:</b>	Done
<b>Project:</b>	<a href="#">UCC_PLM</a>
<b>Component/s:</b>	None
<b>Affects Version/s:</b>	None
<b>Fix Version/s:</b>	None

<b>Type:</b>	Bug	<b>Priority:</b>	Medium
<b>Reporter:</b>	<a href="#">Rajan Rajeshprasad Gupta</a>	<b>Assignee:</b>	<a href="#">Adrian Michel</a>
<b>Resolution:</b>	Closed	<b>Votes:</b>	0
<b>Labels:</b>	None		
<b>Remaining Estimate:</b>	Not Specified		
<b>Time Spent:</b>	Not Specified		
<b>Original Estimate:</b>	Not Specified		

<b>Attachments:</b>	
<b>Team/s:</b>	UCC_XFT2
<b>Found in Build:</b>	UCC Appliance 1.1.0-drop.1
<b>Requirement Status:</b>	UCC Appliance 0.2.1 - UNCOVERED

#### Description

Hello,

As we implement 5G SA roaming in version 1.1, we've noticed that 'visited\_mcc' and 'visited\_mnc' have been added to the 'Site Data.' However, we don't see any entries for Certificates' section.

AutoSave Off Ericsson Ultra Compact Core - Low Level Design-1.1-Updated-N9(Updated by Adria..

File Home Templafy Insert Page Layout Formulas Data Review View Automate Add-ins Help

Templafy

Paste Clipboard Font Alignment Number Styles

H111

	A	B	C	D	E
98		ccdm	eric-ccdm-4gnotif-client	prov4g	prov4g-ccdm-ucc1b.deac.ericsson.se
99		ccdm	eric-ccdm-4gprovisioning-client	prov4g	prov4g-ccdm-ucc1b.deac.ericsson.se
100		ccdm	eric-ccdm-4gprovisioning-server	prov4g	prov4g-ccdm-ucc1b.deac.ericsson.se
101		ccdm	eric-ccdm-4gnotif-server	prov4g	prov4g-ccdm-ucc1b.deac.ericsson.se
102		ccdm	eric-ccdm-4gtraffic-client	udr4g	udr4g-ccdm-ucc1b.5gc.mnc099.mcc24
103		ccdm	eric-ccdm-4gtraffic-server	udr4g	udr4g-ccdm-ucc1b.5gc.mnc099.mcc24
104		ccdm	eric-ccdm-prov-server	prov5g	prov5g-ccdm-ucc1b.deac.ericsson.se
105		ccdm	eric-ccdm-sbi-client	udr	udr-ccdm-ucc1b.5gc.mnc099.mcc244.3
106		ccdm	eric-ccdm-sbi-server	udr	udr-ccdm-ucc1b.5gc.mnc099.mcc244.3
107		ccdm	eric-ccdm-intersite-client	intersite	intersite-ccdm-ucc1b.5gc.mnc099.mcc
108		ccdm	eric-ccdm-intersite-server	intersite	intersite-ccdm-ucc1b.5gc.mnc099.mcc
109		sc	eric-sc-sepp-sbi-client-external	seppext	seppext-sc-ucc1b.5gc.mnc099.mcc244
110		sc	eric-sc-sepp-sbi-server-external	seppext	seppext-sc-ucc1b.5gc.mnc099.mcc244
111		sc	eric-sc-sepp-sbi-client-internal	seppint	seppint-sc-ucc1b.5gc.mnc099.mcc244.
112		sc	eric-sc-sepp-sbi-server-internal	seppint	seppint-sc-ucc1b.5gc.mnc099.mcc244.
113		sc	log-syslog-client	syslog	syslog-sc-ucc1b.deac.ericsson.se
114		cnom	gui-cnom-http-server	oam	oam-cnom-ucc1b.deac.ericsson.se
115		cnom	eric-log-transformer-client	syslog	syslog-cnom-ucc1b.deac.ericsson.se
116					
117					
118					
119					
120					
121					

Site Data UCC EXTERNAL IP Plan UCC IP Plan UCC cabling hostnames **TLS certificates** +

Ready Accessibility: Investigate

#### Question:

For setting up secure communication over the N32 interface between partner PLMNs, do we need the following? This is first step to start integration work;

1. **Partner PLMN FQDN and Certificate:** Is it necessary to have the FQDN and a certificate from the partner PLMN?
1. **Certificate Signing:** Who is responsible for signing the partner's certificate, and how is it loaded into the system?
1. **CA Field in Site Data:** Is there a need for an additional CA field specifically for the partner in the Site Data configuration?

Currently, the information regarding partner FQDN and certificate requirements is not clearly outlined in the CIQ. Could you provide more clarity on these aspects?

## Comments

Comment by Andrei Mihalcea [ 2025-03-26 ]

Hi Rajan,

I think you have older versions of LLD and II, these things are latest things that we are working on it. The new II and LLD will be provided Friday as part of the LFD2.

Regarding the second question, basically you need to generate the new site global based on the latest LLD and then to install the SC.

Cheers,

Andrei,

Comment by Rajan Rajeshprasad Gupta [ 2025-03-26 ]

Hello Andrei,

Thank you for feedback.

I was unable to locate 'point 6' under Chapter 9 in Section II of version PJ9. Have we released a new version of the II and LLD documents?

Another question, In order to access the latest information from the new LLD, should we perform a re-installation from the CCD, or is it sufficient to just re-install the SC?

Comment by Andrei Mihalcea [ 2025-03-26 ]

Hi Rajan,

For the Roaming Partners we are not creating and signing certificates. Certificates are created and signed by the Roaming Partners because they are their certificates. We only need the CA (or signing certificate) to be loaded in our SEPP and this thing is mentioned in II in Chapter 9 point 6.

The FQDNs and other details that are needed to be configured in our SEPP side are mentioned in Site Data tab in LLD.

How the information are requested and received from the Roaming Partner this should be an already established flow (like for all the other Roaming Partner opening) and this is not part of the UCC deployment.

Cheers,

Andrei,

[UCC\_PLM-203] UCC MCN: [UCC 1.1 LLD] N9 IP address Created: 2025-03-04 Updated: 2025-04-24 Resolved: 2025-04-24

Status:	Done
Project:	UCC_PLM
Component/s:	None
Affects Version/s:	None
Fix Version/s:	None

Type:	Bug	Priority:	Medium
Reporter:	Rajan Rajeshprasad Gupta	Assignee:	Unassigned
Resolution:	Closed	Votes:	0
Labels:	None		
Remaining Estimate:	Not Specified		
Time Spent:	Not Specified		
Original Estimate:	Not Specified		

Attachments:	Ericsson Ultra Compact Core - Low Level Design-1.1-Updated-N9.xlsx  Ericsson Ultra Compact Core - Low Level Design.xlsx image-2025-03-05-00-13-00-949.png  image-2025-03-05-00-16-55-564.png  image-2025-03-05-10-28-35-038.png  image-2025-03-12-02-00-40-807.png  image-2025-03-12-01-37-403.png
Other Assignees:	Adrian-Bogdan Iliescu
Sprint:	UCC XFT2 Sprint 6, UCC XFT2 Sprint 7, UCC XFT2 Sprint 8, UCC XFT2 Sprint 9
Team/s:	UCC_XFT2
Found in Build:	UCC Appliance 1.1.0-drop.1
Requirement Status:	UCC Appliance 0.2.1 - UNCOVERED

## Description

Hello,

N9 which is expected to go via media VRF. It should be external routable IP or public IP. However, it looks like we added in LLD private IP.

This will make routing not possible and roaming test at risk.

See in picture1.

ccda	pcx	pcx_media_vips	vip	media	172.16.2.7/32 172.16.2.8/32 172.16.2.9/32 172.16.2.10/32 172.16.2.11/32 172.16.2.12/32 172.16.2.13/32
ccdb	pcx	pcx_ran_vips	vip	ran	214.13.224.165/32 214.13.224.166/32 214.13.224.167/32 214.13.224.168/32 214.13.224.169/32
ccdb	pcx	pcx_sig_vips	vip	sig	172.16.3.1/32 172.16.3.2/32 172.16.3.3/32 172.16.3.4/32 172.16.3.5/32 172.16.3.6/32 172.16.3.14/32 172.16.3.15/32
ccdb	pcx	pcx_media_vips	vip	media	172.16.3.7/32 172.16.3.8/32 172.16.3.9/32 172.16.3.10/32 172.16.3.11/32 172.16.3.12/32 172.16.3.13/32

#### Comments

Comment by [Adrian-Bogdan Iliescu](#) [ 2025-03-14 ]

Hi,

Jinja2 templates for pcx have been updated to use correct n9 ( external routable address ) and push to git.

Thank you

Comment by [Adrian Michel](#) [ 2025-03-12 ]

Hello again [Rajan Rajeshprasad Gupta](#),

here the missing answers:

We are targeting on 5G SA roaming only. We don't consider any case for inter-system intra-PLMN mobility, including handover, in the visited network.

Comment by [Rajan Rajeshprasad Gupta](#) [ 2025-03-12 ]

Thank you [Adrian Michel](#)

Please provide feedback on the intra-PLMN handover between EPS and 5GS so we can close the ticket.

both, non-impacting typographical changes in the LLD will be addressed in the next release.

Comment by [Adrian Michel](#) [ 2025-03-11 ]

Hello [Rajan Rajeshprasad Gupta](#), you are right, missed to change it on the "UCC IP Plan" tab. However this is only cosmetic, as the IPs are taken from the "UCC EXTERNAL IP

Changed it now for next delivery.

Comment by [Rajan Rajeshprasad Gupta](#) [ 2025-03-11 ]

Hello [Adrian Michel](#)

Along with previous question.

In the process of establishing N32 communication between vSEPP and hSEPP, the communication will occur through the primary network using the VRF named `ecfe_sig_ext`.

Good that, we've ensured that the worker IPs are routable to facilitate this communication.

However, there's a challenge: the subnet assigned to `ecfe_sig_ext` overlaps with the `ccd_oam` subnet. PFA attachment.

Could you check and add into correction of LLD?

Network	Type	VLAN ID	TAGGED	Network Instance	ASN	SUBNET	
ccd_oam	ovs	1100	tagged	oam	ucc : 4251110001 router : 4251100001	10.92.239.0/28	gateway bmc_ip ccd_cc
ecfe_oam	ovs	1101	tagged			10.92.239.16/29	gateway ecfe_c
ccd_int	ovs	1102	tagged			172.16.0.16/28	gateway ccd_in ccd_in ccd_cc
ecfe_sig	ovs	1104	tagged			172.16.0.0/29	gateway ecfe_s
ecfe_sig_data	ovs	1105	tagged			172.16.0.8/29	gateway ecfe_s
ecfe_sig_ext	ovs	1103	tagged			10.92.239.8/29	gateway ecfe_s
ccd_oam	ovs	1100	tagged	oam	ucc : 4251110001 router : 4251100001	10.92.239.0/28	gateway bmc_ip ccd_cc
ecfe_oam	ovs	1101	tagged			10.92.239.16/29	gateway ecfe_c
							gateway ccd_in

IP Address:	10.92.239.0
Network Address:	10.92.239.0
Usable Host IP Range:	10.92.239.1 - 10.92.239.14
Broadcast Address:	10.92.239.15
Total Number of Hosts:	16
Number of Usable Hosts:	14
Subnet Mask:	255.255.255.240
Wildcard Mask:	0.0.0.15
Binary Subnet Mask:	11111111.11111111.11111111.11110000
IP Class:	C
CIDR Notation:	/28
IP Type:	Private
Short:	10.92.239.0 /28

Comment by Rajan Rajeshprasad Gupta [ 2025-03-05 ]

Hello Adrian Michel

Thank you. There is a typo in the 'IP Assignment' field. The service name should be 'upf\_n9' instead of 'mme\_s1\_mme\_2'.

Allow me to ask one more questions :

1. Are we targeting on 5G SA roaming only in 1.1?
2. Since the UCC appliance will support both 4G and 5G, do we need EPC roaming for intra-PLMN handover in the visited network between EPS and 5GS?

If yes, then we need to have routable /public IP for s6a+s5s8,

If no, then what should the behavior be for intra-PLMN handover in the visited network between EPS and 5GS?

Comment by [Adrian Michel](#) [ 2025-03-05 ]

[Rajan Rajeshprasad Gupta](#), please check the attached LLD, and let me know if it's looks good to you.

Comment by [Jim Dumont](#) [ 2025-03-05 ]

In progress

Comment by [Rajan Rajeshprasad Gupta](#) [ 2025-03-05 ]

Hello [Adrian Michel](#)

Thank you for highlighting. I suggest we use 'NA' (Not Applicable) for the next-hop.

Since two recursive routes are needed for N9, specifying only one IP as the next hop would make the LLD appear incorrect.

Comment by [Adrian Michel](#) [ 2025-03-05 ]

Thanks that explanation, [Rajan Rajeshprasad Gupta](#). But to shorten the discussion with further queries from me, could you just tell me which IP would you like to see here:

<b>vip_pool_sig_ext</b>	<b>sig_ext</b>	<b>214.13.226.28/30</b>
<b>ccpc_rx</b>	<b>sig_ext</b>	<b>214.13.226.28/32</b>
<b>sepp_sig_ext</b>	<b>sig_ext</b>	<b>214.13.226.29/32</b>

DN	VIP	NEXTHOP	NETWORKINSTANCE	SUBNET	
	pcx_ran_vips	172.16.0.77	ran	214.13.226.0/32	upf_n3
	pcx_media_vips	172.16.0.86		214.13.226.1/32	amf_n
	pcx_ran_vips	172.16.1.77	ran	214.13.226.2/32	amf_n
	pcx_media_vips	172.16.1.86		214.13.226.3/32	mme_n
	pcx_ran_vips	172.16.1.77	ran	214.13.226.4/32	mme_n
	pcx_media_vips	172.16.1.86		214.13.226.10/32	mme_n
	pcx_ran_vips	172.16.1.77	ran	214.13.226.5/32	upf_n3
	pcx_media_vips	172.16.1.86		214.13.226.6/32	amf_n
	pcx_ran_vips	172.16.1.77	ran	214.13.226.7/32	amf_n
	pcx_media_vips	172.16.1.86		214.13.226.8/32	mme_n
	pcx_ran_vips	172.16.1.77	ran	214.13.226.9/32	mme_n
	pcx_media_vips	172.16.1.86		214.13.226.11/32	mme_n

DN	VIP	TYPE	NETWORKINSTANCE	SUBNET	
				214.13.227.192/32	pcx_out

Comment by [Rajan Rajeshprasad Gupta](#) [ 2025-03-05 ]

Hello [Adrian Michel](#)

N9 belongs to UPF.

The UPF will advertise the N9 interface with the next hop set to up:media\_dp\_loopback. We will then need to configure a static route in the R6K, directing the up:media\_dp\_

Comment by [Adrian Michel](#) [ 2025-03-05 ]

What's the nexthop for your n9? Is it mm-forwarder, or vpngw? Something else?

gateway_ip	172.16.1.81
cre:ipfw_media	172.16.1.82
up:ipfw_media	172.16.1.83
up:ipfw_media	172.16.1.84
mm-forwarder	172.16.1.85
vpngw:ipfw_media	172.16.1.86

Comment by [Rajan Rajeshprasad Gupta](#) [ 2025-03-04 ]

Update:

Thanks for Chandra for fixing point1.

1. "UCC IP Plan" – Ok

2. "UCC EXTERNAL IP Plan" –**NOK**, We still need to update the sheet to reflect that N9 is used for external connections under the media VRF . Picture 2.

	ccd	ccpc_rx		sig_ext	10.92.239.220/32		
	ccd	sepp_sig_ext		sig_ext	10.92.239.221/32		
<b>3. SERVICE VIPS</b>							
CLUSTER	FUNCTION	VIP	NEXTHOP	NetworkInstance	SUBNET	IP Assignment	
ccda	pcx	pcx_ran_vips	172.16.0.77	ran	10.92.239.192/32	upf_n3	10.92.239.19
					10.92.239.193/32	amf_n2_1	10.92.239.19
					10.92.239.194/32	amf_n2_2	10.92.239.19
					10.92.239.195/32	mme_s1_mme_1	10.92.239.19
					10.92.239.196/32	mme_s1_mme_2	10.92.239.19
					10.92.239.197/32	upf_n3	10.92.239.19
ccdb	pcx	pcx_ran_vips	172.16.1.77	ran	10.92.239.198/32	amf_n2_1	10.92.239.19
					10.92.239.199/32	amf_n2_2	10.92.239.19
					10.92.239.200/32	mme_s1_mme_1	10.92.239.20
					10.92.239.201/32	mme_s1_mme_2	10.92.239.20
<b>4. ECFE VIPS</b>							
CLUSTER	FUNCTION	VIP	TYPE	NetworkInstance	SUBNET	IP Assignment	
	pcx				10.92.239.64/32	pcx_oam	10.92.239.64
					10.92.239.65/32	pcx_prov	10.92.239.65

#### [UCC\_PLM-202] MANA Vz : Different behavior of AMF and SMF cache service Created: 2025-03-04 Updated: 2025-04-24 Resolved: 2025-04-24

Status:	Done
Project:	UCC_PLM
Component/s:	None
Affects Version/s:	UCC Appliance 1.0.1
Fix Version/s:	None

Type:	Bug	Priority:	Medium
Reporter:	Rajan Rajeshprasad Gupta	Assignee:	Adrian-Bogdan Iliescu
Resolution:	Closed	Votes:	0
Labels:	UCC_Appliance_1.1.0, Verizon		
Remaining Estimate:	Not Specified		
Time Spent:	Not Specified		
Original Estimate:	Not Specified		

Sprint:	UCC XFT2 Sprint 8, UCC XFT2 Sprint 9
Team/s:	UCC_XFT2
Found in Build:	UCC Appliance 1.0.1
Requirement Status:	UCC Appliance 0.2.1 - UNCOVERED

#### Description

Hello,

During the execution of NF redundancy test cases by Verizon for each NF of the UCC, the following issues were reported:

AMF correctly selects AUSF, UDM, and SMF when peer NFs are unavailable.

However, SMF does not correctly select UDM and PCF when peer NFs are unavailable.

Following an initial analysis:

AMF: NRF cache is kept as OFF.

```
verizon@pcx-ccda#show running-config mm nrf-option cache
mm nrf-option cache off
```

SMF : NRF cache is kept as ON.

```
verizon@pcx-ccda#show running-config epg pgw sbi nrf no-cache
% No entries found.
```

as a result, SMF always use cache for selecting peer NF even if peer NF is suspended or de-registered state in NRF.

Test-case is passed by doing manual nrf-cache cleaning on SMF.

Question:

Why there is different behavior across AMF and SMF?

Does need to clear NRF cache on SMF?

#### Comments

Comment by [Adrian-Bogdan Iliescu](#) [ 2025-04-02 ]

hi,

Cache has been disabled also in SMF and config pushed in Git.

Comment by [Reema Sidhwani](#) [ 2025-03-25 ]

Hi Alexander, after some discussion in the TR board, the case mentioned in this TR is agreed to be tested as part of NF redundancy tests. Since you are driving those tests, I am assigning this TR to you.

Thanks!

#### [UCC\_PLM-201] MELA-Telefonica Issue in Patching SSH Key in Authorized Keys File of CCD

Created: 2025-02-28 Updated: 2025-06-04 Resolved: 2025-06-04

Status:	Rejected
Project:	<a href="#">UCC_PLM</a>
Component/s:	None
Affects Version/s:	<a href="#">UCC Appliance 1.0.1</a>
Fix Version/s:	None

Type:	Bug	Priority:	Medium
Reporter:	<a href="#">Akshaya Avin Shetty</a>	Assignee:	<a href="#">Alexander Malikov</a>
Resolution:	Rejected	Votes:	0
Labels:	Telefonica, UCC1.0, UCC_Appliance_1.1.0		
Remaining Estimate:	Not Specified		
Time Spent:	Not Specified		
Original Estimate:	Not Specified		

Attachments:	<a href="#">ccdadm-ccda-config.yaml</a>	<a href="#">image-2025-02-28-21-38-14-345.png</a>	<a href="#">Upgrade_logs.txt</a>
Team/s:	UCC_XFT2		
Found in Build:	UCC Appliance 1.0.1		
Requirement Status:	UCC Appliance 0.2.1 - UNCOVERED		

#### Description

Dear PLM Team,

We are following Section 11.4 Patching Local O&M and Central Management of the Software Guide for UCC1.0\_CP1 where we are patching a public SSH keys into the Authc

We initiated the upgrade, and it has been running for the past four hours without any errors. As per the guide, the steps for upgrade planning and validation were successfu

Below is the public key which we need to add:

- ssh-rsa  
AAAAAB3NzaC1yc2EAAAQABAAQACQDJwaaZ+D2IMgTS+mU/9LlrRGHTe80p6ZbhmcxOB8dQa+A2lg7v9db7/KEvZ90xo7L5FoDdpmWfpswusNZb6jIYQwFK2TKAY/lKpeV  
cdap5gb\5g01@15-5g01

Below are the 3 steps followed during upgrade procedure mentioned in the guide:

ccdadm cluster upgrade plan : Successfully executed

ccdadm cluster config validate-upgrade : Successfully executed

ccdadm cluster upgrade all: it didn't execute successfully it going on with no error

Logs attached for reference: [Upgrade\\_logs.txt](#) [ccdadm-ccda-config.yaml](#)

We are observing below alarm in ECCD:

The terminal window shows several commands being run:

```
eccd@ucc-ccda:~$ kubectl get pods -A | grep -v -E "([0-9]+)\.\|1" | grep -v -E Completed
NAMESPACE     NAME                           READY   STATUS    RESTARTS   AGE
eccd@ucc-ccda:~$ kubectl get pod -A | grep -v "1/1\|2/2\|3/3\|4/4\|5/5\|6/6\|7/7\|8/8\|9/9\|10/10\|Completed"
NAMESPACE     NAME                           READY   STATUS    RESTARTS   AGE
eccd@ucc-ccda:~$ kubectl get svc/eric-pm-alertmanager -n monitoring -o jsonpath='{.spec.clusterIP}'
eccd@ucc-ccda:~$ curl -s http://192.168.0.238:8080/v1/alerts | jq .
{
  "status": "success",
  "data": [
    {
      "labels": {
        "alertgroup": "Cluster",
        "alarmname": "Cluster Upgrade Ongoing",
        "cluster": "ucc",
        "component": "controlplane",
        "criticismActiveEventType": "1",
        "criticismActiveMajorType": "193",
        "criticismActiveMinorType": "08895969",
        "criticismActiveProbableCause": "1",
        "instance": "192.168.0.238:8080",
        "job": "node-metrics-pods",
        "severity": "Warning",
        "type": "Cluster"
      },
      "annotations": {
        "description": "Cluster Upgrade Ongoing. Currently \"controlplane\" operation is ongoing",
        "summary": "Cluster Upgrade Ongoing. Currently \"controlplane\" operation is ongoing"
      },
      "startAt": "2025-02-28T11:31:46.852866204Z",
      "endAt": "2025-02-28T11:41:46.852866204Z",
      "generatorURL": "http://eric-victoria-metrics-alert-server-5c6b876496-sxhx4:8080/vmalert/alert?group_id=14404546371269367105&alert_id=85231003408667776871",
      "scans": [
        {
          "status": "Success",
          "stateReady": null,
          "stateNotReady": null
        }
      ],
      "receivers": [
        "praveenreddy-sreedhar"
      ]
    }
  ]
}
```

The browser window shows a Prometheus alert with the following details:

- Description:** Cluster Upgrade Ongoing. Currently "controlplane" operation is ongoing
- Summary:** Cluster Upgrade Ongoing. Currently "controlplane" operation is ongoing
- Start At:** 2025-02-28T11:31:46.852866204Z
- End At:** 2025-02-28T11:41:46.852866204Z
- Generator URL:** http://eric-victoria-metrics-alert-server-5c6b876496-sxhx4:8080/vmalert/alert?group\_id=14404546371269367105&alert\_id=85231003408667776871

Please help us to confirm if there is any issue in our files or why cluster upgrade is not completing?

For the WA i have manually added the keys in the authorised\_keys files of ECCD. So that customer can access ECCD without jumphost. But we need to confirm about this pr  
Regards,

Akshaya Shetty

## Comments

Comment by Alexander Malikov [2025-06-04]

Hello Akshaya and Reema,

Reema Sidhwani, could you please help Akshaya to raise requirement for this functionality?

Best regards,  
Alex

Comment by Akshaya Avin Shetty [2025-06-04]

Hello Alexander,

Thanks for your response.

I understand that the current functionality does not support adding new SSH keys post-installation. Could you please let me know if there are any plans to include this feature in an upcoming release?

This capability is essential for our customers. For instance, a customer might set up a few SSH keys during the initial installation. However, after six months, they may need to add additional SSH keys, perhaps due to acquiring new laptops or onboarding new team members. In such scenarios, the ability to add SSH keys without a complete reinstallation would be highly beneficial.

Regards,

Akshaya Shetty

Comment by Zhigang Han [2025-06-03]

Hi Akshaya,

The only way to close the ticket is to reject the ticket. If you agree, I will reject the ticket from my side.

Thanks,

BR/Zhigang

Comment by [Alexander Malikov](#) [ 2025-06-03 ]

Hello,

This functionality is not supported. We can add ssh\_key only during CCD installation process. Please close it.

Best regards,

Alex

Comment by [Akshaya Avin Shetty](#) [ 2025-06-02 ]

Hello,

UCC is in the Army location and jumphost is not shipped to Army location. They wanted to connect UCC through laptop's for which keys were not added. Customer have not shared the ssh key with us so in LLD SSH key was not added. So we required to patch the SSH key.

We require to validate the Section 11.4 Patching Local O&M and Central Management of the Software Guide for UCC1.0\_CP1 if it works

Comment by [Fredrik Gustavsson](#) [ 2025-03-05 ]

To summarize, and if I understand correctly, the background is that in a running system with already configured and available ssh keys, the need is to insert one, or more, additional keys.

The closest description for this, in the documentation, is chapter 11.4, but this chapter is meant as a break-the-glass description on how to re-establish the possibility for a remote connection after the last ssh key has been lost.

In the situation that lead to this, since remote connectivity is present, connecting and adding additional ssh public keys in /home/eccd/.ssh/authorized\_keys should be the way forward.

The actions, that I see as a result for this are:

1. Clearly describe the purpose of chapter 11.4, including when and when not to apply those steps
2. Include an instruction on how to insert an additional ssh key, when we have cluster node connectivity
3. Test the procedure in 11.4 (this was not in scope for 1.0.0 or 1.0.1, but is planned for 1.1.0)

Comment by [Zhigang Han](#) [ 2025-03-03 ]

Hi Akshaya,

From the log you attached, we could see the error messages repeated in the log:

```
2025/02/28 09:37:47 INFO: [pkg/controller/capi/upgrade/controlplane.go:640] Checking Addons Status of: [cert-manager kyverno mgmt-cpu-override siptls coredns external-snapshotter ingress calico ccd-task-exec-fw ecfe multus local-storage-provisioner pm metrics-server pm_webhook_snmp sriov-network-device-plugin ovs-cni ccd-licensing cr-registry]
2025/02/28 09:42:47 INFO: [pkg/addons/manager.go:802] Addon "external-snapshotter" is not ready yet... Current pod counts (desired/updated/ready): 0/0/0
2025/02/28 09:42:47 INFO: [pkg/controller/capi/upgrade/controlplane.go:645] WARNING! Addon "external-snapshotter" is not ready. Reason: timed out while waiting for addon "external-snapshotter" to get ready. Reason: All attempts fail:#1: deployments.apps "snapshot-controller" not found#2: deployments.apps "snapshot-controller" not found#3: deployments.apps "snapshot-controller" not found#4: deployments.apps "snapshot-controller" not found#5: deployments.apps "snapshot-controller" not found#6: deployments.apps "snapshot-controller" not found
```

after this repeated error message, we could see there is one suggested message:

```
2025/02/28 09:42:48 INFO: [pkg/controller/capi/upgrade/controlplane.go:651] WARNING! Not all addons are ready. Use the healthcheck command for more details before proceeding
```

In this situation we should run the healthcheck command before running the upgrade command at step 6 to make sure ccd cluster is in good healthy stage.

we could see the healthcheck command is at step 9.

unfortunately, we do not have test system to perform the test. we could see step 6 upgrade is stuck at the error message until the engineer stopped the script forcefully.

one thing you could check from your side about the new yaml file:

you could diff the old ccdadm-ccda-config.yaml with the new generated yaml file. we did perform the diff from our site file with the file you attached. Here is the list of the differences:

1, ip is not the same ==> it is ok

2, fqdn is not the same ==> it is ok

3, key values are not the same ==> it is normal for us also

we do not see any issues which cause step 6 is hanging there. Please perform the diff between the old ccdadm-ccda-config.yaml and the new generated file from your side.

The last thing if the customer just wants to access ccd cluster with passwordless. You donot need to perform 11.4 but you could simply add the new public ssh key in /home/ecccd/.ssh/authorized\_keys file. For us, this post-deployment step will not impact ccd because CCD deployment has completed successfully at this point. 11.4 just injects the new public ssh key into ccd cluster, however from your case, there is one checking failed at step 6 which cause the script hanging there.

We have assigned the ticket to the design team. Let us wait for the response from the design side.

Thanks,

BR/Zhigang

Comment by [Zhigang Han](#) [2025-02-28]

Hi Akshaya,

from CP1 II 11.4, it said 11.4 is only necessary if we donot have public SSH key in LLD. Have you put public SSH keys in LLD? If so, there is no need to do anything with 11.4 one thing: please add jumphost public SSH Keys in the LLD.

Thanks,

BR/Zhigang

[UCC\_PLM-246] [MANA-Vz# ccdm eric-ctrl-bro-0 continuous restart](#) Created: 2025-02-27 Updated: 2025-06-03 Resolved: 2025-06-03

Status:	Rejected
Project:	<a href="#">UCC_PLM</a>
Component/s:	None
Affects Version/s:	<a href="#">UCC Appliance 1.0.0</a>
Fix Version/s:	None

Type:	Bug	Priority:	Medium
Reporter:	<a href="#">Rajan Rajeshprasad Gupta</a>	Assignee:	<a href="#">Alvaro Martin</a>
Resolution:	Rejected	Votes:	0
Labels:	UCC, UCC_Appliance_1.1.0, Verizon		
Remaining Estimate:	Not Specified		
Time Spent:	Not Specified		
Original Estimate:	Not Specified		

Attachments:	vz-bro-pod.txt
Other Assignees:	Gonzalo Poveda
Team/s:	UCC_XFT2
Found in Build:	UCC Appliance 1.0.0
Requirement Status:	UCC Appliance 0.2.1 - UNCOVERED

#### Description

Hello,

During power recycle testing by Vz.

They have observed that the eric-ctrl-bro-0 pod from ccdm namespace continuously restart.

ecccd@ucc-ccda:~> kubectl get pod -A | grep -i bro

ccdm	eric-ctrl-bro-0	0/1	Running	<b>7940 (2m42s ago)</b>	<b>42d</b>
ccrc	eric-ctrl-bro-0	1/1	Running	8 (89m ago)	94d
ccsm	eric-ctrl-bro-0	1/1	Running	8 (89m ago)	93d
cnom	eric-ctrl-bro-7fc4ccfcf8-cfzcq	1/1	Running	7	92d

eda	eric-ctrl-bro-0	1/1	Running	7 (89m ago)	92d
ep5g	eric-ctrl-bro-0	1/1	Running	8 (89m ago)	93d
ep5g	eric-probe-event-report-broker-767c6d4c69-9p5mn	1/1	Running	7 (89m ago)	93d

Initial analysis indicate, Pod is restarting because of CMMRestClient (See below logs.)

Please help to find route cause and fix.

```
eccc@ucc-ccda:~> kubectl logs eric-ctrl-bro-0 -n ccdm | grep CMMRestClient | grep -i error
{"version":"1.2.0","timestamp":"2025-02-27T14:46:27.618-05:00","severity":"error","service_id":"eric-ctrl-bro","metadata":\{"pod_name":"eric-ctrl-bro-0","container_name":"eric-ctrl-bro","namespace":"ccdm"}
,"message":"Request failed with response <I/O error on GET request for \"https://eric-cm-mediator:5004/cm/api/v1/configurations\": Connection reset by peer (Write failed); nested exception is java.net.SocketException: Connection reset by peer (Write failed)>, due to <class org.springframework.web.client.ResourceAccessException>,"extra_data":{"location":
{"class":"com.ericsson.adp.mgmt.backupandrestore.cminterface.CMMRestClient"}}

}}
{"version":"1.2.0","timestamp":"2025-02-27T14:46:28.707-05:00","severity":"error","service_id":"eric-ctrl-bro","metadata":\{"pod_name":"eric-ctrl-bro-0","container_name":"eric-ctrl-bro","namespace":"ccdm"}
,"message":"Request failed with response <I/O error on GET request for \"https://eric-cm-mediator:5004/cm/api/v1/configurations\": Connection reset by peer (Write failed); nested exception is java.net.SocketException: Connection reset by peer (Write failed)>, due to <class org.springframework.web.client.ResourceAccessException>,"extra_data":{"location":
{"class":"com.ericsson.adp.mgmt.backupandrestore.cminterface.CMMRestClient"}}

}}
{"version":"1.2.0","timestamp":"2025-02-27T14:46:29.818-05:00","severity":"error","service_id":"eric-ctrl-bro","metadata":\{"pod_name":"eric-ctrl-bro-0","container_name":"eric-ctrl-bro","namespace":"ccdm"}
,"message":"Request failed with response <I/O error on GET request for \"https://eric-cm-mediator:5004/cm/api/v1/configurations\": Connection reset by peer (Write failed); nested exception is java.net.SocketException: Connection reset by peer (Write failed)>, due to <class org.springframework.web.client.ResourceAccessException>,"extra_data":{"location":
{"class":"com.ericsson.adp.mgmt.backupandrestore.cminterface.CMMRestClient"}}

}}
 {"version":"1.2.0","timestamp":"2025-02-27T14:46:30.836-05:00","severity":"error","service_id":"eric-ctrl-bro","metadata":\{"pod_name":"eric-ctrl-bro-0","container_name":"eric-ctrl-bro","namespace":"ccdm"}
,"message":"Request failed with response <I/O error on GET request for \"https://eric-cm-mediator:5004/cm/api/v1/configurations\": Received fatal alert: decrypt_error; nested exception is javax.net.ssl.SSLHandshakeException: Received fatal alert: decrypt_error>, due to <class org.springframework.web.client.ResourceAccessException>,"extra_data":{"location":
{"class":"com.ericsson.adp.mgmt.backupandrestore.cminterface.CMMRestClient"}}

}}
 {"version":"1.2.0","timestamp":"2025-02-27T14:46:31.904-05:00","severity":"error","service_id":"eric-ctrl-bro","metadata":\{"pod_name":"eric-ctrl-bro-0","container_name":"eric-ctrl-bro","namespace":"ccdm"}
,"message":"Request failed with response <I/O error on GET request for \"https://eric-cm-mediator:5004/cm/api/v1/configurations\": Connection reset by peer (Write failed); nested exception is java.net.SocketException: Connection reset by peer (Write failed)>, due to <class org.springframework.web.client.ResourceAccessException>,"extra_data":{"location":
{"class":"com.ericsson.adp.mgmt.backupandrestore.cminterface.CMMRestClient"}}

}}
eccc@ucc-ccda:~> kubectl logs eric-ctrl-bro-0 -n ccdm | grep CMMRestClient | grep -i error | wc
   31    933  19830
eccc@ucc-ccda:~>
eccc@ucc-ccda:~>
eccc@ucc-ccda:~> kubectl logs eric-ctrl-bro-0 -n ccdm | grep CMMRestClient | grep -i error | wc
   33    995  21108
eccc@ucc-ccda:~>
eccc@ucc-ccda:~>
eccc@ucc-ccda:~>
eccc@ucc-ccda:~> kubectl logs eric-ctrl-bro-0 -n ccdm | grep CMMRestClient | grep -i error | wc
   35   1049  22392
```

## Comments

Comment by Alexander Malikov [2025-06-03]

It's not reproducible with UCC 1.1

Comment by [Gonzalo Poveda](#) [2025-03-26]

For UCC 1.1, we could not observed this issue as we have more relevant issue after system restart with multiple pods from different NFs.. Once this generic issues is solved, we will check whether this particular pod still have this reported issue in UCC 1.1 or not

Comment by [Jim Dumont](#) [2025-02-28]

Test - did email go out because I added a comment?

Comment by [Zhigang Han](#) [2025-02-28]

Hi Rajan,

Yes, I totally agree with you about the idea to add the logic in our ISP pod to avoid the issue. I have assigned the ticket to the design team. Let us wait for the evaluation from the design team.

Thanks,

BR/Zhigang

Comment by [Rajan Rajeshprasad Gupta](#) [2025-02-28]

Hello Zhigang,

Thank you for feedback. you are right.

I found similar case as [https://metis.internal.ericsson.com/\\_layouts/ericsson.Metis/home.aspx#Permalink/ER/ER2937275](https://metis.internal.ericsson.com/_layouts/ericsson.Metis/home.aspx#Permalink/ER/ER2937275)

This is happening due to conflict issue between BRO and CM YangProvider.

Work-around applied:

Perform restart of pod eric-ctrl-bro-0 using 'kubectl -n ccdm delete pod eric-ctrl-bro-0'

Next step:

I see any opportunity to add logic in isp pod for work-around to avoid issue notice to our customer.

~8K restart for pod is not normal. Simple logic of verifying pod restart >100 and restarting eric-ctrl-bro-0 can solve problem.

Please let me know your view.

Comment by [Zhigang Han](#) [2025-02-28]

Hi Rajan,

from the error message, the error might happen from eric-cm-mediator pod side. Could you run the command on ccd server:

curl -k <https://eric-cm-mediator:5004/cm/api/v1/configurations> from the server to see if the connection is there or not?

you might need to find the service IP for eric-cm-mediator.

kubectl get svc -n ccdm | grep -i cm

```
eccd@ucc-ccda:~> kubectl get svc -n ccdm |grep -i cm
eric-cm-mediator           ClusterIP   10.101.53.97    <none>        5003/TCP,5004/TCP          30d
eric-cm-yang-provider       ClusterIP   10.104.132.245   <none>        8090/TCP                  30d
eric-cm-yang-provider-external LoadBalancer 10.110.106.13  172.20.180.66  830/TCP,22/TCP          30d
eric-udr-cmagent           ClusterIP   10.111.50.176   <none>        8080/TCP
```

curl -k <https://10.101.53.97:5004/cm/api/v1/configurations>

the result of the command looks like this:

```
eccd@ucc-ccda:~> curl -k https://10.101.53.97:5004/cm/api/v1/configurations
```

```
[{"name": "ericsson-data-collector-adp", "title": "diagnostic-data-collector"}, {"name": "ietf-keystore", "title": "Store ietf-keystore schema: v1.0"}, {"name": "ietf-system", "title": "ietf-system uploaded by AUM"}, {"name": "ietf-truststore", "title": "Store ietf-truststore schema: v1.0"}, {"name": "adp-gs-pm-br", "title": "ADP-GS PM Bulk Reporter Configuration"}, {"name": "ietf-netconf-acm", "title": ""}, {"name": "ericsson-swim", "title": "Ericsson Software Inventory Manager - Config: 1.1.0"}, {"name": "ericsson-brm", "title": "ericsson-brm"}, {"name": "ericsson-nrf-agent", "title": ""}, {"name": "ericsson-udr", "title": ""}, {"name": "ericsson-app-counters-udr", "title": ""}]
```

if service ip is not working, you could try the end point ip:

```
eccd@ucc-ccda:~> kubectl describe svc eric-cm-mediator -n ccdm
```

Name: eric-cm-mediator

Namespace: ccdm

Labels: app.kubernetes.io/instance=eric-ccdm-3

app.kubernetes.io/managed-by=Helm

app.kubernetes.io/name=eric-cm-mediator

```

app.kubernetes.io/version=8.14.0_16
helm.sh/chart=eric-cm-mediator-8.14.0_16
sidecar.istio.io/inject=false
Annotations: ericsson.com/product-name: CM Mediator HELM
ericsson.com/product-number: CXC 201 1506
ericsson.com/product-revision: 8.14.0
meta.helm.sh/release-name: eric-ccdm-3
meta.helm.sh/release-namespace: ccdm
Selector: app=eric-cm-mediator,release=eric-ccdm-3
Type: ClusterIP
IP Family Policy: SingleStack
IP Families: IPv4
IP: 10.101.53.97
IPs: 10.101.53.97
Port: http-rest 5003/TCP
TargetPort: http-rest/TCP
Endpoints: 192.168.1.254:5003
Port: https-rest 5004/TCP
TargetPort: https-rest/TCP
Endpoints: 192.168.1.254:5004
Session Affinity: None
Events: <none>

```

you could use end point ip to run curl command:

```
curl -k https://192.168.1.254:5004/cm/api/v1/configurations
```

the result looks like this:

```
eccd@ucc-ccda:~> curl -k https://192.168.1.254:5004/cm/api/v1/configurations
[{"name": "ericsson-data-collector-adp", "title": "diagnostic-data-collector"}, {"name": "ietf-keystore", "title": "Store ietf-keystore schema: v1.0"}, {"name": "ietf-system", "title": "ietf-system uploaded by AUM"}, {"name": "ietf-truststore", "title": "Store ietf-truststore schema: v1.0"}, {"name": "adp-gs-pm-br", "title": "ADP-GS PM Bulk Reporter Configuration"}, {"name": "ietf-netconf-acm", "title": ""}, {"name": "ericsson-swim", "title": "Ericsson Software Inventory Manager - Config: 1.1.0"}, {"name": "ericsson-brm", "title": "ericsson-brm"}, {"name": "ericsson-nrf-agent", "title": ""}, {"name": "ericsson-udr", "title": ""}, {"name": "ericsson-app-counters-udr", "title": ""}]
```

If both service IP and end point ip curl commands are not working, the issue probably is related to eric-cm-mediator pod. Probably after server is restarted, eric-cm-mediator pod is not coming up properly.

you need to delete eric-cm-mediator pod and then check if eric-ctrl-bro pod is up properly or not

Thanks,

BR/zhigang

#### [UCC\_PLM-199] Method to define additional PLMN post initial deployment Created: 2025-02-21 Updated: 2025-04-24 Resolved: 2025-04-24

<b>Status:</b>	Rejected
<b>Project:</b>	<a href="#">UCC_PLM</a>
<b>Component/s:</b>	None
<b>Affects Version/s:</b>	None
<b>Fix Version/s:</b>	None

<b>Type:</b>	Task	<b>Priority:</b>	Low
<b>Reporter:</b>	<a href="#">Jossy Pallan</a>	<b>Assignee:</b>	<a href="#">Jossy Pallan</a>
<b>Resolution:</b>	Rejected	<b>Votes:</b>	0
<b>Labels:</b>	None		
<b>Remaining Estimate:</b>	Not Specified		
<b>Time Spent:</b>	Not Specified		

<b>Original Estimate:</b>	Not Specified
---------------------------	---------------

#### Description

Customer would like to have a MoP for adding PLMN (5G/4G) post initial deployment with single PLMN.
---

#### Comments

Comment by <a href="#">Fredrik Gustavsson</a> [ 2025-02-21 ] Hi Jossy Pellan, this is a request for a procedure not currently part of the product. Please open a feature request to allow the architecture board to review it.
---

<b>[UCC_PLM-198] MELA: Telf # Static IP assignment to UE</b> Created: 2025-02-19 Updated: 2025-02-20 Resolved: 2025-02-20
---

<b>Status:</b>	Rejected
<b>Project:</b>	UCC_PLM
<b>Component/s:</b>	None
<b>Affects Version/s:</b>	None
<b>Fix Version/s:</b>	None

<b>Type:</b>	Bug	<b>Priority:</b>	Medium
<b>Reporter:</b>	Rajan Rajeshprasad Gupta	<b>Assignee:</b>	Reema Sidhwani
<b>Resolution:</b>	Rejected	<b>Votes:</b>	0
<b>Labels:</b>	None		
<b>Remaining Estimate:</b>	Not Specified		
<b>Time Spent:</b>	Not Specified		
<b>Original Estimate:</b>	Not Specified		

<b>Team/s:</b>	UCCPOCDEV
<b>Found in Build:</b>	UCC Appliance 1.0.1
<b>Requirement Status:</b>	UCC Appliance 0.2.1 - UNCOVERED

#### Description

Hello,  Telf customer needs static ip assignment for the apn pool. static ip assignment is nowhere mention as supported / not supported by ucc(restricted by ucc).  We offer ip-stickyness feature on smf, to allow 24 hour Ipaddress strickness which is near static ip address assignment.  Telf customer is not happy with feature as they have plan to power off ucc servers and router every day to save energy cost.  Question1: To feedback on roadmap to support UE static ip assignment? This also comes as one of the requirements from bubble7. So keep coming as requirement from different UCC customers.  Question2: Do we have any document or steps to support customer requirement or already tested with UCC?  If not, To support customer, we are thinking to prepare customize configuration for provisioning and pcx to meet requirement.
--

#### Comments

Comment by <a href="#">Zhigang Han</a> [ 2025-02-20 ]  Hi Rajan,  We do not think we support the fixed IP feature for UCC now. Please open a feature request from your side.  Thanks, BR/Zhigang
---

[UCC_PLM-197] MANA: cnat is clipping the leading zero forcing a 6 digit PLMN to 5 digit PLMN			
Created: 2025-02-14 Updated: 2025-04-24 Resolved: 2025-04-24			
Status:	Done		
Project:	<a href="#">UCC_PLM</a>		
Component/s:	None		
Affects Version/s:	<a href="#">UCC Appliance 1.0.1</a>		
Fix Version/s:	None		
Type:	Bug	Priority:	High
Reporter:	<a href="#">Rajan Rajeshprasad Gupta</a>	Assignee:	Unassigned
Resolution:	Closed	Votes:	0
Labels:	BAH, UCC_Appliance_1.1.0		
Remaining Estimate:	Not Specified		
Time Spent:	Not Specified		
Original Estimate:	Not Specified		
Issue Links:	<b>Association</b> Associates with <a href="#">UCCSUPPORT-45</a> cnat is clipping the leading zero for... Fix available - WFC Is Associated with <a href="#">UCCSUPPORT-45</a> cnat is clipping the leading zero for... Fix available - WFC		
Defect code_qmt:	1- Functional		
Sprint:	UCC XFT2 Sprint 6, UCC XFT2 Sprint 7, UCC XFT2 Sprint 8, UCC XFT2 Sprint 9		
Detected in phase:	Production		
Team/s:	UCC_XFT2		
Severity_qmt:	3- Medium		
Found in Build:	UCC Appliance 1.0.1		
Requirement Status:	UCC Appliance 0.2.1 - UNCOVERED		
<b>Description</b> cnat is clipping the leading zero forcing a 6 digit PLMN to 5 digit PLMN. This is causing authentication failure. Example scenario: 31001400000001 series for 310-014 PLMN This has caused issues in testing and additional PLMN config needed across the NF configuration.  <pre>ericsson@fe1-sfs:~/campus_ucc/old_config/templates/pcx\$ grep -e mnc *jinja2 pc-cre-config.txt:jinja2:{%- set mnc_short = mnc.lstrip('0') %} pc-cre-config.txt:jinja2:{%- set sig_domain = '5gc.mnc' + mnc + '.mcc' + mcc + '.3gppnetwork.org' %} pc-mm-config.txt:jinja2:{%- set mnc_short = mnc.lstrip('0') %} pc-mm-config.txt:jinja2:{%- set sig_domain = '5gc.mnc' + mnc + '.mcc' + mcc + '.3gppnetwork.org' %} pc-mm-config.txt:jinja2:mm amf selected-plmn-mobile-network-code mnc_short pc-mm-config.txt:jinja2:mm dns 5gc.mnc{{mnc}}.mcc{{mcc}}.3gppnetwork.org. pc-mm-config.txt:jinja2: dns-server dns1.mnc099.mcc244.3gppnetwork.org. pc-mm-config.txt:jinja2: dns-server dns2.mnc099.mcc244.3gppnetwork.org. pc-mm-config.txt:jinja2: mobile-network-code mnc_short pc-mm-config.txt:jinja2:mm imsins mcccnc_short pc-mm-config.txt:jinja2: default-apn-operator-id mnc{{mnc}}.mcc{{mcc}}.gprs pc-mm-config.txt:jinja2:mm plmn mcc mnc_short pc-mm-config.txt:jinja2: plmn-name mcccnc_short pc-mm-config.txt:jinja2:mm supi-range mcccnc_short pc-mm-config.txt:jinja2: default-dnn-operator-id mnc{{mnc}}.mcc{{mcc}}.gprs pc-sm-config.txt:jinja2:{%- set mnc_short = mnc.lstrip('0') %} pc-sm-config.txt:jinja2:{%- set sig_domain = '5gc.mnc' + mnc + '.mcc' + mcc + '.3gppnetwork.org' %} pc-sm-config.txt:jinja2:epg pgw home-plmn [ mcccnc_short ] values-ccpc.yaml:jinja2:{%- set mnc_short = mnc.lstrip('0') %} values-ccpc.yaml:jinja2:{%- set sig_domain = '5gc.mnc' + mnc + '.mcc' + mcc + '.3gppnetwork.org' %} values-pcc.yaml:jinja2:{%- set mnc_short = mnc.lstrip('0') %} values-pcc.yaml:jinja2:{%- set sig_domain = '5gc.mnc' + mnc + '.mcc' + mcc + '.3gppnetwork.org' %} values-pcg.yaml:jinja2:{%- set mnc_short = mnc.lstrip('0') %} values-pcg.yaml:jinja2:{%- set sig_domain = '5gc.mnc' + mnc + '.mcc' + mcc + '.3gppnetwork.org' %} ericsson@fe1-sfs:~/campus_ucc/old_config/templates/pcx\$</pre>			

## Comments

Comment by [Fredrik Gustavsson](#) [ 2025-03-20 ]

Thanks [Adrian-Bogdan Iliescu](#)! This is great news!

Comment by [Adrian-Bogdan Iliescu](#) [ 2025-03-20 ]

Config tested with success,

Fix is pushed in git in branch UCC\_Appliance\_Sprint\_7.

system\_admin@pcx-ccda#epg pgw apn internet user-info

result

output: -----

gc-0/1/1 (psc-0)

APN: internet

pdp_id	imsi	msisdn	nsapi	ip_address	dual_ip_address	delegated_ipv6_prefix	session_time	state
0xaaaaaaaaaaa0dabe410	244099000006001	860810000006001	5	10.23.0.2			164	IDLE(164s)
0xaaaaaaaaaaa05b63600	2440990000000001	860810000000001	5	10.23.0.3			8	IDLE(7s)

system\_admin@pcx-ccda#

system\_admin@pcx-ccda#

system\_admin@pcx-ccda#epg pgw user-info

Possible completions:

value Identifier for IMSI or Identifier for MSISDN

—

identifier-type

system\_admin@pcx-ccda#epg pgw user-info identifier-type im

Possible completions:

imei International Mobile Equipment Identity

imsi International Mobile Subscriber Identity

system\_admin@pcx-ccda#epg pgw user-info identifier-type imsi value 244099000000001

result

mobile-user-information:

subscriber-information:

imsi: 244099000000001

msisdn: 860810000000001

imei: 123400000000010

active-pdu-sessions:

active-pdu-session:

configuration-id: 82dq59ma-6vva-bqbe-r5z6-4qyynuc875xq

pdu-session-id: 5

dnn-in-use: internet

ue-requested-dnn: internet

dnn-selection-mode: VERIFIED

network-instance: iac

network-instance-selection:

n6-network-instance: iac

n3-network-instance: ran

ue-time-zone: UTC +00:00, Daylight Saving: +0h

rat-type: NR

charging-characteristic: 0(0x0000)

pcscf-reselection-support: No

an-type: 3GPP

pdu-type-in-use: IPv4

ssc-mode: SSC\_MODE\_1

ue-address-1:

ipv4: 10.23.0.3

ip-address-allocation-method: Shared IP Pool

eps-interworking-indication: WITH\_N26

shared-ip-pool: shared-ip-pool-iac-ccda

session-ambr:

uplink-kbps: 512000

downlink-kbps: 512000

pause-charging:

paused-charging-supported: No

charging-paused: No

policy-charging-rule-scope: pc\_ruleScope1

policy-control-information:

- n7-profile-id: n7-1
- local-policy-control-profile: lpc\_profile1
- supported-n7-features: -
- event-triggers: SE\_AMBR\_CH, DEF\_QOS\_CH, PLMN\_CH, RAT\_TY\_CH

single-nssai:

- slice-service-type: 1
- slice-differentiator: 000001

nr-location:

tai:

- plmn-id: mnc099.mcc244
- tac: 2

ncgj:

- plmn-id: mnc099.mcc244
- nr-cell-id: 328925184

timestamp: 2025-03-20T12:00:54Z

amf-information:

- amf-id: d67766fc-210f-4ecf-858f-000000a1c1d1
- address: not available

n3-interface:

ran-fteid:

- teid: 1342177282
- address: 172.5.32.0

upf-fteid:

- teid: 391118884
- address: 214.13.226.0

up-status: activated

n4-interface:

local-fseid:

- seid: 95827456
- address: 172.16.2.4

remote-fseid:

- seid: 3359685459457343619
- address: 172.16.2.6

n7-interface:

npcf-sm-policy-control:

- nf-service-id: d67766fc-210f-4ecf-858f-000000c1c1d1 npcf-smpolicycontrol
- nf-set-id: set01.pcfset.5gc.mnc099.mcc244
- binding-indication: bl=nf-instance; nfinst=d67766fc-210f-4ecf-858f-000000c1c1d1; nfset=set01.pcfset.5gc.mnc099.mcc244

ip-end-points:

- ip-end-point:

fqdn: pcf-pcx-stcucc6a.5gc.mnc099.mcc244.3gppnetwork.org

sm-policy-id: 24409900000001%7C5%7C1742472054777232

n10-interface:

nudm-uecm:

- nf-service-id: 841d1b7c-5103-11e9-8c09-55444da1c1d1 nudm-uecm
- nf-set-id: -
- binding-indication: -

ip-end-points:

- ip-end-point:

fqdn: udm-ccsm-stcucc6a.5gc.mnc099.mcc244.3gppnetwork.org

nudm-sdm:

- nf-service-id: 841d1b7c-5103-11e9-8c09-55444da1c1d1 nudm-sdm
- nf-set-id: -
- binding-indication: -

ip-end-points:

- ip-end-point:

fqdn: udm-ccsm-stcucc6a.5gc.mnc099.mcc244.3gppnetwork.org

n11-interface:

namf-comm:

  nf-service-id: d67766fc-210f-4ecf-858f-000000a1c1d1 namf-comm-https

  nf-set-id: set001.region01.amfset.5gc.mnc099.mcc244

  binding-indication: bl=nf-instance; nfinst=d67766fc-210f-4ecf-858f-000000a1c1d1; nfset=set001.region01.amfset.5gc.mnc099.mcc244

  ip-end-points:

    ip-end-point:

      fqdn: amf-pcx-stcucc6a.amf.5gc.mnc099.mcc244.3gppnetwork.org

nsmf-pdusession:

  binding-indication: bl=nf-instance; nfinst=d67766fc-210f-4ecf-858f-000000a1c1d1; nfset=set001.region01.amfset.5gc.mnc099.mcc244; scope=callback;

servname=custom-000193-namf-smfstatusnotify

  sm-context-status-uri: <https://amf-pcx-stcucc6a.amf.5gc.mnc099.mcc244.3gppnetwork.org:8443/callbacks/nsmf-pdusession/v1/imsi-244099000000001/sm-contexts/-576460752303415069>

qos-flows:

predefined-rules:

  pcc-rule:

    name: acr-unconditional

    rating-group-id: 255

    offline-charging: Disabled

    online-charging: Disabled

    status: active

  activated-by:

    local-policy:

      condition: unconditional

session-rules:

  session-rule:

    name: 244099000000001|5|1742472054777232;sessRuleId1

    status: in-use

  auth-session-ambr:

    downlink-kbps: 512000

    uplink-kbps: 512000

  auth-default-qos:

    fiveQi: 6

  arp:

    priority-level: 7

    pre-emption-capability: Enabled

    pre-emption-vulnerability: Enabled

qos-flow:

  qos-flow-id: 5

  charging-id: 2617246061

  qos-in-use:

    fiveqi: 6

    uplink-dscp-value: AF31

    downlink-dscp-value: AF31

    mbr-dl-kbps: 512000

    mbr-ul-kbps: 512000

    gbr-dl-kbps: 0

    gbr-ul-kbps: 0

  allocation-retention-priority:

    priority-level: 7

    pre-emption-capability: Enabled

    pre-emption-vulnerability: Enabled

pcf-binding-information:

  snssai-sst: 1

  snssai-sd: 000001

  ueip: 10.23.0.3

  dnn: internet

  ipDomain:

  supi: imsi-244099000000001

  gpsi: msisdn-86081000000001

pcfId: d67766fc-210f-4ecf-858f-000000c1c1d1  
pcfDiameterHost:  
pcfDiameterRealm:  
smPolicyId: 244099000000001%7C5%7C1742472054777232  
pcfIpEndPoints:  
pcfFqdn: pcf-pcx-stcucc6a.5gc.mnc099.mcc244.3gppnetwork.org

creation-time: 2025-03-20 12:00:54

pdr-in-use:

pdr:  
pdr-id: 1  
type: predefined-pcc-rule  
qfi: 5  
far-id: 1  
qer-id-list: 1  
precedence: 255  
source\_interface: Access  
predefined-pcc-rule-name: acr-unconditional

pdr:  
pdr-id: 2  
type: predefined-pcc-rule  
far-id: 2  
qer-id-list: 1, 4  
precedence: 255  
source\_interface: Core  
predefined-pcc-rule-name: acr-unconditional

far-in-use:

far:  
far-id: 1  
qfi: 5  
direction: Uplink  
destination\_interface: Core

far:  
far-id: 2  
qfi: 5  
direction: Downlink  
destination\_interface: Access

qer-in-use:

qer:  
qer-id: 1  
type: Apn-Ambr  
dl-gate-status: OPEN  
ul-gate-status: OPEN  
mbr-ulink-kbps: 512000  
mbr-dlink-kbps: 512000

qer:  
qer-id: 4  
type: Qfi  
qfi: 5  
dl-gate-status: OPEN  
ul-gate-status: OPEN

system\_admin@pcx-ccda#epg pgw user-info identifier-type imsi value 244099000006001

result

mobile-user-information:

subscriber-information:  
imsi: 244099000006001  
msisdn: 860810000006001  
imei: 123400000060010  
imeisv: 1234000000600101  
imsi-authenticated: Yes  
low-access-priority-indication: No

active-pdn-connections:

active-pdn-connection:  
configuration-id: 82dq59ma-6vva-bqbe-r5z6-4qyynuc875xq  
suspended: No

apn-in-use: internet  
apn-selection-mode: UE or NW provided APN, subscribed verified  
network-instance: iac

network-instance-selection:  
  n6-network-instance: iac

ue-time-zone: UTC +00:00, Daylight Saving: +0h  
charging-characteristic: 256(0x0100)  
policy-charging-rule-scope: pc\_ruleScope1  
charging-characteristic-profile: profile1  
pcscf-reselection-support: No  
pdn-type-in-use: IPv4  
framed-route: 0.0.0.0/0  
ip-address-allocation-method: Shared IP Pool  
support-5gs-interworking: Yes

nssai:  
  slice-service-type: 1  
  slice-differentiator: 000001

shared-ip-pool: shared-ip-pool-iac-ccda  
access-type: 3GPP\_ACCESS

addresses-in-use:  
  end-user-address-1: 10.23.0.2

apn-ambr:  
  uplink-kbps: 512000  
  downlink-kbps: 512000

serving-plmn-rate-control:  
  splmn-dl-status: Disabled  
  splmn-dl-rate: 0  
  splmn-ul-rate: 0

sx:  
  control-plane-sx-ip-address: 172.16.2.4  
  control-plane-seid: 229368848  
  user-plane-sx-ip-address: 172.16.2.6  
  user-plane-seid: 3359685459457343618

policy-control-information:  
  n7-profile-id: n7-1  
  local-policy-control-profile: lpc\_profile1  
  supported-n7-features: -  
  event-triggers: SE\_AMBR\_CH, DEF\_QOS\_CH, PLMN\_CH, RAT\_TY\_CH

authorized-qos:  
  apn-ambr-ul-kbps: 512000  
  apn-ambr-dl-kbps: 512000  
  default-bearer-qci: 6

default-bearer-arp:  
  priority-level: 7  
  pre-emption-capability: Enabled  
  pre-emption-vulnerability: Enabled

n7-interface:

  npcf-sm-policy-control:  
    nf-service-id: d67766fc-210f-4ecf-858f-000000c1c1d1 npcf-smPolicyControl  
    nf-set-id: set01.pcfset.5gc.mnc099.mcc244  
    binding-indication: bl=nf-instance; nfinst=d67766fc-210f-4ecf-858f-000000c1c1d1; nfset=set01.pcfset.5gc.mnc099.mcc244

  ip-end-points:  
    ip-end-point:  
      fqdn: pcf-pcx-stcucc6a.5gc.mnc099.mcc244.3gppnetwork.org  
      sm-policy-id: 244099000006001%7C5%7C1742471898383330

creation-time: 2025-03-20 11:58:18

active-bearers:

  active-bearer:  
    bearer-id: 5  
    bearer-type: Default  
    bearer-control-mode: Network and UE

rat-type: EUTRAN  
plmn-id: mnc099.mcc244  
ims-signaling-bearer: No  
protocol-in-use: GTPv2  
charging-id: 3892314986  
dt-active-for-this-bearer: No

serving-node:  
  serving-node-in-use: Combined SGW/PGW  
  control-plane-ip-address: 172.16.2.11  
  control-plane-teid: 229114032  
  user-plane-ip-address: 172.16.2.13  
  user-plane-teid: 391118882

gateway-node:  
  gateway-node-in-use: PGW  
  control-plane-ip-address: 172.16.2.9  
  control-plane-teid: 229368848  
  cpb-location: gc-0/1/1  
  user-plane-ip-address: 214.13.226.10  
  user-plane-source-port: 2152  
  user-plane-teid: 391118882

predefined-rules:

  pcc-rule:  
    name: acr-unconditional  
    rating-group-id: 255  
    offline-charging: Disabled  
    online-charging: Disabled  
    status: active

  activated-by:  
    local-policy:  
      condition: unconditional

  qos-in-use:  
    uplink-dscp-value: AF31  
    downlink-dscp-value: AF31  
    mbr-dl-kbps: -  
    mbr-ul-kbps: -  
    gbr-dl-kbps: -  
    gbr-ul-kbps: -  
    qci: 6

  allocation-retention-priority:  
    priority-level: 7  
    pre-emption-capability: Enabled  
    pre-emption-vulnerability: Enabled

pcf-binding-information:  
  snssai-sst: 1  
  snssai-sd: 000001  
  uelp: 10.23.0.2  
  dnn: internet  
  ipDomain:  
    supi: imsi-244099000006001  
    gpsi: msisdn-860810000006001  
    pcfId: d6776fc-210f-4ecf-858f-000000c1c1d1  
    pcfDiameterHost:  
    pcfDiameterRealm:  
      smPolicyId: 244099000006001%7C5%7C1742471898383330  
      pcfIpEndPoint:  
        pcfFqdn: pcf-pcx-stcucc6a.5gc.mnc099.mcc244.3gppnetwork.org

pdr-in-use:

  pdr:  
    pdr-id: 1  
    type: predefined-pcc-rule  
    bearer-id: 5  
    far-id: 1  
    qer-id-list: 1  
    precedence: 255

```
source_interface: Access
predefined-pcc-rule-name: acr-unconditional

pdr:
  pdr-id: 2
  type: predefined-pcc-rule
  bearer-id: 5
  far-id: 2
  quer-id-list: 1
  precedence: 255
  source_interface: Core
  predefined-pcc-rule-name: acr-unconditional

far-in-use:

far:
  far-id: 1
  bearer-id: 5
  direction: Uplink
  destination_interface: Core

far:
  far-id: 2
  bearer-id: 5
  direction: Downlink
  destination_interface: Access

quer-in-use:
```

```
quer:
  quer-id: 1
  type: Apn-Ambr
  dl-gate-status: OPEN
  ul-gate-status: OPEN
  mbr-ulink-kbps: 512000
  mbr-dlink-kbps: 512000
```

system\_admin@pcx-ccda#

Comment by [Fredrik Gustavsson](#) [ 2025-03-19 ]

Thanks for the update [Adrian-Bogdan Iliescu](#)!

Comment by [Adrian-Bogdan Iliescu](#) [ 2025-03-19 ]

hi,  
we are working on this.  
We agreed and updated LLD to support mnc with 3 or 2 digits and now we are working to implement and test.

Thank you and sorry for late reply

Comment by [Fredrik Gustavsson](#) [ 2025-02-25 ]

[Adrian-Bogdan Iliescu](#), do you have any suggestion for how to move this forward?

Comment by [Rajan Rajeshprasad Gupta](#) [ 2025-02-14 ]

Hello Fredrik, Adrian,

Please find this information from the MANA Pre-staging environment, where we are attempting to simulate the issue reported for BAH

```
system_admin@pcx-ccda#show mm amf
mm amf
amf-fqdn      amf-pcx-jucca.amf.5gc.mnc014.mcc310.3gppnetwork.org
amf-inter-plmn-fqdn amf-pcx-jucca.amf.5gc.mnc014.mcc310.3gppnetwork.org
gnodeb 310-014-782064
gnodeb-name      UERANSIM-gnb-310-14-782064
gnodeb-status    disconnected
equipment-position 0.0
last-gnodeb-status-update 2025-02-13,14:12:52
gnodeb 310-14-782064
gnodeb-name      UERANSIM-gnb-310-14-782064
gnodeb-status    disconnected
equipment-position 0.0
last-gnodeb-status-update 2025-02-13,16:03:07
ng-tracking-area 310-014-41201
ng-tracking-area 310-14-41201
ng-tracking-area-authorized-slice 310-014-41201
authorized-slice ""
ng-tracking-area-authorized-slice 310-14-41201
authorized-slice ""
ng-tracking-area-supported-slice 310-014-41201
```

```
supported-slice      1-1
slice-consistent-check consistent
ng-tracking-area-supported-slice 310-14-41201
supported-slice      1-1
slice-consistent-check consistent
system_admin@pcx-ccda#
```

Comment by [Fredrik Gustavsson](#) [ 2025-02-14 ]

Rajan Rajeshprasad Gupta, if you have access to the customer system, or can ask someone that has, please give us the output from "show mm amf" so we can verify the fqdns calculated by AMF.

Comment by [Fredrik Gustavsson](#) [ 2025-02-14 ]

Thanks Adrian,

I agree with step #1 and #3, but could the below be another alternative to overcome the fqdn requirements?

- in case the mnc is two digits, then pad with a leading zero for the fqdns only

That way we will preserve the mnc, as specified in the LLD, for the amf/smf (or other CNFs).

We also spoke about presenting the IMSI sequence that must be used based on the LLD input for MCC/MNC. But that should be easy if we use the MCC/MNC as specified.

Comment by [Adrian-Bogdan Iliescu](#) [ 2025-02-14 ]

Ok, So as we discussed, we can't just remove this lstrip function, but I see a good solution to change the approach:

1. define in LLD mnc and MCC as it should be ( if you want to have imsi range 24499 , then will be a pair of 244 and 99, if you want to have the imsi range 244099 then the pair will be 244/099).
2. AMF fqdn and other parts from MM will not accept "0" in front, like I shown above and for these we have to remove unused "0"
3. propagate this in all scripts/files and perform 2 tests with 6 digits and 5 digits.
4. Estimation time 1week with many CNF deployments

Comment by [Fredrik Gustavsson](#) [ 2025-02-14 ]

Thanks Adrian-Bogdan Iliescu,

It is worrying that PCX doesn't support this. We need to verify if this is introduced there or if it is coming from PCC/PCG.

The example that the customer faced was with MNC=014:

*cnav is clipping the leading zero forcing a 6 digit PLMN to 5 digit PLMN. This is causing authentication failure. Example scenario:  
31001400000001 series for 310-014 PLMN*

Comment by [Adrian-Bogdan Iliescu](#) [ 2025-02-14 ]

Hi Fredrik Gustavsson,

the thing is that in PCX if mnc is starting with 0 it is needed sometimes all 3 digits other times we need to remove the 0 in front, for example:

```
system_admin@pcx-ccda(config)#do show running-config mm amf
...
mm amf selected-plmn-mobile-country-code 244
mm amf selected-plmn-mobile-network-code 99
...
system_admin@pcx-ccda(config)#mm amf selected-plmn-mobile-network-code 099
system_admin@pcx-ccda(config)#validate
```

Failed: 'eypvalid:yang-provider-validation': Validation failed: Validation failed for module ericsson-pc-mm, errors:

/ericsson-pc-mm:mm/plmn:**Error** amf selected-plmn-mobile-network-code 099 selected-plmn-mobile-country-code 244; Inconsistent Configuration; amf selected-plmn-mobile-network-code Mnc selected-plmn-mobile-country-code Mcc; The selected PLMN can not be found in the list of PLMNs. Ensure that the MNC and MCC match an existing PLMN that supports NR.

```
system_admin@pcx-ccda(config)#mm amf selected-plmn-mobile-network-code 99
system_admin@pcx-ccda(config)#validate
```

**Validation complete**

just skipping the strip of mnc will not work, config will not be accepted by PCC.

We need to investigate more deeper. Maybe you can provide more concrete examples

Comment by [Fredrik Gustavsson](#) [ 2025-02-14 ]

This seems to be part of the jinja templates produced by UCC. E.g.:

```
./config/templates/pcx/pc-cre-config.txt.jinja2:{% set mnc_short = mnc.lstrip('0') %}
```

MCCs are always 3 digits, and MNCs may be two or three digits and should never be altered.

An MNC=010 is different than an MNC=10

I'm forwarding this to design for an investigation of the fix.

[UCC\_PLM-196] UCC 1.0 : Unnecessary Router Configurations Causing Concerns for Customers Created: 2025-02-12 Updated: 2025-04-24 Resolved: 2025-04-24

Status:	Done
Project:	UCC_PLM
Component/s:	None
Affects Version/s:	UCC Appliance 1.0.1
Fix Version/s:	None

Type:	Bug	Priority:	Medium
Reporter:	Rajan Rajeshprasad Gupta	Assignee:	Unassigned
Resolution:	Closed	Votes:	0
Labels:	UCC_Appliance_1.1.0		
Remaining Estimate:	Not Specified		
Time Spent:	Not Specified		
Original Estimate:	Not Specified		

Issue Links:	Association		
	Is Associated with	<a href="#">UCCSUPPORT-42</a>	T-Mobile Request to disable bpdu tow...
Defect code_qmt:	3- Usability		
Detected in phase:	Staging		
Team/s:	UCC_XFT2		
Severity_qmt:	3- Medium		
Found in Build:	UCC Appliance 1.0.1		
Requirement Status:	UCC Appliance 0.2.1 - UNCOVERED		

#### Description

Hello,  
As per 1.0 LLD design.  
Ports 1/23 and 1/24 are used for customer network connections. CNAT generates router configurations for these ports, with VLAN tags assigned as 1100, 1101, and 1313.  
Could you please clarify the purpose of these additional VLAN tags and explain how it will benefit the customer?  
We should not generate dummy configuration which is questionable by customer. Please help to correct CNAT for router configuration generation if above tagging is dummy.

See configuration generated by CNAT:

```
port ethernet 1/23 10ge
description customer uplink
no shutdown
encapsulation dot1q
!
!
service-instance 1100
match
dot1q 1100
!
service-instance 1101
match
dot1q 1101
!
service-instance 1313
match
dot1q 1313
!
port ethernet 1/24 10ge
description customer uplink
no shutdown
encapsulation dot1q
!
!
service-instance 1100
match
dot1q 1100
```

```
!
service-instance 1101
match
dot1q 1101
!
service-instance 1313
match
dot1q 1313
!
```

## Comments

Comment by [Adrian Michel](#) [ 2025-03-19 ]

The ports are now removed from the bridges. Basically the fix is the solution for this ticket:  
[UCCXFT-740](#) UCC1.1 drop2: router configuration created by cnat gives CCT no found - eTeamProject Alpha  
It will come with the next drop.

Comment by [Fredrik Gustavsson](#) [ 2025-03-04 ]

Thanks [Andrea Maio](#), this makes it more clear.

[Meryam Nachi](#), I believe that this will result in two tasks for your team:

1. Update the router configuration to remove the existing port 23/24 config
2. Document this need for integration and what contexts are used for what

Comment by [Andrea Maio](#) [ 2025-03-04 ]

Hi,

I forgot to mention that from the security team we are receiving requests to implement ACLs in the external interfaces of the router to comply with GPR.

In order to automate this process over time, it is reasonable to place the border of the automation process at interface level where the ACLs will be configured.

Thanks.

Comment by [Andrea Maio](#) [ 2025-03-04 ]

Hi,

We are removing from the automation process the VLAN, and routing configuration, for external links in UCC 1.1. It was not there anyway in UCC 1.0.

Due to the many possible solutions, as part of the delta configuration, the engineer will need to negotiate with the customer the external connectivity (uplinks) for the interfaces N6(s), N32,Rx,RAN, OAM, Sig\_Ext.

This decision comes after confronting CUs and the architects board: customers embed the UCC in very different ways in their solutions. Thus, it is very difficult, if not impossible, to provide automation all the way down to VLAN and port level, there are too many different cases. It seems clear that we are already configuring these levels as delta.

We identified a reasonable border for the automation process for the router at interface level. That means, that for the external links we configure the interfaces, and their IPs, in the relevant VRFs, while, as delta in prestige, the engineer would need to bind the ports (physical + VLAN/LAG) and configure the routing (static/dynamic) in the peripherical VRFs of the router.

Many Thanks

Comment by [Meryam Nachi](#) [ 2025-02-18 ]

Hi [Soner Mus](#) and [Fredrik Gustavsson](#) : This should be part of the IP Design team. We can also check if Lucas can help here as well.

Comment by [Soner Mus](#) [ 2025-02-14 ]

Hello [Fredrik Gustavsson](#),

Due to resource constraints, Andrea from my team is currently supporting the IP Study (including IPv6, Mobility, etc.). However, tasks related to Router Configuration or LLD (such as facilitating CNAT configuration creation) are not within the scope of this support.

XFT3 is assisting with Network Design due to limited availability and expertise/know-how. While CNAT serves as a tool to automate procedures and configurations, its core logic and templating are not part of the development efforts.

[Meryam Nachi](#) do you think it is part of XFT2 responsibility ?

Many Thanks

Comment by [Fredrik Gustavsson](#) [ 2025-02-14 ]

Hi [Soner Mus](#), this seems related to the overall network design of UCC that Andrea has been working on lately.

I believe that if we are to use VLANs on the UCC front, then those must be defined in the LLD site data for the customer to be able to alter them.

Please investigate on how we can improve in this area.

[UCC\_PLM-195] UCC MELA : CRE complaints for OOM while running ITC to capture BGP messages Created: 2025-02-12 Updated: 2025-06-19 Resolved: 2025-06-19

Status:	Rejected
Project:	UCC_PLM
Component/s:	None
Affects Version/s:	UCC Appliance 1.0.1
Fix Version/s:	None

Type:	Bug	Priority:	Low
Reporter:	Rajan Rajeshprasad Gupta	Assignee:	Adrian-Bogdan Iliescu
Resolution:	Rejected	Votes:	0
Labels:	Telefonica		
Remaining Estimate:	0h		
Time Spent:	4h		
Original Estimate:	Not Specified		

Defect code_qmt:	3- Usability
Sprint:	UCC XFT2 Sprint 11
Detected in phase:	Production
Team/s:	UCC_XFT2
Severity_qmt:	3- Medium
Found in Build:	UCC Appliance 1.0.1
Requirement Status:	UCC Appliance 0.2.1 - UNCOVERED

#### Description

Hello,

Telf UCC is experiencing an issue with setting up BGP on the R6K router.

To troubleshoot the BGP failure on the PCX, standard CPI troubleshooting CLI commands were utilized, as outlined below

"tracing itc start service routing-engine"

However, the UCC cRE has insufficient memory, which is preventing the use of basic troubleshooting CLI commands

```
system_admin@pcx-ccda#tracing itc start service routing-engine
Error:Failed to execute action start, message: Failed: Application error: eric-pc-routing-engine-9b598c5b5-phzqq;eric-pc-routing-engine: Out of memory.;"
```

```
eccd@ucc-ccda:~> kubectl top pod eric-pc-routing-engine-9b598c5b5-phzqq -n ep5g
NAME                  CPU(cores)   MEMORY(bytes)
eric-pc-routing-engine-9b598c5b5-phzqq  20m        107Mi
eccd@ucc-ccda:~>
```

```
eccd@ucc-ccda:~> kubectl describe pod eric-pc-routing-engine-9b598c5b5-phzqq -n ep5g | grep memory
memory:                 512Mi
memory:                 100Mi
```

Kindly assess the current situation and consider one of the following actions:

- Increase the memory of the pod to enable at least the basic troubleshooting capabilities.
- Document UCC-specific troubleshooting guidelines to replace the standard PCC CPI and adhere to the UCC-specific approach

#### Comments

Comment by <a href="#">Zhigang Han</a> [ 2025-06-19 ]
Hi Rajan,

for the second question from you, I think you could open an improvement ticket.

Thanks,

BR/Zhigang

Comment by [Adrian-Bogdan Iliescu](#) [ 2025-06-19 ]

Ok,

It is rejected.

We'll find a place in our documents to mentioned that ITC is not supported. Thank you

Comment by [Zhigang Han](#) [ 2025-06-19 ]

Hi Adrian,

Could you reject the ticket from your side if we do not support the feature?

Thanks,

BR/Zhigang

Comment by [Adrian-Bogdan Iliescu](#) [ 2025-06-19 ]

Hi colleagues,

We received confirmation from EP5G that ITC is not supported(implemented) so increasing the memory is not helping.

Thx

Comment by [Adrian-Bogdan Iliescu](#) [ 2025-06-13 ]

hi,

I opened the TR as you suggested:

[ [PCTR-94543] [UCC] [PCX 1.16EP1] - CRE out-of-memory when ITC tracing is started - PDU Packet Core JIRA | <https://pdupc-jira.internal.ericsson.com/browse/PCTR-94543> ] ]

Comment by [Alexander Malikov](#) [ 2025-06-13 ]

[Adrian-Bogdan Iliescu](#), could you please raise a ticket towards to EP5G PDU to confirm if this feature is supported or not in our resource profile?

Comment by [Rajan Rajeshprasad Gupta](#) [ 2025-05-02 ]

[Jim Dumont](#) It is not fixed yet. waiting for feedback from XFT.

Comment by [Jim Dumont](#) [ 2025-05-01 ]

[Rajan Rajeshprasad Gupta](#) is this still an issue with UCC 1.1? If not, can it be cancelled/rejected as not reproducible?

Comment by [Zhigang Han](#) [ 2025-02-19 ]

Hi Rajan,

Due to the limitation of hardware resource for UCC solution, UCC will not fully support for 5GC features. We have assigned the ticket to the design team. Let us wait for the design's response.

Thanks,

BR/Zhigang

Comment by [Rajan Rajeshprasad Gupta](#) [ 2025-02-14 ]

Hello Zhigang,

Thank you for feedback.

While troubleshooting Telf UCC issue, we tried with help to customer to set lowest buffer of "1", however it fails as cRE memory assigned in UCC is too low.

Some print from UCC system.

```
system_admin@pcx-ccda#tracing itc start service routing-engine buffer 50
Error:Failed to execute action start, message: Failed: Application error: eric-pc-routing-engine-5644fc4bcf-4d4lz:eric-pc-routing-engine: Out of memory.:
system_admin@pcx-ccda#tracing itc start service routing-engine buffer 10
Error:Failed to execute action start, message: Failed: Application error: eric-pc-routing-engine-5644fc4bcf-4d4lz:eric-pc-routing-engine: Out of memory.:
system_admin@pcx-ccda#tracing itc start service routing-engine buffer 1
Error:Failed to execute action start, message: Failed: Application error: eric-pc-routing-engine-5644fc4bcf-4d4lz:eric-pc-routing-engine: Out of memory.:
system_admin@pcx-ccda#tracing itc start service routing-engine
Error:Failed to execute action start, message: Failed: Application error: eric-pc-routing-engine-5644fc4bcf-4d4lz:eric-pc-routing-engine: Out of memory.:
system_admin@pcx-ccda#timestamp enable
system_admin@pcx-ccda#tracing itc start service routing-engine
Fri Feb 14 13:11:26.848 UTC-06:00
Error:Failed to execute action start, message: Failed: Application error: eric-pc-routing-engine-5644fc4bcf-4d4lz:eric-pc-routing-engine: Out of memory.:
system_admin@pcx-ccda#tracing itc start service routing-engine buffer 1
```

Fri Feb 14 13:12:15.973 UTC-06:00

Error:Failed to execute action start, message: Failed: Application error: eric-pc-routing-engine-5644fc4bcf-4d4l;eric-pc-routing-engine: Out of memory.; system\_admin@pcx-ccda#

- ◦   ▪ IDLE TIMEOUT \*\*\*

Connection to 10.97.117.64 closed.

Comment by [Fredrik Gustavsson](#) [ 2025-02-14 ]

Hi [Meryam Nachi](#), please look into this issue.

As you can see, we have at least two alternatives to move forward:

1. instructions on what buffer sized to use to support UCC profile
2. altering the allocated/max pod memory size

Comment by [Zhigang Han](#) [ 2025-02-14 ]

Hi Rajan,

Here is the reason we are having the error message out of memory:

If the configured buffer size exceeds 50% of the current free memory buffer on a PC VPN Gateway Forwarder or a Routing Engine instance, ITC cannot be started on this instance.

An error message is displayed for this instance when starting ITC.

"system\_admin@pcx-ccda#tracing itc start service routing-engine

Error:Failed to execute action start, message: Failed: Application error: eric-pc-routing-engine-9b598c5b5-phzqq;eric-pc-routing-engine: Out of memory;"

the command which you used is probably using the default buffer size which the buffer size is exceeds 50% of the current free memory on a routing engine instance.

Actually we could define the buffer size. Here is the example :

user@host#tracing itc start service routing-engine buffer 65524

65524 is just an example. you could play around with the buffer size.

We do not think we should hack the pod memory size, but we should be able to set the small buffer size.

Thanks,

BR/Zhigang

### [UCC\_PLM-193] MELA-Observing No license in Router for port 1/29 to 1/36 after Power OFF

Created: 2025-02-07 Updated: 2025-02-25 Resolved: 2025-02-25

Status:	Rejected
Project:	<a href="#">UCC_PLM</a>
Component/s:	None
Affects Version/s:	<a href="#">UCC Appliance 1.0.1</a>
Fix Version/s:	None

Type:	Bug	Priority:	High
Reporter:	<a href="#">Akshaya Avin Shetty</a>	Assignee:	Unassigned
Resolution:	Rejected	Votes:	0
Labels:	None		
Remaining Estimate:	Not Specified		
Time Spent:	Not Specified		
Original Estimate:	Not Specified		

Attachments:	<a href="#"> After reboot logs-1.zip</a> <a href="#"> After reboot logs.zip</a> <a href="#"> BGP logs ECCD.txt</a> <a href="#"> image-2025-02-07-19-34-52-339.png</a> <a href="#"> image-2025-02-10-20-00-47-468.png</a> <a href="#"> image-2025-02-10-20-01-16-961.png</a> <a href="#"> image-2025-02-10-20-01-34-582.png</a> <a href="#"> image-2025-02-14-11-12-06-363.png</a> <a href="#"> image-2025-02-18-23-57-49-038.png</a> <a href="#"> image-2025-02-20-11-44-47-118.png</a> <a href="#"> router-config-diff.txt</a> <a href="#"> router-config-post-reset.txt</a> <a href="#"> Router logs after 2nd reboot-1.zip</a> <a href="#"> Router logs after 2nd reboot.zip</a> <a href="#"> Router logs before 2nd reboot-1.zip</a> <a href="#"> Router logs before 2nd reboot.zip</a> <a href="#"> Routers_Output.txt</a> <a href="#"> show configuration_Feb 11.txt</a> <a href="#"> show configuration_router.txt</a> <a href="#"> Telefonica_logs.zip</a> <a href="#"> UCC_0.2.2_cabling.png</a> <a href="#"> UCC_1.0_CP1_cabling.png</a>
Detected in phase:	Staging

<b>Team/s:</b>	UCC_PLM
<b>Found in Build:</b>	UCC Appliance 1.0.1
<b>Requirement Status:</b>	UCC Appliance 0.2.1 - UNCOVERED

#### Description

Hello All,

We recently upgraded UCC from 0.2.2 to 1.0\_CP1 in the Telefonica network. After the upgrade, we successfully tested both 4G and 5G calls. However, after performing a shutdown and powering the system back on, we encountered multiple alarms on PCX (Diameter, S10, Sx, etc.).

Upon investigation, we found that:

BGP neighbors are down in context sig and other context too

Ports 1/29 to 1/36 show "No License".

Router license check indicates that the Capacity Key for R6000-1x25G port capacity license and R6000-1x100G port license have expired and their granted capacity level & licensed capacity limit are both zero.

The previous router license (ordered for UCC 0.2.2) did not include these capacity keys, yet these ports worked before.

We require your confirmation on the following:

Which capacity key is needed for ports 1/29 to 1/36?

Does UCC 1.0\_CP1 require additional capacity keys for the router?

If this is not a capacity-key issue, what could be the possible cause?

We would appreciate your prompt support in resolving this issue. Please let us know the necessary actions to restore the functionality of these ports.

[Telefonica\\_logs.zip](#)

#### Comments

Comment by [Fredrik Gustavsson](#) [ 2025-02-25 ]

Ok, thanks for the update. I will proceed to close this ticket now.

Comment by [Akshaya Avin Shetty](#) [ 2025-02-25 ]

Hello [Fredrik Gustavsson](#) Now the customer have changed the router. We cannot make any changes now

Comment by [Fredrik Gustavsson](#) [ 2025-02-24 ]

Hi [Akshaya Avin Shetty](#),

To proceed, please respond to one or both of the below:

1. Please install the router configuration exactly as generated by UCC and confirm if you have any issues.
2. To ask the r6k team about any question, please formulate the question you want them to answer. In the meantime, I'll try to locate the Q&A support line.

Thanks

Comment by [Akshaya Avin Shetty](#) [ 2025-02-24 ]

Hello [Fredrik Gustavsson](#)

To bring the ccd-oam interface up customer did some troubleshooting which are the below steps:

- Initially, they changed the CCD-OAM configuration from local to OAM context, but this did not resolve the issue.
- After further investigation, the solution was to redefine the port BVI BVI-CCD-OAM back to local context.
- Then they proceeded with a reconfiguration by applying a shutdown command, followed by a no shutdown command.

We have the issue. Like after graceful shutdown some interfaces are in bound state. It was not the configuration issue. please can you help to raise a ticket towards R6000?

Comment by [Fredrik Gustavsson](#) [ 2025-02-21 ]

To summarize: This issue was found to be caused by a faulty router configuration made by the customer and not a product fault.

Comment by [Akshaya Avin Shetty](#) [ 2025-02-20 ]

[Fredrik Gustavsson](#) as per the customer now issue is resolved. They are able to ping ILO IP and able to login eccd.

- Initially, they changed the CCD-OAM configuration from local to OAM context, but this did not resolve the issue.
- After further investigation, the solution was to redefine the port BVI BVI-CCD-OAM back to local context.
- Then they proceeded with a reconfiguration by applying a shutdown command, followed by a no shutdown command.

After which the in show ip interface brief the ccd-oam interface came up.

```
[oam]router6000(config)#exit
[oam]router6000#context local
[local]router6000#show ip brief
[local]router6000#show ip brief interface
^
% Invalid input at '^' marker

[local]router6000#show ip interface brief
Wed Feb 19 09:28:27 2025
Name          Address          MTU  Stat
ccd-oam       172.16.247.1/28   1500  Boun
ecfe-oam     172.16.247.17/29  1500  Up
[local]router6000#show port bvi bvi-ccd-oam
BVI Port Name      Admin State CCT Name CCT
bvi-ccd-oam        DOWN       bvi-ccd-oam
                                         UP       bvi-ccd-oam
[local]router6000#show port bvi bvi-ccd-oam detail
^
% Invalid input at '^' marker

[local]router6000#configure
Enter configuration commands, one per line, 'end' to e
[local]router6000(config)#port bvi bvi-ccd-oam
[local]router6000(config-port)#no shutdown
[local]router6000(config-port)#commit
Transaction committed.
[local]router6000(config-port)#exit
[local]router6000(config)#exit
[local]router6000#show ip interface brief
Wed Feb 19 09:29:25 2025
Name          Address          MTU  Sta
ccd-oam       172.16.247.1/28   1500  Up
ecfe-oam     172.16.247.17/29  1500  Up
[local]router6000#ping 172.16.247.5
PING 172.16.247.5 (172.16.247.5): source 172.16.247.1
timeout is 1 second
!!!!
----172.16.247.5 PING Statistics----
5 packets transmitted, 5 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 0.380/0.519/0.838/0.1
```



Comment by [Rajan Rajeshprasad Gupta](#) [ 2025-02-18 ]

Hello [Fredrik Gustavsson](#)

Some observation from logs:

Circuit mapping:

Port	Status	OVS/SRIOV	Used for	Before Power off	Status	After Power On
1/29	Up	OVS	UCCA	4a:2d:fd:ff:4a:54 1100 D 1/29:511:63:31/1/2/11 0x00000000	Ok	2a:67:62:e8:19:06 1100 D 1/29:511:63:31/1/2/11
1/30	Up	SRIOV	UCCA			
1/31	Up	OVS	UCCB	7a:17:fc:31:71:c2 1100 D 1/31:511:63:31/1/2/46 0x00000000	Ok	
1/32	Up	SRIOV	UCCB			
1/33	Up	OVS	UCCA			
1/34	Up	SRIOV	UCCA			
1/35	Up	OVS	UCCB			46:6f:b0:eb:c3:24 1100 D 1/35:511:63:31/1/2/116
1/36	Up	SRIOV	UCCB			

1. "Before Power off" both ccda and ccdcb mac address where learned from 1/29 and 1/31 and connection was fine.
2. "After power on" both ccda and ccdcb mac address showing as learned from 1/29 and 1/35 [ switch of NIC]however, we dont see any actual mac address including s
3. "After power on" mac address change is expected as power off/on will result in ecfce pod re-creation and will result in new mac address.

This looks like R6K is unable to handle both NIC and mac address change which causing some function not to behave correctly and causing problem of keeping self-interface

Hello [Akshaya Avin Shetty](#)

Below steps can be tried to understand behavior of R6K

Option1: To shut redundant OVS Port

1. To shut redundant OVS port [ 1/33 and 1/35 ]
2. To save configuration
3. To reload R6K and see behavior

Option2: To shut primary OVS Port

1. To shut redundant OVS port [ 1/29 and 1/31 ]
2. To save configuration
3. To reload R6K and see behavior

To enable debug logs on circuit & Share logs.

!To enable debug on circuit

debug isis circuit detail

logging debug

terminal monitor

!wait for 5-10minutes

!To disable debug on circuit

no debug isis circuit detail

no logging debug

no terminal monitor

!To collect logs and share

show log

Comment by [Rajan Rajeshprasad Gupta](#) [ 2025-02-18 ]

Hello [Fredrik Gustavsson](#)

Will you help to raise ticket to R6000? as we see same behavior of interface going into "Bound" state for each reboot.

It is problem for port 1/29 to 1/36.

ccd\_oam vlan 1100 goes via 1/31 as per logs.

Comment by [Fredrik Gustavsson](#) [ 2025-02-18 ]

Hi again,

in the info provided, the Router started and loaded a config made on Wed Feb 12 13:42:55 UTC 2025

```
Feb 17 11:44:38: %SNMP-6-INFO: MID numPollAttempts:1,serverConfigured:1,numQuerySucceed:1,stop_flag:FALSE,ribQueryRc:4,last_start:0,last_config_change:1739367775
```

It is possible that the iLO configuration changed between the reconfiguration activities performed.

We know that at least one reconfiguration was made after the last save operation and before the reboot activity.

Comment by [Akshaya Avin Shetty](#) [ 2025-02-18 ]

No config changes done [Fredrik Gustavsson](#) .

Comment by [Fredrik Gustavsson](#) [ 2025-02-18 ]

Thanks [Akshaya Avin Shetty](#),

we see that there were some config changes made. Can you please clarify what was done and if that affected the iLO connectivity?

```
diff before/config after/config
6c6
< ! Configuration last changed by user 'mcce' at Thu Feb 13 15:28:52 2025
> ! Configuration last changed by user 'mcce' at Mon Feb 17 12:53:48 2025
```

Comment by [Akshaya Avin Shetty](#) [2025-02-17]

Hello Team,

Today, the customer performed another power-off and power-on cycle. This time, we are facing issues accessing the ILO IP, and the eccd node is unable to SSH from the juniper. While 5G and 4G calls are working fine, we are unable to access OAM.

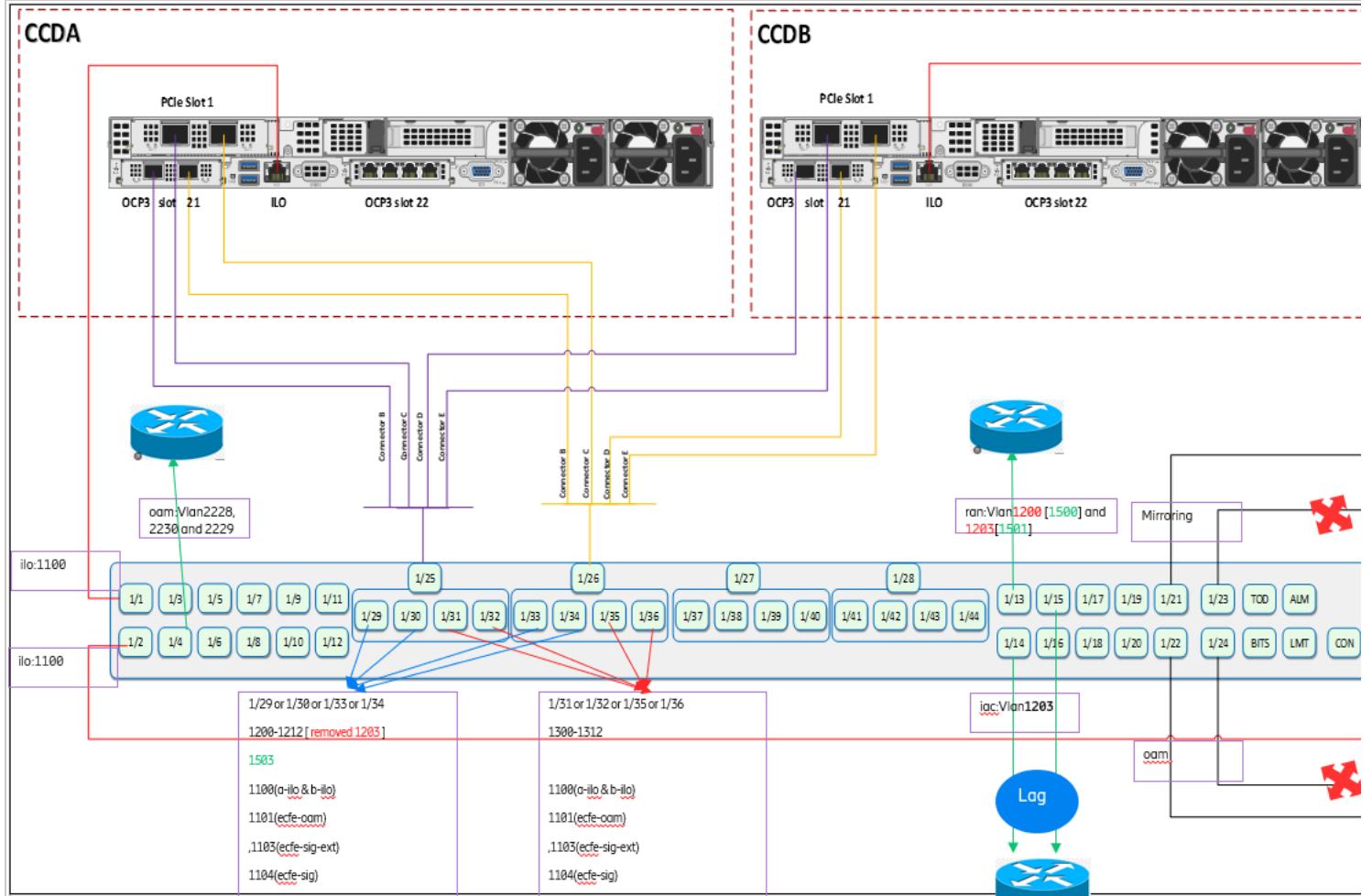
On the router, the ccd-oam interface is in Bound state. All configurations, including the BVI port and bridge settings for ccd-oam, are correct.

Requesting your support in troubleshooting this issue. Please let me know if any additional logs or details are required.

[Router logs after 2nd reboot.zip](#)

[Router logs before 2nd reboot.zip](#)

Comment by [Rajan Rajeshprasad Gupta](#) [2025-02-14]



T100 Router Configuration Design!

Comment by [Fredrik Gustavsson](#) [2025-02-13]

After factory reset of the router and recreation of the config based on the generated UCC config for UCC appliance 1.0.1 plus the specific customer adaptations, traffic for 4G and 5G is still not working. In a few days, the customer will test a new power-off and power-on cycle to verify that the system recovers.

The new config is added [router-config-post-reset.txt](#) and the diff from previous to the new one ([router-config-diff.txt](#)).

Comment by [Akshaya Avin Shetty](#) [2025-02-11]

[Fredrik Gustavsson](#) we have checked the clock both in router as well as in server they are synced.

After checking the clock we proceeded with the graceful shutdown and found the same issue. After that we loaded the licenses still no luck.

In sig,ran,media and iac context some Neighbours are in Bound state.

Checked the bgp status in ECCD all are up. All pods are also up in both eccd.

Logs are attached for reference

Kindly help to resolve it asap

[After reboot logs.zip](#)

[show configuration\\_Feb 11.txt](#)

---

Comment by [Fredrik Gustavsson](#) [2025-02-10]

In the router config we can see "! Configuration last changed by user '<NO USER>' at Thu Jan 1 00:00:00 1970".

This could mean that upon startup, the router had an incorrect date. It might be ok now, but it's worth checking on router and on both servers. (run "show clock" on the router). We can also verify that the server time sync is operational by running "sudo systemctl is-active chronyd.service" and "chronyc -c sourcestats" inside each CCD. If the date was incorrect at startup, it might be worth investigating if a router restart might resolve any issue.

The procedure for this may be found in the Installation Instruction chapter 20: "Graceful Power-off and Power-on".

For the servers, please check that all containers are running. This can be done with the command below, inside each CCD:

```
kubectl get pods --no-headers -A | grep -vE "([0-9]+)\|Completed"
```

---

Comment by [Akshaya Avin Shetty](#) [2025-02-10]

[Fredrik Gustavsson](#) We restarted the router in UCC 0.2.2 all worked fine we didn't had any issue before. After upgrading to UCC 1.0+CP1 this is first time we are restarting the router.

Issue 1: License issue for port 1/29 to 1/36

For which David have already ordered the missing licenses.

As per the customer's show port license output, we observe that licenses are not present for ports 1/29 to 1/36, but all ports are up and not down. Based on this, they suspect that there is a configuration issue with the port settings.

I have checked the routes and did not find any missing entries. Additionally, in ECCD, all BGP sessions are up, but on the router, BGP sessions are down. This inconsistency suggests a configuration issue with the BGP settings.

Could you please help analyze the possible causes and confirm if there are any configuration issues impacting BGP or routing?

Looking forward to your support.

[sig]router6000#show ip interface brief

Fri Feb 7 12:11:05 2025

Name	Address	MTU	State	Bindings
ecfe-sig	172.16.0.1/29	1500	Up	dot1q BVI 2 vlan-id 1104
pcx-sig-a	172.16.0.65/29	1500	Bound	dot1q BVI 5 vlan-id 1200
pcx-sig-b	172.16.1.65/29	1500	Bound	dot1q BVI 11 vlan-id 1300

[local]router6000#

[local]router6000#show port

Slot/Port	Type
1/3	10ge
1/13	10ge
1/14	10ge
1/15	10ge
1/17	10ge
1/21	10ge
1/29	25ge
1/30	25ge
1/31	25ge
1/32	25ge
1/33	25ge
1/34	25ge

1/34	25ge
1/35	25ge
1/36	25ge
Type	Total Tokens
-----	-----
10ge	20
100ge	0
25ge	0
[local]router6000#	

support MobaXterm by subscribing to the p

```
[local]router6000#debug bg  
[local]router6000#debug bg  
[local]router6000#debug bg  
[local]router6000#debug bg  
[local]router6000#debug bg  
[local]router6000#terminal m  
[local]router6000#context  
[sig]router6000#debug bgp  
[sig]router6000#terminal m  
[sig]router6000#Feb 10 08:  
Feb 10 08:46:09: [0003]: %  
Feb 10 08:46:09: [0003]: %  
Feb 10 08:46:24: [0003]: %  
Feb 10 08:46:24: [0003]: %  
Feb 10 08:46:24: [0003]: %
```



support MobaXterm by subscribing to the pro



### [Routers\\_Output.txt](#)

Comment by [Fredrik Gustavsson](#) [ 2025-02-10 ]

Early analysis has shown that the 100g port is unlicensed and therefore the 4x25g subports are not possible to use.

One question is why the missing license was not identified earlier? Was the router never restarted?

The recommendation is to acquire and install the missing license ASAP.

Comment by [David Heras Cano](#) [ 2025-02-10 ]

Here is the timeline:

6<sup>th</sup> Feb

- Finishing all CNF deployment & Integration. 4G & 5G attach test completed. 4G & 5G pdp context test completed.
- Customer shuts down UCC (Server first & Router last)

7<sup>th</sup> Feb

- Customer powers up UCC (Router first & servers last)
- Customer states alarms appearing (see attached)
- Investigation reveals that some BGP sessions are not being established

<a href="#">[UCC_PLM-192] Mismatch in NTP server IP provided</a>	
Created: 2025-02-05 Updated: 2025-02-07 Resolved: 2025-02-07	
<b>Status:</b>	Rejected
<b>Project:</b>	<a href="#">UCC_PLM</a>
<b>Component/s:</b>	None
<b>Affects Version/s:</b>	<a href="#">UCC Appliance 1.0.1</a>
<b>Fix Version/s:</b>	None

<b>Type:</b>	Bug	<b>Priority:</b>	Medium
<b>Reporter:</b>	<a href="#">Akshaya Avin Shetty</a>	<b>Assignee:</b>	Unassigned
<b>Resolution:</b>	Rejected	<b>Votes:</b>	0
<b>Labels:</b>	None		
<b>Remaining Estimate:</b>	Not Specified		
<b>Time Spent:</b>	Not Specified		
<b>Original Estimate:</b>	Not Specified		

<b>Defect code_qmt:</b>	1- Functional
<b>Detected in phase:</b>	Staging
<b>Team/s:</b>	<a href="#">UCC_PLM</a>
<b>Severity_qmt:</b>	3- Medium
<b>Found in Build:</b>	<a href="#">UCC Appliance 1.0.1</a>
<b>Requirement Status:</b>	<a href="#">UCC Appliance 0.2.1 - UNCOVERED</a>

#### Description

NTP configured on router was 172.18.234.1 as per the previous release which was provide in LLD. We generated the config using NTP IP 172.18.234.1. But CCD installation started failing with error scp: /home/eccd/.kube/config: No such file or directory.
We observed that in Router and CCD time was not synchronized. So new NTP IP was provided 172.16.50.21. After synchronization CCD installation was successful

#### Comments

Comment by <a href="#">Ahmed Elkhouly</a> [ 2025-02-07 ]
Thanks <a href="#">Eric Fenger</a> and <a href="#">Fredrik Gustavsson</a> . Wrong NTP IP was provided by CU. No further action is needed.
Comment by <a href="#">Fredrik Gustavsson</a> [ 2025-02-07 ]
Thanks <a href="#">Eric Fenger</a> and <a href="#">Akshaya Avin Shetty</a> , according to my understanding, and the lack of further clarity from the source, this problem occurred due to incorrect values in the LLD, that was manually patched later, without rerunning the full installation.
I will reject this issue.
Please reopen if further information is found regarding the background of this.
Comment by <a href="#">Eric Fenger</a> [ 2025-02-07 ]
Hi <a href="#">Fredrik Gustavsson</a> ,
do you say there is a mismatch between CCD configuration and R6K configuration for NTP? This ticket should go to IP team to evaluate the issue. I do not know the details on this level. If there is misconfiguration caused by LLD, then this sounds more like a bug.
Comment by <a href="#">Fredrik Gustavsson</a> [ 2025-02-05 ]
<a href="#">Eric Fenger</a> , I don't know if you can bring more clarity for this issue.
To my understanding of this ticket:
1. The system was installed with UCC Appliance 1.0.0
2. The external NTP server changed IP address
3. The UCC Appliance 1.0.1 LLD was updated using the old NTP IP (step #1)
4. The UCC Appliance 1.0.1 installation failed at the CCD step
5. There was a manual correction of the NTP server IP configuration (to step #2 IP) in the router but the full installation was not restarted (regeneration of config from LLD, router update, CCD re-installation ...)

The UCC Appliance 1.0.1 LLD has two fields for external NTP IP. Both require an IP address (I assume this means "fixed IP") and not an FQDN (I assume this would be "not fixed IP")

However, if the change is not done in the LLD and the configs are not regenerated, then we will only have the update according to the manual setting. This is not according to the installation instruction, and I don't see any indication of a product fault in this case.

There could be another use-case, not to be handled as a PLM ticket but as a Feature Request, to allow for post-installation change of NTP server IP address.

Comment by [Akshaya Avin Shetty](#) [ 2025-02-05 ]

Issue is customer didn't gave the updated NTP sever IP. After updating the new NTP server Ip which is reachable from Router The issue is resolved

CCD is successfully installed in both CCD, Issue is resolved.

Ahmed have asked to raise the ticket so that we need to set the LLD to have a fixed NTP IP to avoid IP mismatch in every upgrade.

Comment by [Fredrik Gustavsson](#) [ 2025-02-05 ]

[Akshaya Avin Shetty](#), to understand the issue, please confirm the following:

1. Confirm that the UCC Appliance 1.0.1 router config was applied
2. Confirm that the LLD, for the UCC Appliance 1.0.1 installation, was prepared with the correct information, including the correct external NTP server address

Comment by [Akshaya Avin Shetty](#) [ 2025-02-05 ]

NTP server was not reachable from router. So they gave new NTP IP which is reachable from router

Comment by [Fredrik Gustavsson](#) [ 2025-02-05 ]

Was the installation instruction followed for the UCC Appliance 1.0.1 release, including applying the regenerated router configuration? If so, do we see a difference between the router config NTP and the CCD configuration for NTP?

#### [UCC\_PLM-191] CNAT log file naming improvement Created: 2025-01-22 Updated: 2025-02-10 Resolved: 2025-02-10

Status:	Resolved
Project:	UCC_PLM
Component/s:	None
Affects Version/s:	None
Fix Version/s:	None

Type:	Task	Priority:	Low
Reporter:	Zhigang Han	Assignee:	Unassigned
Resolution:	Resolved	Votes:	0
Labels:	None		
Remaining Estimate:	Not Specified		
Time Spent:	Not Specified		
Original Estimate:	Not Specified		

Team/s:	UCC_XFT3
---------	----------

#### Description

Hi team,

CNAT log file naming is a bit unclear for us. For example, we have this log name "CNAT\_uninstall\_20250122133523.log" but it is not clear for us what CNAT script is doing. Could we add "ccd cluster name" and "cnf namespace" in the CNAT log file naming?

Thanks,

BR/Zhigang

#### Comments

Comment by [Soner Mus](#) [ 2025-02-10 ]

included in the latest CNAT, also merged to the development branch as of now.

Thanks

Comment by [Soner Mus](#) [ 2025-02-06 ]

Change included in Development Branch and released internally with [7b081ff9](#) version. UCC 1.1 release will have the improvement.

Comment by [Sherif Farag F](#) [ 2025-01-23 ]

Hello,

I have updated the code and tested to include the namespace in the log filename,

Please let me know if that is what you requested,

## namespace:

```
(cnat_env) stcucc2@ucc-jumphost:~/dev-soldev/config/ccda/hss_validator$ python3 ~/cnat1-10-2/ucc-cnat/src/cnat.py -k ccda -i -ng
_____
/ ___\ \ \ \ \ \
/ / \ \ \ \ \ \ \
\_\_/_ / / \_, \_\_Cloud Native Deployment Automation Tool2025/01/23 00:48:58 INFO: Saving debug logs to file:
/home/stcucc2/cnat_log/CNAT_install_ed4_20250123004858.log
2025/01/23 00:48:58 INFO: CNAT Version: $CNAT_VERSION
2025/01/23 00:48:58 INFO: CNAT env: /home/stcucc2/.cnat_env.yaml
```

namespace + clustername:

Br, Sherif//

[UCC_PLM-190] MELA: CCRC DNS Configuration and Verification Steps are mis-aligned in II				Created: 2025-01-20 Updated: 2025-03-10 Resolved: 2025-03-10					
Status:	Rejected								
Project:	UCC_PLM								
Component/s:	None								
Affects Version/s:	UCC Appliance 1.0.1								
Fix Version/s:	None								
Type:	Bug	Priority:	Low						
Reporter:	Rajan Rajeshprasad Gupta	Assignee:	Alvaro Martin						
Resolution:	Rejected	Votes:	0						
Labels:	None								
Remaining Estimate:	Not Specified								
Time Spent:	Not Specified								
Original Estimate:	Not Specified								
Attachments:									
Defect code_qmt:	3- Usability								
Detected in phase:	Staging								
Team/s:	UCC_XFT2								
Severity_qmt:	4-Low/Cosmetic								
Found in Build:	UCC Appliance 1.0.1								
Requirement Status:	UCC Appliance 0.2.1 - UNCOVERED								

## Description

Hello

In the doc. step 12.4 contains geored sync and 12.5 is CCBC DNS config

This is incorrect order, as without DNS configuration, ccrc geo-red sync will never happen.

**10. Execute the steps in chapter "15.2.2 Synchronize Data Between Sites".**

**11. Configure DNS according to chapter 12.5 CCRC DNS Configuration**

Please correct order of installation guide so first time UCC Installer can follow and install UCC without any confusion.

**Comments**

Comment by Alvaro Martin [ 2025-03-10 ]

The order is correct. It has to be executed in that specific order.

After deploying second CCRC, first thing to do is to "Synchronize Data Between Sites" in order to ensure the replication channel is established and updates in any site are replicated on the other. Then when that's achieved, the DNS config in the second site can be applied, and then it will be reflected in site 1.

This order was defined like this after some issues found out with the replication.

**[UCC\_PLM-189] Failed to populate registry with EDA images** Created: 2025-01-16 Updated: 2025-04-23 Resolved: 2025-04-23

<b>Status:</b>	Done
<b>Project:</b>	UCC_PLM
<b>Component/s:</b>	None
<b>Affects Version/s:</b>	UCC Appliance 1.0.1
<b>Fix Version/s:</b>	None

<b>Type:</b>	Bug	<b>Priority:</b>	Medium
<b>Reporter:</b>	Fredrik Gustavsson	<b>Assignee:</b>	Unassigned
<b>Resolution:</b>	Closed	<b>Votes:</b>	0
<b>Labels:</b>	Expericom		
<b>Remaining Estimate:</b>	Not Specified		
<b>Time Spent:</b>	Not Specified		
<b>Original Estimate:</b>	Not Specified		

<b>Attachments:</b>	<a href="#">CMD Logs.txt</a>	<a href="#">CNAT_batch_install_20250114113215.log</a>
<b>Defect code_qmt:</b>	1- Functional	
<b>Detected in phase:</b>	Production	
<b>Team/s:</b>	UCC_XFT2	
<b>Severity_qmt:</b>	3- Medium	
<b>Found in Build:</b>	UCC Appliance 1.0.1	
<b>Requirement Status:</b>	UCC Appliance 0.2.1 - UNCOVERED	

**Description**

This was experienced during an installation of UCC Appliance 1.0.1 at ExperiCom.

```
ucc@ns113-ucc-ks:~/data/config/ccda/batch$ cnat -k ccda -bi \
$config_dir/config/ccda/batch/vnf-images-onboard.yaml
...
2025/01/14 11:32:16 INFO [MainProcess]: Loading info for all CNFs
2025/01/14 11:32:16 INFO [MainProcess]: VNF info file: /home/ucc/data/config/ccda/eda/vnf-images-eda.yaml
2025/01/14 11:32:16 ERROR [MainProcess]: Traceback (most recent call last):
  File "vnf/vnf.py", line 142, in _load_vnf_info
    self.csar = Csar(self.info['vnflcm'][['csar-file']])
    ^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^
  File "vnflcm/csar.py", line 26, in __init__
    self._init_vnf_node_type_and_template()
  File "vnflcm/csar.py", line 44, in _init_vnf_node_type_and_template
    for node_type_id, node_type in self.vnfd["node_types"].items():
    ^^^^^^
TypeError: string indices must be integers, not 'str' During handling of the above exception, another exception occurred:Traceback (most recent call last):
  File "cnat.py", line 59, in <module>
  File "vnflcm/install.py", line 183, in batch_install
    vnf = Vnf(new_config)
    ^^^^^^
  File "vnf/vnf.py", line 39, in __init__
    self._load_vnf_info()
  File "vnf/vnf.py", line 155, in _load_vnf_info
    raise Exception(f"Failed to load VNF info.
```

## Comments

Comment by [Meryam Nachi](#) [ 2025-02-21 ]

Those steps are not needed anymore with UCA 1.2 which will be released in UCC 1.1

Comment by [Fredrik Gustavsson](#) [ 2025-01-17 ]

This is coming from an error in the installation instruction where an absolute path is used when injecting the TOSCA.yaml into the UCA csar file.

The current Installation Instruction, Rev "", 2024-09-06, Chapter 12.1, bullet 4, reads:

```
4. Add TOSCA.yaml file to the csar
zip -g $software_dir/EDA/eric-act-uca-1.63.128.csar \
$software_dir/EDA/Definitions/TOSCA.yaml
```

This will not replace the "Definitions/TOSCA.yaml" file but add another file "home/ucc/software/EDA/Definitions/TOSCA.yaml" (with \$software\_dir=/home/ucc/software).

One way to resolve this is to follow the steps:

```
cd $software_dir/EDA
zip -g $software_dir/EDA/eric-act-uca-1.63.128.csar Definitions/TOSCA.yaml
```

Please update the Installation Instruction to resolve this issue.

Comment by [Fredrik Gustavsson](#) [ 2025-01-16 ]

After confirming with [Marco de Rouw](#), the CNAT error comes from that the parser cannot find node\_types in TOSCA.yaml from the csar file.

We proceeded to unpack and check the contents of the csar and got this:

```
ucc@ns113-ucc-ks:~/data/software/EDA/tmp$ more Definitions/TOSCA.yaml
template base file
ucc@ns113-ucc-ks:~/data/software/EDA/tmp$ more home/ucc/data/software/EDA/Definitions/TOSCA.yaml
#template base file
node_types:
Ericsson.EDA.1.63.128-6.CSH109706_R19A_2.18.0:
  derived_from: tosca.nodes.nfv.VNF
  properties:
    descriptor_id:
      type: string
...
...
```

This indicates a packaging error of the csar and we asked the customer to verify that the steps had been followed.

## [UCC\_PLM-188] MANA: Multiple defaultDnnIndicator in UDM Profile

Created: 2025-01-15 Updated: 2025-01-17 Resolved: 2025-01-17

Status:	Rejected
Project:	<a href="#">UCC_PLM</a>
Component/s:	None
Affects Version/s:	None
Fix Version/s:	None

Type:	Bug	Priority:	Medium
Reporter:	<a href="#">Rajan Rajeshprasad Gupta</a>	Assignee:	<a href="#">Fredrik Gustavsson</a>
Resolution:	Rejected	Votes:	0
Labels:	None		
Remaining Estimate:	Not Specified		
Time Spent:	Not Specified		
Original Estimate:	Not Specified		

Attachments:			
Found in Build:	1.0.1		
Requirement Status:	UCC Appliance 0.2.1 - UNCOVERED		

## Description

Hello,  
Ideally one DNN should be defaultDnnIndicator in UDM profile. However, I notice, UDM allows to configure multiple DNN as defaultDnnIndicator.  
Also I see UDM send multiple DNN with defaultDnnIndicator based on provisioning.

Question1: Why we have so many defaultDnnIndicator in eda templates? Is it required?

Question2: We have only 2 DNNs in LLD, "internet" and "iot". Why do we have unwanted DNN in eda templates?

See normal behavior documented in CPI:

Can we have more than one APN with defaultDnnIndicator

No, only one APN can have `defaultDnnIndicator` set to true at a time **4**.

1. IMS IMPU Object    2. EPS Static Information ...    3. Configuration of RAs, R...    4. Business Logic  
5. EPS Static Information ...    more...

See UDM sending multiple DNN with defaultDnnIndicator, send by UDM to AMF. Attached PCAP.

No.	Time	ID	Source	Destination	Protocol	AVP	Result	Fran	HI (Hand)	5GS	RAT	F-TI	Origin-R	Orig	Dest	Type
31	2025-01-14 22:55:08.043000		172.16.2.1	172.16.2.71	HTTP2											
32	2025-01-14 22:55:08.065000		172.16.2.71	172.16.2.1	HTTP2/JSON											

Object

  Member: dnnInfos

    Array

      Object

        Member: dnn

          [Path with value: /subscribedSnssaiInfos/1-000001/dnnInfos/[]/dnn:ims]

          [Member with value: **dnn:ims**]

          String value: ims

          Key: dnn

          [Path: /subscribedSnssaiInfos/1-000001/dnnInfos/[]/dnn]

        Member: defaultDnnIndicator

          [Path with value: /subscribedSnssaiInfos/1-000001/dnnInfos/[]/defaultDnnIndicator:true]

          [Member with value: **defaultDnnIndicator:true**]

          True value

          Key: defaultDnnIndicator

          [Path: /subscribedSnssaiInfos/1-000001/dnnInfos/[]/defaultDnnIndicator]

        Member: lboRoamingAllowed

        Member: iwkEpsInd

      Object

        Member: dnn

          [Path with value: /subscribedSnssaiInfos/1-000001/dnnInfos/[]/dnn:internet]

          [Member with value: **dnn:internet**]

          String value: internet

          Key: dnn

          [Path: /subscribedSnssaiInfos/1-000001/dnnInfos/[]/dnn]

        Member: defaultDnnIndicator

          [Path with value: /subscribedSnssaiInfos/1-000001/dnnInfos/[]/defaultDnnIndicator:true]

          [Member with value: **defaultDnnIndicator:true**]

          True value

          Key: defaultDnnIndicator

          [Path: /subscribedSnssaiInfos/1-000001/dnnInfos/[]/defaultDnnIndicator]

        Member: lboRoamingAllowed

        Member: iwkEpsInd

      Object

        Member: dnn

          [Path with value: /subscribedSnssaiInfos/1-000001/dnnInfos/[]/dnn:VZWINTERNET]

          [Member with value: **dnn:VZWINTERNET**]

          String value: VZWINTERNET

          Key: dnn

          [Path: /subscribedSnssaiInfos/1-000001/dnnInfos/[]/dnn]

        Member: defaultDnnIndicator

          [Path with value: /subscribedSnssaiInfos/1-000001/dnnInfos/[]/defaultDnnIndicator:true]

          [Member with value: **defaultDnnIndicator:true**]

          True value

          Key: defaultDnnIndicator

Question3: Is this normal? What is use-case of so many dnn with defaultDnnIndicator

Above questions comes from vz customer.

vz has use-case, where users handset will not have any dnn configured and amf will use udm profile to filter out defaultDnnIndication and select defaultDnn for PDUsession

So it is required to understand reason and correct default template of eda which reflect use-case of UCC.

#### Comments

Comment by [Fredrik Gustavsson](#) [ 2025-01-17 ]

Hi, for improvements, please open a Feature Request according to this instruction: [UCC Feature Request Process](#) and it will be analyzed by the correct team. For the PLM ticket, I will proceed to close this one.

#### [UCC\_PLM-187] MANA: Testing expiry of ADP internal certs Created: 2025-01-15 Updated: 2025-01-17 Resolved: 2025-01-17

Status:	Rejected
Project:	<a href="#">UCC_PLM</a>
Component/s:	None
Affects Version/s:	None
Fix Version/s:	None

Type:	Bug	Priority:	Medium
Reporter:	<a href="#">Rajan Rajeshprasad Gupta</a>	Assignee:	<a href="#">Fredrik Gustavsson</a>
Resolution:	Rejected	Votes:	0
Labels:	None		
Remaining Estimate:	Not Specified		
Time Spent:	Not Specified		
Original Estimate:	Not Specified		

Attachments:	
Team/s:	<a href="#">UCC_PLM</a>
Found in Build:	UCC 1.0.1
Requirement Status:	UCC Appliance 0.2.1 - UNCOVERED

#### Description

Hello,

Raytheon UCC is "power off" @ 23<sup>rd</sup> Dec 2024 and Power on @7<sup>th</sup> Jan 2025 [ This is done by Customer to save power during New year holidays ]

We have not seen any issue with 5G SA Calls as number of days system is powered off >7 days.

Similarly,

We have vz ucc powered on after >30 days.

I see similar behavior with vz ucc, After power on, sip-tls pods were restarted few times before it become stable.

We tested 1<sup>st</sup> 5g sa registration and it works fine [ not sure on impact on sip-tls certificate expiry in detail, basic understanding internal communication will fail ]

See logs as below:

```
eccd@ucc-ccda:~> kubectl get pod -A | grep sip-tls
```

ccdm	eric-sec-sip-tls-main-7b965cbff8-46rb	2/2	Running	8 (4d19h ago)	48d
ccrc	eric-sec-sip-tls-main-6dbbf86d58-g8cnt	2/2	Running	8 (4d19h ago)	50d
ccsm	eric-sec-sip-tls-main-76d94d4b5c-2nchq	2/2	Running	8 (4d19h ago)	48d
cnom	eric-sec-sip-tls-main-766496558c-jkxjk	3/3	Running	12 (4d19h ago)	48d
cnom	eric-sec-sip-tls-main-766496558c-wqzsp	3/3	Running	12 (4d19h ago)	48d
eda	eric-sec-sip-tls-main-86cd67d77d-627sc	3/3	Running	12 (4d19h ago)	48d
ep5g	eric-sec-sip-tls-main-559768cb6f-6r8w4	2/2	Running	8 (4d19h ago)	49d
kube-system	eric-sec-sip-tls-main-564f7cf59d-9c2cn	2/2	Running	10 (4d19h ago)	52d

```
monitoring      eric-sec-sip-tls-main-67fdb6848f-sq7cs          2/2    Running   10 (4d19h ago)  52d

eccd@ucc-ccda:~> kubectl logs eric-sec-sip-tls-main-564f7cf59d-9c2cn -n kube-system | grep "renewal will happen"
Defaulted container "sip-tls" out of: sip-tls, sip-tls-supervisor
{"version": "1.2.0", "timestamp": "2025-01-09T18:05:41.165Z", "severity": "info", "service_id": "eric-sec-sip-tls", "metadata": {"pod_name": "eric-sec-sip-tls-main-564f7cf59d-9", "namespace": "kube-system"}}

, "message": "[Thread-2] manager_base.py:125 Certificate expires at 2025-01-16 18:05:41.165193 UTC, renewal will happen in advance at 2025-01-15 12:07:46.165193 UTC fc secret"}
{"version": "1.2.0", "timestamp": "2025-01-09T18:06:17.490Z", "severity": "info", "service_id": "eric-sec-sip-tls", "metadata": {"pod_name": "eric-sec-sip-tls-main-564f7cf59d-9", "namespace": "kube-system"}}

, "message": "[Thread-2] manager_base.py:125 Certificate expires at 2025-01-10 18:06:17.490739 UTC, renewal will happen in advance at 2025-01-10 15:25:23.490739 UTC fc cert"}
{"version": "1.2.0", "timestamp": "2025-01-09T18:06:17.526Z", "severity": "info", "service_id": "eric-sec-sip-tls", "metadata": {"pod_name": "eric-sec-sip-tls-main-564f7cf59d-9", "namespace": "kube-system"}}

, "message": "[Thread-2] manager_base.py:125 Certificate expires at 2025-01-10 18:06:17.526325 UTC, renewal will happen in advance at 2025-01-10 13:48:44.526325 UTC fc"
{"version": "1.2.0", "timestamp": "2025-01-09T18:06:17.557Z", "severity": "info", "service_id": "eric-sec-sip-tls", "metadata": {"pod_name": "eric-sec-sip-tls-main-564f7cf59d-9", "namespace": "kube-system"}}

, "message": "[Thread-2] manager_base.py:125 Certificate expires at 2025-01-16 18:06:17.557692 UTC, renewal will happen in advance at 2025-01-16 00:17:41.557692 UTC fc
eccd@ucc-ccda:~>
```

I have collected more detailed ADP logs to dig SIP-TLS behavior for kube-system and ep5g namespace.

#### vz-sip-tls-adp

This time, I took adp sip-tls script to understand bit more about certificate renewal and expiry within different network function.

Eg.

**kube-system** name space. I do see some of the certificate are expired or not found.

**ccsm** namespace. No certificate is expired.

**ep5g** namespace. No certificate is expired.

**ccdm** namespace. No certificate is expired.

**cnom** namespace. No certificate is expired.

**ccrc** namespace . I do see some of the certificate are expired or not found.

**eda** namespace. I do see some of the certificate are expired

attached log. Ticket is raised handshake with ADP team to understand this expired certificate and impact of it.

## Comments

Comment by Fredrik Gustavsson [ 2025-01-17 ]

Hi Rajan Rajeshprasad Gupta, you stated that the system came up after power-on and that the pods restarted a few times until it became stable. Please monitor the system for instability and if found, raise a ticket for this.

As a PLM organization, we can only investigate bugs, but the larger organization may initiate studies or altering the product via a Feature Request.

Comment by Rajan Rajeshprasad Gupta [ 2025-01-17 ]

Hello Fredrik Gustavsson

What you do mean by working as expected?

Ticket is raised to understand expected behavior from ADP. are we supported to see expired cert

"Ticket is raised handshake with ADP team to understand this expired c

JOURNAL OF CLIMATE

Comment by Fredrik Gustavsson [ 2025-01-17 ]

Since the system seems to be working as intended, I don't see this as a bug.

For improvements, please open a Feature Request

For the PLM ticket, I will proceed to close this one.

Comment by Rajan Rajeshprasad Gupta [2025-01-15] | SID: T1G-2023-00001 | Page 1 of 1

### Comments about the model's behavior

ccdm eric-sec-sip-tls-main-7b965chff8-46rbh

ccrc eric-sec-sip-tls-main-6dbbf86d58-g8cnt

ccsm eric-sec-sip-tls-main-76d94d4b5c-2nchq

eric-sec-sip-tls-main-766496558c-jkxjk  
eric-sec-sip-tls-main-766496558c-jkxjk

eric-sec-sip-tls-main-760490338c-wqzsp  
eric-sec-sip-tls-main-86cd67d77d-637ec

ep5q eric-sec-sip-tls-main-559768cb6f-6r8w4

kube-system eric-sec-sip-tls-main-564f7cf59d-9c2e

monitoring eric-sec-sip-tls-main-67fdb6848f-sq7c

```
eccc@ucc-ccda:~> kubectl describe pod eric-sec-sip-t
```

Labels: app=eric-sec-sip-tls

app.kubernetes.io/instance=eric-ccdm-3

app.kubernetes.io/name=eric-sec-sip-tls

app.kubernetes.io/version=9.0.0\_23

```

eccd@ucc-ccda:~> kubectl describe pod eric-sec-sip-tls-main-6dbbf86d58-g8cnt -n ccrc | grep -i app
Labels:      app=eric-sec-sip-tls
              app.kubernetes.io/instance=eric-ccrc-2
              app.kubernetes.io/name=eric-sec-sip-tls
              app.kubernetes.io/version=7.3.0_35
eccd@ucc-ccda:~> kubectl describe pod eric-sec-sip-tls-main-76d94d4b5c-2nchq -n ccsm | grep -i app
Labels:      app=eric-sec-sip-tls
              app.kubernetes.io/instance=eric-ccsm-3
              app.kubernetes.io/name=eric-sec-sip-tls
              app.kubernetes.io/version=11.0.0_29
eccd@ucc-ccda:~> kubectl describe pod eric-sec-sip-tls-main-766496558c-jkxjk -n cnom | grep -i app
Labels:      app=eric-sec-sip-tls
              app.kubernetes.io/instance=eric-cnom
              app.kubernetes.io/name=eric-sec-sip-tls
              app.kubernetes.io/version=7.3.0_35
eccd@ucc-ccda:~> kubectl describe pod eric-sec-sip-tls-main-766496558c-wqzsp -n cnom | grep -i app
Labels:      app=eric-sec-sip-tls
              app.kubernetes.io/instance=eric-cnom
              app.kubernetes.io/name=eric-sec-sip-tls
              app.kubernetes.io/version=7.3.0_35
eccd@ucc-ccda:~> kubectl describe pod eric-sec-sip-tls-main-86cd67d77d-627sc -n eda | grep -i app
Labels:      app=eric-sec-sip-tls
              app.kubernetes.io/instance=eric-eda
              app.kubernetes.io/name=eric-sec-sip-tls
              app.kubernetes.io/version=11.0.0_29
              container.apparmor.security.beta.kubernetes.io/logshipper: runtime/default
              container.apparmor.security.beta.kubernetes.io/sip-tls: runtime/default
              container.apparmor.security.beta.kubernetes.io/sip-tls-supervisor: runtime/default
Topology Spread Constraints: kubernetes.io/hostname:ScheduleAnyway when max skew 1 is exceeded for selector app.kubernetes.io/instance=eric-eda,app.kubernetes.io/name=eric-sec-sip-tls
eccd@ucc-ccda:~> kubectl describe pod eric-sec-sip-tls-main-559768cb6f-6r8w4 -n ep5g | grep -i app
Labels:      app=eric-sec-sip-tls
              app.kubernetes.io/instance=eric-pc-controller
              app.kubernetes.io/name=eric-sec-sip-tls
              app.kubernetes.io/version=10.1.0_23
eccd@ucc-ccda:~> kubectl describe pod eric-sec-sip-tls-main-564f7cf59d-9c2cn -n kube-system | grep -i app
Labels:      app=eric-sec-sip-tls
              app.kubernetes.io/instance=eric-sec-sip-tls
              app.kubernetes.io/name=eric-sec-sip-tls
              app.kubernetes.io/version=10.2.0_15
              container.apparmor.security.beta.kubernetes.io/sip-tls: runtime/default
              container.apparmor.security.beta.kubernetes.io/sip-tls-supervisor: runtime/default
eccd@ucc-ccda:~> kubectl describe pod eric-sec-sip-tls-main-67fdb6848f-sq7cs -n monitoring | grep -i app
Labels:      app=eric-sec-sip-tls
              app.kubernetes.io/instance=eric-sec-sip-tls
              app.kubernetes.io/name=eric-sec-sip-tls
              app.kubernetes.io/version=10.2.0_15
              container.apparmor.security.beta.kubernetes.io/sip-tls: runtime/default
              container.apparmor.security.beta.kubernetes.io/sip-tls-supervisor: runtime/default
eccd@ucc-ccda:~> date
Wed 15 Jan 2025 02:46:27 PM EST
eccd@ucc-ccda:~>
```

[\[UCC\\_PLM-245\] MANA: UCC servers power on bios setting](#) Created: 2025-01-15 Updated: 2025-07-14 Resolved: 2025-06-03

<b>Status:</b>	Done
<b>Project:</b>	UCC_PLM
<b>Component/s:</b>	None
<b>Affects Version/s:</b>	UCC Appliance 1.0.1
<b>Fix Version/s:</b>	None

<b>Type:</b>	Bug	<b>Priority:</b>	Medium
<b>Reporter:</b>	Rajan Rajeshprasad Gupta	<b>Assignee:</b>	Alexander Malikov
<b>Resolution:</b>	Closed	<b>Votes:</b>	0

<b>Labels:</b>	UCC_Appliance_1.2.0
<b>Remaining Estimate:</b>	Not Specified
<b>Time Spent:</b>	Not Specified
<b>Original Estimate:</b>	Not Specified

<b>Attachments:</b>	
<b>Defect code_qmt:</b>	1- Functional
<b>Detected in phase:</b>	Production
<b>Team/s:</b>	UCC_XFT2
<b>Severity_qmt:</b>	3- Medium
<b>Found in Build:</b>	UCC Appliance 1.0.1
<b>Requirement Status:</b>	UCC Appliance 0.2.1 - UNCOVERED

#### Description

Hello,

When powering UCC servers after shipping, we see 2 behaviors:

- Raytheon: servers came up automatically
- Verizon: servers did not come up automatically – we have to manually power on

We assume this behavior is how the servers came setup in BIOS(See Print screen).

Nowhere UCC installation document or any document in UCC gives information what should be servers power on bios setting.

Question1: Do we have any standard setting for all UCC servers?

Question2: Can we document clearly in installation guide/ verification by CNAT?

#### Note:

1. HP servers coming from factory can have different servers power on bios setting which will result in undesired behavior by our customers.
2. Power on / Power off is regular activity for UCC Customers.

See screen print which we identified for such different behavior.

[Server Power](#)   [Power Meter](#)   [Power Settings](#)   [Power](#)   [Fans & Cooling Modules](#)   [Temperatures](#)

## Virtual Power Button

System Power:	ON
Graceful Power Off:	Momentary Press
Force Power Off:	Press and Hold
Force Power Cycle:	Cold Boot
Force System Reset:	Reset

## System Power Restore Settings

**Auto Power-On**

Always Power On

Always Remain Off

Restore Last Power State

**Power-On Delay**

Minimum Delay

15 Second Delay

30 Second Delay

45 Second Delay

60 Second Delay

Random up to 120 Seconds

**Apply**

### Comments

Comment by [Rajan Rajeshprasad Gupta](#) [ 2025-07-14 ]

Hello team,

As a work-around : A manual checkpoint has been added to the installation guide, which should be followed before powering off the UCC server in the new installation guide settings.

AutoSave On ⏴ ⏵ ⏵ ⏵ Ericsson Ultra Compact Core - Appliance - Software Installation Guide - new.docx

File Home Templafy Insert Draw Design Layout References Mailings Review View Help

Templafy Ericsson Hilda 11

Paste Clipboard

Font Paragraph Styles Editing Dictation

Navigation nano Search paused

Headings Pages Results

19 IoT Adaptation

20 MCPTT Feature Activation

▲ 21 Cleanup of UCC

    21.1 Uninstalling the CNFs

    21.2 Manual Cleanup of UCC CNFs

▲ 22 Graceful Power-off and Power-on

    22.1 Preparations Before Graceful Shutdown

    ▲ 22.2 Graceful Shutdown and Startup Procedure

        22.2.1 Power Off the Servers

        22.2.2 Power Off the Router

        22.2.3 Power On the Router

        22.2.4 Power On the Servers

    22.3 Health Check after Startup

    22.4 Apply Workaround for Known Issues

▲ 23 Known Issues

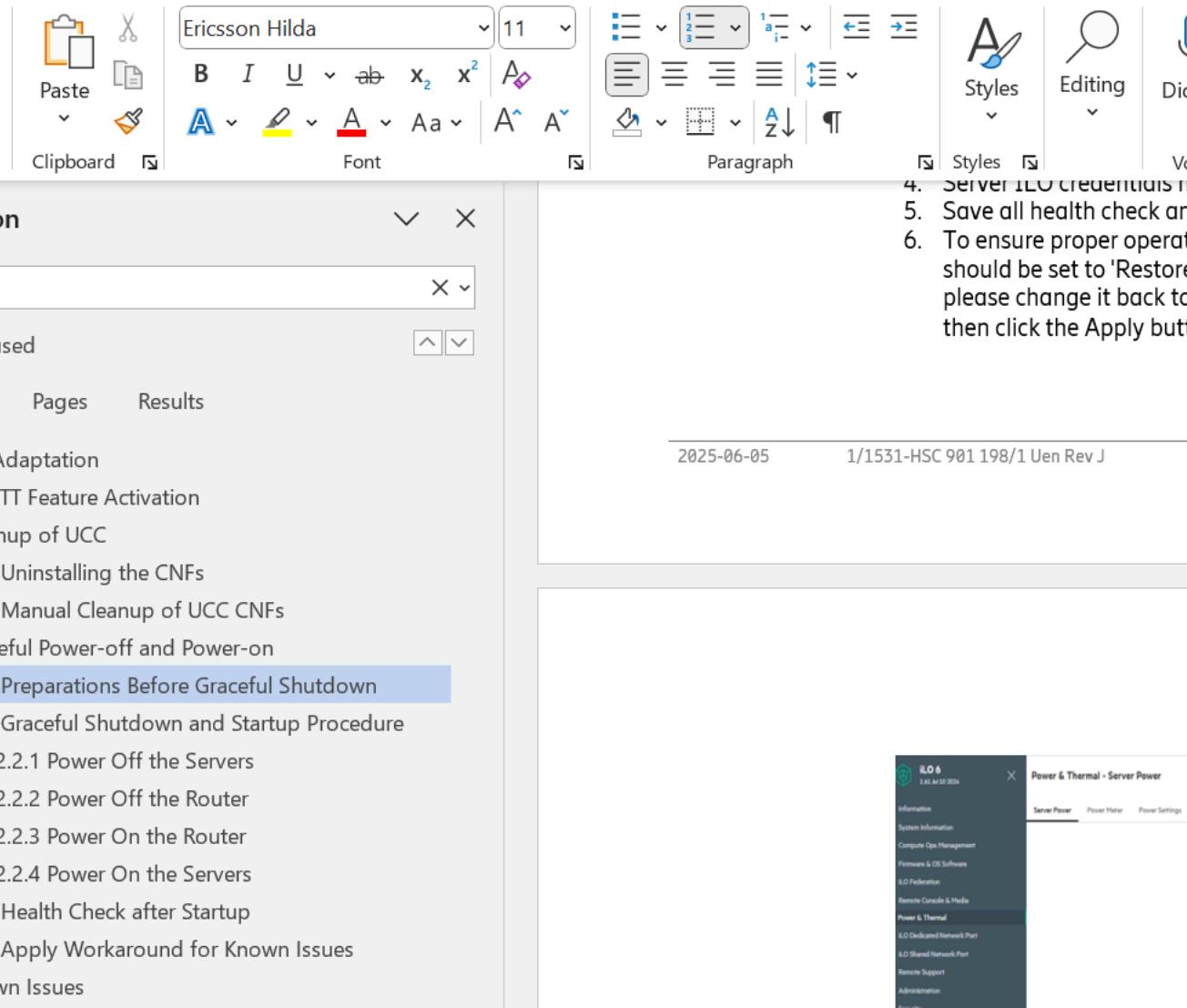
    23.1 Issue 1 – Residual DataPlane Not Cleaned

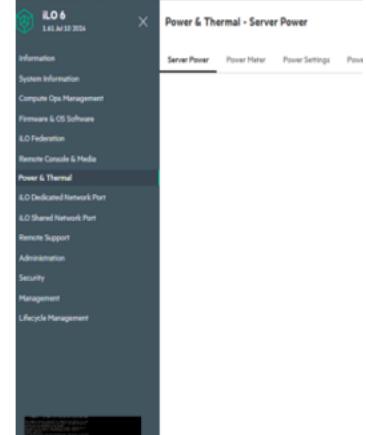
    23.2 Issue 2 – PCC-MM S6a Diameter HSS Down...

    23.3 Issue 3 – CCRC DNS KPIs Show Permanent 6...

    23.4 Issue 4 – Possible Fail UE Session Establish, T...

2025-06-05 1/1531-HSC 901 198/1 Uen Rev J





Comment by Meryam Nachi [ 2025-06-03 ]

New feature request for UCC 1.2 has been created.

Comment by Fredrik Gustavsson [ 2025-02-05 ]

We have received the answer from CCD: "Bios setting are outside of CCD documentation".

After confirmation by [Eric Fenger](#), I am now forwarding this to the UCC design team to include the necessary "System Power Restore" BIOS setting in the documentation.

Comment by Fredrik Gustavsson [2025-02-05]

Hi Rajan

yes, the "System Power Restore Settings" is not described in the CPI. I do not know if ccdadm is adjusting this but the log entry you sent is the correct area where it is likely.

In UCC, we are relying on CCD for these settings and since it's unclear if this is managed by ccdadm, I raised a support ticket with them (ECCDSUPP-5250).

Comment by Rajan Rajeshprasad Gupta (2025-02-02)

Dear Fredrik,

Thank you for your feedback

I have re-checked the CCD CPI but, unfortunately, I was unable to find the correct information regarding the BIOS power settings. Could you please provide a specific link to

Regarding the CCD installation steps, I reviewed the installation logs and noted that two servers were powered on and off. However, the installation debug and information Could you please confirm if this is the step where CCD sets the BIOS settings?

```

Line 103: 2024/09/10 16:31:00 INFO: 2024/09/10 16:31:00 DEBUG: [pkg/controller/singleserver/utils/ss_utils.go:195] Target node power state is :On      Line 104: 202
[pkg/controller/singleserver/utils/ss_utils.go:258] Node is not Power OFF yet: Power is not OFF yet      Line 105: 2024/09/10 16:31:06 INFO: 2024/09/10 16:31:06 DEBUG
state is :Off   Line 106: 2024/09/10 16:31:06 INFO: 2024/09/10 16:31:06 INFO: [pkg/controller/singleserver/utils/ss_utils.go:679] Node from HPE BMC had been Power 0
[pkg/controller/singleserver/utils/ss_utils.go:195] Target node power state is :Off      Line 114: 2024/09/10 16:31:14 INFO: 2024/09/10 16:31:14 INFO: [pkg/controller
not ON yet   Line 115: 2024/09/10 16:31:19 INFO: 2024/09/10 16:31:19 DEBUG: [pkg/controller/singleserver/utils/ss_utils.go:195] Target node power state is :Reset
[pkg/controller/singleserver/utils/ss_utils.go:299] Node is not Power ON yet: Power is not ON yet      Line 117: 2024/09/10 16:31:25 INFO: 2024/09/10 16:31:25 DEBUG
state is :Reset Line 118: 2024/09/10 16:31:25 INFO: 2024/09/10 16:31:25 INFO: [pkg/controller/singleserver/utils/ss_utils.go:299] Node is not Power ON yet: Power is
DEBUG: [pkg/controller/singleserver/utils/ss_utils.go:195] Target node power state is :On      Line 120: 2024/09/10 16:31:32 INFO: 2024/09/10 16:31:32 INFO: [pkg/c
Power On.   Line 484: 2024/09/10 16:52:34 INFO: 2024/09/10 16:52:34 DEBUG: [pkg/ssh/manager.go:590] SSH task [Run update registry images script] completed succes
monitorccdfw-managerccd-infra-controllerccd-license-consumercdd-task-exec-fwccd-task-exec-jobbccd-troubleshooting-toolscert-manager-cainjectorcert-manager-controllerc
driver-registrarcsi-provisionercsi-resizercsi-snapshotterdefaultbackenddexdrainoeric-cr-bragenteric-cr-initeric-cr-migrationeric-cr-registryeric-cr-sidecareric-data-d
smart-helm-hooks-hooklaunchereric-lm-database-migrationeric-lm-license-consumer-handlereric-lm-license-server-clienteric-lm-model-initeric-pm-br-initcontainereric-pm
server-utilseric-pm-sftperic-sec-sip-tls-maineric-sec-sip-tls-supervisoreric-si-application-sys-info-handlereric-tm-external-connectivity-frontend-controllereric-tm-e
managerkeepalivekube-apiserverkube-controller-managerkubectl-clientkube-dns-node-cachekube-proxykube-rbac-proxykuberokube-schedulerkube-scheduler-taskyvernokyverno
controllerlinuxptp-daemonlivelinessprobmanagementcpuoverridemdm_configmetrics-servermultusnetwork-resources-injectornginx-ingress-controllernginx-tls-terminatornodenod
markerovs-cni-clipausepmbr-config-managerpod2daemon-flexvolpodmonpower-metrics-exporterpowers-node-agentpower-operatorprometheus-webhook-isp-loggerprometheus-webhook
device-pluginsrion-network-metrics-exportervmagentvmaertvmbckupvmctlvminsertvmrestorevmselectvmstoragevolume-group-provisionervolume-group-snapshottervolume-mutato
[pkg/addons/manager.go:1123] will install addons [[cert-manager kyverno siptls external-snapshotter ingress dex auth-client tiller calico enhanced-host-security ccd-t
whereabouts pm metrics-server pm_webhook_snmp prometheus-webhook-isp-logger pm-bulk-reporter fluent-bit fluentd network-resources-injector sriov-network-device-plugin
discovery node-problem-detector falco kube-scheduler-tas qdr ptp cr-registry k8s-power-manager]], and priority addons [[calico cert-manager kyverno mgmt-cpu-override]
[pkg/addons/manager.go:635] No valid user config found for this addon[k8s-power-manager] action. Skipping.   Line 655: 2024/09/10 16:53:43 INFO: 2024/09/10 16:53:
k8s-power-manager   Line 1063: 2024/09/10 16:54:51 INFO: 2024/09/10 16:54:51 DEBUG: [pkg/addons/manager.go:1123] will install addons [[cert-manager kyverno siptls
security ccd-task-exec-fw local-storage-provisioner ccd-central-registry ecfe multus whereabouts pm metrics-server pm_webhook_snmp prometheus-webhook-isp-logger pm-bu

```

As for the UCC power on/off, the documentation only addresses ILO-based power operations and does not provide specific details on setting power configurations in the BI  
Specially section of power setting in bios is not at all highlighted in prints.

The request from this ticket is to clarify the appropriate UCC BIOS power settings and to confirm whether any scripts are modifying these settings during the CCD installation guide.

Please advise

Comment by [Fredrik Gustavsson](#) [ 2025-01-17 ]

Since UCC is using CCD as its platform, during the CCD installation some BIOS settings are being made. For more information about CCD, please see the CCD CPI.

In UCC, we also have some specific settings on top of the CCD ones. These are described in the Installation Instruction.

Regarding upstart or restart procedures, they are covered in the chapter "Graceful Shutdown and Startup procedure" where currently, the router must be brought up and ch

Please monitor post-CCD installation power setting state, before any manual BIOS alteration, and report any discrepancy within the same CCD version.

#### [UCC\_PLM-185] Missing certificate requirements - PKCS#1 key format Created: 2025-01-03 Updated: 2025-04-23 Resolved: 2025-04-23

<b>Status:</b>	Done
<b>Project:</b>	UCC_PLM
<b>Component/s:</b>	None
<b>Affects Version/s:</b>	UCC Appliance 1.0.1
<b>Fix Version/s:</b>	None

<b>Type:</b>	Bug	<b>Priority:</b>	Medium
<b>Reporter:</b>	Fredrik Gustavsson	<b>Assignee:</b>	Unassigned
<b>Resolution:</b>	Closed	<b>Votes:</b>	0
<b>Labels:</b>	5GCompad		
<b>Remaining Estimate:</b>	Not Specified		
<b>Time Spent:</b>	Not Specified		
<b>Original Estimate:</b>	Not Specified		

<b>Attachments:</b>	
<b>Issue Links:</b>	<b>Association</b>
	Is Associated with <a href="#">ECD-22442</a> generate-certs.sh dependency on opens... Done
<b>Detected in phase:</b>	Production
<b>Team/s:</b>	UCC_XFT2
<b>Severity_qmt:</b>	3- Medium
<b>Found in Build:</b>	UCC Appliance 1.0.1

**Requirement Status:**

UCC Appliance 0.2.1 - UNCOVERED

**Description**

In the Software Installation Guide, Rev "", 2024-09-06, accessed from [Ultra Compact Core \(UCC\) 1.0](#), there are missing requirements related to customer provided certificates.

These certificates must use private keys with PKCS #1 format to be able to install UCC.

It might be relevant to also state that the RSA algorithm must be used, although this can be inferred from the PKCS #1 requirement.

The sections relevant, include:

- Chapter 2, Introduction
  - A pair of CA certificate and corresponding asymmetric keys is required for CCD installation (ca-ccd.crt and ca-ccd.key), and another pair is needed to generate certificates for secure communication with/between network functions included in UCC (ca.crt, ca.pem and ca.key)
- Chapter 5.2, Requirements for Certificates
  - The SSL keys provided with certificates must be unencrypted and not password protected.
  - The minimum key size in bits must be 112 or greater.
  - A certificate must use SHA-256 (also known as SHA-2).

**Comments**

Comment by [Fredrik Gustavsson](#) [ 2025-02-06 ]

We should specify that only 2048 bits is supported in the current release:

Rajan Rajeshprasad Gupta 01-29 6:02 Edited  
Hello Dapeng Jiao  
I was trying to deploy CCD with 4096 bit public keys for CCD ca.crt and ca.keys.  
I realised from CPI, CCD is only supporting only 2048 RSA Keys. Can you help to share your views?  
Ericsson Cloud Container Distribution 2.10.2 | Version v | Help | EGTRUM

Ganesh Vasudevan 01-29 6:17  
Yes. We we are working on the 4096 support.  
1 2

Comment by [Meryam Nachi](#) [ 2025-02-06 ]

the requirements are updated into:

- The SSL keys provided with certificates must be unencrypted and not password protected.
- The certificates must use private keys in the PKCS#1 format (RSA) with a key size of minimum 2048 bits.
- The certificates must use SHA-256 (also known as SHA-2).

Comment by [Alexander Malikov](#) [ 2025-01-09 ]

In regards to your ticket, I'm going to introduce following changes in the chapter 5.2 of UCC installation instructions:

**Requirements for Certificates**

- The SSL keys provided with certificates must be unencrypted and not password protected.
- \* The certificates must use private keys with PKCS #1 format.
- \* The RSA algorithm must be used for the certificates.\*
- The minimum key size in bits must be 112 or greater.
- The certificates must use SHA-256 (also known as SHA-2).

Please check and give the feedback if it will address the issue reported in the ticket.

Comment by [Fredrik Gustavsson](#) [ 2025-01-03 ]

If a PKCS #8 format is used, then we see the following error:

```
kubectl -n kyverno logs deploy/kyverno-admission-controller
2025-01-03T15:29:05Z    ERROR  setup.runtime-checks    runtime/utils.go:101    failed to validate certificates      {"error": "x509: failed to parse private key\n(use ParsePKCS8PrivateKey instead for this key format)"}
```

<b>Status:</b>	Done
<b>Project:</b>	<a href="#">UCC_PLM</a>
<b>Component/s:</b>	None
<b>Affects Version/s:</b>	<a href="#">UCC Appliance 1.0.1</a>
<b>Fix Version/s:</b>	None

<b>Type:</b>	Bug	<b>Priority:</b>	Medium
<b>Reporter:</b>	<a href="#">Fredrik Gustavsson</a>	<b>Assignee:</b>	<a href="#">Meryam Nachi</a>
<b>Resolution:</b>	Closed	<b>Votes:</b>	0
<b>Labels:</b>	5GCompad		
<b>Remaining Estimate:</b>	Not Specified		
<b>Time Spent:</b>	Not Specified		
<b>Original Estimate:</b>	Not Specified		

<b>Detected in phase:</b>	Production
<b>Team/s:</b>	UCC_XFT2
<b>Severity_qmt:</b>	3- Medium
<b>Found in Build:</b>	UCC Appliance 1.0.1
<b>Requirement Status:</b>	UCC Appliance 0.2.1 - UNCOVERED

#### Description

In Software Installation Guide, revision "", date "2024-09-06" accessed via [Ultra Compact Core \(UCC\) 1.0](#), in chapter 7 "Jump Host Preparation", bullet 6, the second command is:

```
tar -xvzf $software_dir/UCC_Artifacts_-_Configuration_Files.gz \
--directory $config_dir
```

However, when using the UCC SW package CXS1010198\_1-R1D.zip from UCC 1.0.1 (1.0 CP1), this will result in the structure:

```
$config_dir
└── ucc-config
    ├── certificates
    └── config
```

There are no additional instructions on how to remove the "ucc-config" intermediate folder, and the remainder of the document assumes that the "certificates" and "config" folders are placed directly under the \$config\_dir.

An alternative correction could be to remove the "ucc-config" top folder from the tar-ball.

#### [UCC\_PLM-183] Certs classification

Created: 2024-12-20 Updated: 2025-01-16 Resolved: 2025-01-16

<b>Status:</b>	Rejected
<b>Project:</b>	<a href="#">UCC_PLM</a>
<b>Component/s:</b>	None
<b>Affects Version/s:</b>	None
<b>Fix Version/s:</b>	None

<b>Type:</b>	Task	<b>Priority:</b>	Medium
<b>Reporter:</b>	<a href="#">Jossy Pallan</a>	<b>Assignee:</b>	<a href="#">Fredrik Gustavsson</a>
<b>Resolution:</b>	Rejected	<b>Votes:</b>	0
<b>Labels:</b>	None		
<b>Remaining Estimate:</b>	Not Specified		
<b>Time Spent:</b>	Not Specified		
<b>Original Estimate:</b>	Not Specified		

#### Description

Hi,

As discussed in 1.0 CP1 discussion, please do the exercise in classifying UCC certificates in groups or External, Internal and External but optional (if any in the 3rd group).

BR  
Debajit

#### Comments

Comment by [Fredrik Gustavsson](#) [ 2025-01-16 ]

Hi, for improvements, please open a Feature Request according to this instruction: [UCC Feature Request Process](#) and it will be analyzed by the correct team. For the PLM ticket, I will proceed to close this one.

Comment by [Debajit Mitra](#) [ 2025-01-13 ]

Happy new year! [Fredrik Gustavsson](#), yes task is fine. Thank you.

Comment by [Fredrik Gustavsson](#) [ 2024-12-30 ]

[Jossy Pallan, Debajit Mitra](#), this issue is raised as a Task, is this correct or should it be handled as a Bug?

[UCC\_PLM-182] Missing revision and incorrect date of UCC Software Installation Guide Created: 2024-12-19 Updated: 2025-04-23 Resolved: 2025-04-23

Status:	Done
Project:	<a href="#">UCC_PLM</a>
Component/s:	None
Affects Version/s:	<a href="#">UCC Appliance 1.0.1</a>
Fix Version/s:	None

Type:	Bug	Priority:	Medium
Reporter:	<a href="#">Fredrik Gustavsson</a>	Assignee:	Unassigned
Resolution:	Closed	Votes:	0
Labels:	None		
Remaining Estimate:	Not Specified		
Time Spent:	Not Specified		
Original Estimate:	Not Specified		

Attachments:	
Defect code_qmt:	3- Usability
Sprint:	UCC_XFT2 Sprint 5
Detected in phase:	PDU
Team/s:	UCC_XFT2
Severity_qmt:	3- Medium
Found in Build:	UCC Appliance 1.0.1
Requirement Status:	UCC Appliance 0.2.1 - UNCOVERED

#### Description

In the UCC Software Installation Guide Rev "", 2024-09-06 part of UCC 1.0.1 CPI EN/LZN7041198 R1B, the revision is missing, and the date is incorrect.

2024-09-06

Rev

© Ericsson AB 2024

2 (228)

Also, in the revision history, a preliminary revision is listed:

## 1 Revision History

Revision	Modifications	Date	Author
A	UCC 1.0	2024-09-26	Dev Team
PG2	UCC 1.0 CP1	2024-12-11	Dev Team

[UCC_PLM-181] UCC 1.0(BAH): Hardcoded APN names <small>Created: 2024-12-16 Updated: 2025-02-13 Resolved: 2025-02-13</small>						
Status:	Rejected					
Project:	<a href="#">UCC_PLM</a>					
Component/s:	None					
Affects Version/s:	None					
Fix Version/s:	None					
Type:	Bug	Priority:	Medium			
Reporter:	<a href="#">Rajan Rajeshprasad Gupta</a>	Assignee:	Unassigned			
Resolution:	Rejected	Votes:	0			
Labels:	None					
Remaining Estimate:	Not Specified					
Time Spent:	Not Specified					
Original Estimate:	Not Specified					
Issue Links:	<b>Z DO NOT USE Replaces</b> is replaced by <a href="#">UCCXFT-662</a> UCC 1.0(BAH): Hardcoded APN names					
Found in Build:	UCC 1.0					
Requirement Status:	UCC Appliance 0.2.1 - UNCOVERED					
<b>Description</b> <p>Hello,</p> <p>There is no option in LLD to take input of APN name</p> <p>APN= internet is hardcoded for SMF, PCF and Eda Provisioning files.</p> <p>As a results for customer who needs customized APN name like BAHUCC01 , It require manual work and customization which is difficult for each time during LCM.</p>						
<b>Comments</b> <p>Comment by <a href="#">Fredrik Gustavsson</a> [ 2025-02-13 ]            Thanks <a href="#">Jim Dumont!</a></p> <p>Comment by <a href="#">Jim Dumont</a> [ 2025-02-13 ]            Improvement story <a href="https://eteamproject.internal.ericsson.com/browse/UCCXFT-662">https://eteamproject.internal.ericsson.com/browse/UCCXFT-662</a> linked to this ticket.</p> <p>Comment by <a href="#">Fredrik Gustavsson</a> [ 2025-02-12 ]            I have assigned <a href="#">Jim Dumont</a> to this case.            Jim will raise an improvement request and link it to this issue.            We will then proceed to close (reject) this issue as this is not a bug.</p> <p>Comment by <a href="#">Eric Fenger</a> [ 2025-02-11 ]            Hi <a href="#">Rajan Rajeshprasad Gupta</a> ,            to make APN names customizable, is a new requirement. For now only the manual option            is possible.  <a href="#">Andreas Göthe</a> is aware of this improvement request.            BR Eric</p> <p>Comment by <a href="#">Rajan Rajeshprasad Gupta</a> [ 2025-02-11 ]            Hello <a href="#">Eric Fenger</a>            Thank you for your valuable feedback.            I would like to share insights from different UCC projects concerning MANA and MELA in relation to UCC 1.0.            It has become evident that every customer is requesting their own specific APN name. This requirement is leading us to manually add APNs post-deployment (either during initial installation or upgrade/reinstall) as part of our service delivery process.            This manual step is creating additional work, and it could potentially impact the LCM processes planned for the upcoming 1.1 release.            Could you please provide guidance on whether we should continue with the manual APN addition post-deployment to meet customer needs, or if there is an alternative approach we should consider?</p>						

Comment by Eric Fenger [ 2025-02-11 ]

Hi Rajan Rajeshprasad Gupta ,

this is not a bug, but it was a conscious decision taken in pre-config study where this is documented.

This is an improvement request (new functionality).

BR Eric

Comment by Zhigang Han [ 2024-12-17 ]

Hi team,

PLM team has discussed with Rajan about the priority. We dropped the priority from critical to medium. It will be the improvement for the future release.

Thanks,

BR/Zhigang

Comment by Fredrik Gustavsson [ 2024-12-17 ]

Hi Meryam Nachi, please investigate if this can be parameterized.

#### [UCC\_PLM-180] Router config: incorrect IP and BGP Neighbor IPs for sig\_ext Created: 2024-12-11 Updated: 2024-12-12 Resolved: 2024-12-12

Status:	Duplicated
Project:	UCC_PLM
Component/s:	None
Affects Version/s:	UCC Appliance 1.0.0
Fix Version/s:	None

Type:	Bug	Priority:	Medium
Reporter:	Fredrik Gustavsson	Assignee:	Fredrik Gustavsson
Resolution:	Duplicate	Votes:	0
Labels:	None		
Remaining Estimate:	Not Specified		
Time Spent:	Not Specified		
Original Estimate:	Not Specified		

Attachments:			
Issue Links:	<b>Duplicate</b> duplicates <a href="#">UCC_PLM-116</a> UCC MCN : Duplicate IP address used i... Done		
Detected in phase:	PDU		
Severity_qmt:	3- Medium		
Found in Build:	UCC Appliance 1.0.0		
Requirement Status:	UCC Appliance 0.2.1 - UNCOVERED		

#### Description

In the generated router config, we have incorrect entries for the sig\_ext context:

```
context sig_ext
!
!
interface ecfe-sig-ext
description ecfe-sig-ext
ip address 172.16.0.25/29
!
!
router bgp 425120008
multi-paths external 8
address-family ipv4 unicast
redistribute connected
redistribute static
!
neighbor 172.16.0.26 external
remote-as 425121008
description ecfe-sig-ext-ccd-a
ebgp-multihop 2
address-family ipv4 unicast
```

```
!
neighbor 172.16.0.27 external
remote-as 4251210008
```

According to the IP plan in the LLD, we should have the interface IP 172.16.0.33/29 and the neighbors should have IPs 172.16.0.34 and 172.16.0.35.

sig_ext	ucc : 4251210008 router : 4251200008	172.16.0.32/29	gateway_ip ecfe_sig_ext_ip	172.16.0.33 172.16.0.34
sig_ext	ucc : 4251210008 router : 4251200008	172.16.0.32/29	gateway_ip ecfe_sig_ext_ip	172.16.0.33 172.16.0.35

#### Comments

Comment by [Fredrik Gustavsson](#) [2024-12-12]

This is likely a duplicate of UCC\_PM-116 and occurred in the system based on the manual update steps, post-CNAT config generation. This made the discrepancy to appear.

[UCC\_PLM-179] [MANA-Vz: UCC 1.0 : httpproxies are not in valid state](#) Created: 2024-12-09 Updated: 2025-06-03 Resolved: 2025-06-03

Status:	Rejected
Project:	<a href="#">UCC_PLM</a>
Component/s:	None
Affects Version/s:	None
Fix Version/s:	None

Type:	Bug	Priority:	Medium
Reporter:	<a href="#">Rajan Rajeshprasad Gupta</a>	Assignee:	<a href="#">Alexander Malikov</a>
Resolution:	Rejected	Votes:	0
Labels:	UCC_Appliance_1.1.0, Verizon		
Remaining Estimate:	Not Specified		
Time Spent:	Not Specified		
Original Estimate:	Not Specified		

Attachments:	<a href="#">PLM-179.docx</a>
Detected in phase:	Production
Team/s:	UCC_XFT2
Found in Build:	UCC Appliance 1.0.0
Requirement Status:	UCC Appliance 0.2.1 - UNCOVERED

#### Description

Hello,

It is observed number of httpproxies are not in valid state(See list for ccrc,ccsm etc)

Customer would like to know plan to either delete if this are not required or if required how to make them valid?

Same behavior is observed across all UCC deployments.

```
eccc@ucc-ccda:~> kubectl get httpproxies.projectcontour.io -A
```

NAMESPACE	NAME	FQDN	TLS SECRET	STATUS	STATUS DESCRIPTION
ccdm	eric-adp-nomn-httpproxy	cnom.ccdm1-oam.n99-eccc1.sero.gic.ericsson.se.5gc.mnc480.mcc311.3gppnetwork.org	iccr-external-tls-secret		
<b>NotReconciled Waiting for controller</b>					
ccrc	eric-adp-5g-udm-nomn-httpproxy	cnom-ccrc-ericucc1a.ericucc1.internal.ericsson.com	iccr-external-tls-secret	valid	Valid
<b>HTTPProxy</b>					
ccrc	eric-nrf-provision-httpproxy	prov-ccrc-ericucc1a.ericucc1.internal.ericsson.com	eric-ccrc-nrf-provision-server-certs	invalid	At least
<b>one error present, see Errors for details</b>					
ccsm	eric-ccsm-adp-nomn-httpproxy	oam-cnom-ericucc1a.ericucc1.internal.ericsson.com	iccr-external-tls-secret	NotReconciled	
<b>Waiting for controller</b>					
cnom	eric-cnom-server	oam-cnom-ericucc1a.ericucc1.internal.ericsson.com	eric-cnom-server-certm-certificate-secret	valid	Valid
<b>HTTPProxy</b>					
eda	eric-act-cna-notif-ingress	notif.eda-ericucc1a.ericucc1.internal.ericsson.com	eric-act-cna-notif-secret	valid	Valid
<b>HTTPProxy</b>					

eda	eric-act-cna-oam-ingress	oam.eda-ericucc1a.ericucc1.internal.ericsson.com	eric-act-cna-oam-secret-uca102	valid	Valid
HTTPProxy					
eda	eric-act-cna-prov-ingress	prov.eda-ericucc1a.ericucc1.internal.ericsson.com	eric-act-cna-prov-secret-uca102	valid	Valid
HTTPProxy					
eda	eric-act-cna-prov-notif-ingress	notif-mtls.eda-ericucc1a.ericucc1.internal.ericsson.com	eric-act-cna-prov-notif-secret	valid	Valid
HTTPProxy					
eccc@ucc-ccda:~>					

#### Comments

Comment by <a href="#">Alexander Malikov</a> [ 2025-06-03 ]
Not observed in UCC 1.1
Comment by <a href="#">Jim Dumont</a> [ 2025-04-28 ]
<b>Meryam Nachi</b> - is this still an issue with UCC 1.1 - or can we simply cancel it as essentially "obsolete"?
Comment by <a href="#">Cheng-Jun Li</a> [ 2024-12-13 ]
See attached detailed investigation.
Summary:
1) The issue is reproduceable on different deployment.
2) For " <b>'invalid' status for eric-ccrc0nrf-provision-server-certs</b> ", based on the commands outputs, the cause might be "Spec.VirtualHost.TLS client validation is invalid: invalid CA Secret "ccrc/eric-ccrc-nrf-provision-server-certs-cacert": empty "ca.crt" key"
3) For the " <b>NotReconciled Waiting for controller</b> ", not sure whether "tls.crt: 0 bytes; tls.key: 0 bytes" is the cause, maybe not, because tls.crt and tls.key for " <b>eric-adp-cnom-httpproxy</b> " are present yet we still get the NotReconciled state.
So design need to take a look and confirm whether it's a bug, if so, provide a fix.
For 2), we assume the fixe can be either in the II (adding steps to load the ca.crt) or in deployment script to load the ca.crt automatically.
For 3), not sure. Didn't find more logs to provide hint on why the "NotReconciled" state.

[UCC_PLM-173] Installation Instructions refers to the use of self-signed certificates	
<b>Status:</b>	Done
<b>Project:</b>	<a href="#">UCC_PLM</a>
<b>Component/s:</b>	None
<b>Affects Version/s:</b>	None
<b>Fix Version/s:</b>	None

<b>Type:</b>	Bug	<b>Priority:</b>	High
<b>Reporter:</b>	<a href="#">Mirac Gunes</a>	<b>Assignee:</b>	Unassigned
<b>Resolution:</b>	Closed	<b>Votes:</b>	0
<b>Labels:</b>	UCC_Appliance_1.0.1		
<b>Remaining Estimate:</b>	0h		
<b>Time Spent:</b>	4h		
<b>Original Estimate:</b>	0h		

<b>Attachments:</b>	
<b>Issue Links:</b>	<b>Z DO NOT USE Gantt End to End</b>
<b>Defect code_qmt:</b>	3- Usability
<b>Sprint:</b>	UCC XFT2 Sprint 3, UCC XFT2 Sprint 4
<b>Team/s:</b>	UCC_XFT2
<b>Severity_qmt:</b>	2- High
<b>Found in Build:</b>	UCC Appliance 1.0.0
<b>Requirement Status:</b>	UCC Appliance 0.2.1 - UNCOVERED

#### Description

"Any references to the usage of Self-Signed certs (while perhaps in use inside our labs) should be removed from any customer supported/facing documentation." - Daniel Smith

Chapter 9 in the II is contradicting to it,

**Important Note**

Certificate management is out of the scope of Ericsson Ultra Compact Core. The customer should provide the certificates as described in the table.

For testing purposes, we provide the following procedure to generate certificates signed by locally provided root CA in case the customer does not have the possibility to provide TLS certificates.

"... in the case the customer does not have the possibility to provide TLS certificates" - Daniel Smith.

According to this statement, why are we worried about the customer not being able to provide TLS certificates?

We shall also add a PKI to this list in the II to make it extra clear.

The following items are not included in the Ericsson Ultra Compact Core product and should be secured by the customer:

- Licensing server (**NeLS**) which can be used by UCC to fetch licenses.
- At least one Domain Name System (**DNS**) server should be available and reachable from UCC.
- At least one Network Time Protocol (**NTP**) server should be available and reachable from UCC.
- External connectivity of UCC should be secured by the customer.

This proposal has been verified by Daniel,

"Good stuff..

*all of this needs to be corrected and updated yup, the II is for sure customer facing, the others i dont know.*

*thanks for keeping us honest.*

#### Comments

Comment by [Mirac Gunes](#) [ 2025-01-17 ]

Awesome, thanks for the changes!

Comment by [Fredrik Gustavsson](#) [ 2025-01-17 ]

Thanks! I will go ahead and close this ticket since the reported issue has been corrected according to the proposal. If any future improvements are needed, they will be han

Comment by [Alexander Malikov](#) [ 2025-01-17 ]

Changes in installation instructions were agreed and release in UCC 1.0 CP1 and more corrections will be introduced in UCC 1.1.

[Mirac Gunes](#) Do we still need to keep this ticket open or we can close it?

Comment by [Alexander Malikov](#) [ 2024-12-11 ]

Installation guide was updated and shared with I&V for testing.

<https://ericsson.sharepoint.com/:b/r/sites/UltraCompactCoreUCC/Shared%20Documents/General/DEV-DOCUMENTS-WORKDIR/UCC%201.0CP1/Ericsson%20Ultra%20Com> csf=1&web=1&e=0Qr5vx&xsdatta=MDV8MDJ8UGFuYWdpb3RhLBhcHBhQGVyaWNzc29uLmNvbXw1MzM5ZmQ4ODIxNzU0MGZjOWRjODA4ZGQxOWQxZDM5OHw5MmU

Comment by [Fredrik Gustavsson](#) [ 2024-12-10 ]

Hi [Alexander Malikov](#), assigning to you as the current author of the II. Thanks!

Comment by [Fredrik Gustavsson](#) [ 2024-12-10 ]

Hi [Meryam Nachi](#), please ensure that the II is updated as per above for UCC Appliance 1.0.1

Comment by [Mirac Gunes](#) [ 2024-12-05 ]

A humble input, this is very much related however may be missed due to the size of the II. So it could be merged with the other issue or linked to it.

Comment by [Jim Dumont](#) [ 2024-12-04 ]

[Reema Sidhwani](#) - does this doc bug need to be fixed along with the actual software bug that was discussed 2024/12/04 that is delaying CP1 release? Obviously we don't v

[UCC\_PLM-172] [Test](#) Created: 2024-11-27 Updated: 2024-12-10 Resolved: 2024-12-10

Status:	Cancelled
Project:	UCC_PLM
Component/s:	None
Affects Version/s:	None
Fix Version/s:	<a href="#">test fix version xyz 123</a>

Type:	Story	Priority:	Low
-------	-------	-----------	-----

<b>Reporter:</b>	Jim Dumont	<b>Assignee:</b>	Reema Sidhwani
<b>Resolution:</b>	Cancelled	<b>Votes:</b>	0
<b>Labels:</b>	None		
<b>Remaining Estimate:</b>	Not Specified		
<b>Time Spent:</b>	Not Specified		
<b>Original Estimate:</b>	Not Specified		

<b>Requirement Status:</b>	UCC Appliance 0.2.1 - UNCOVERED
----------------------------	---------------------------------

Description	
Test	

<a href="#">[UCC_PLM-171] CCSM- Open Alarms for UDM &amp; HSS</a> Created: 2024-11-22 Updated: 2025-03-11 Resolved: 2024-12-05			
<b>Status:</b>	Done		
<b>Project:</b>	UCC_PLM		
<b>Component/s:</b>	None		
<b>Affects Version/s:</b>	UCC Appliance 1.0.0-rc2		
<b>Fix Version/s:</b>	None		

<b>Type:</b>	Bug	<b>Priority:</b>	Medium
<b>Reporter:</b>	Rishi Shekhar	<b>Assignee:</b>	Unassigned
<b>Resolution:</b>	Closed	<b>Votes:</b>	0
<b>Labels:</b>	None		
<b>Remaining Estimate:</b>	0h		
<b>Time Spent:</b>	16h		
<b>Original Estimate:</b>	0h		

<b>Attachments:</b>	CNAT_install_20241128182341.log	screenshot-1.png	screenshot-2.png
<b>Issue Links:</b>	<b>Duplicate</b>		
duplicates	<a href="#">UCCXFT-155</a>	UCC 1.0 CP1: CCSM alarms 'UDM Fail to...	Done
<b>Other Assignees:</b>	Rishi Shekhar		
<b>Sprint:</b>	UCC XFT2 Sprint 2		
<b>Detected in phase:</b>	Production		
<b>Team/s:</b>	UCC_XFT2		
<b>Severity_qmt:</b>	3- Medium		
<b>Found in Build:</b>	UCC 1.0 GA		
<b>Requirement Status:</b>	UCC Appliance 0.2.1 - UNCOVERED		

Description	
Hi Team,	
We have observed below open alarm on CCSM from MANA UCC 1.0 GA release.	
ccsmoam@ccda#	
ccsmoam@ccda#show alarm	
udmNhssHssConnectionFailure	
active-severity Major	
service-name eric-udm-common	
event-type CommunicationsAlarm	
expires 599	
source /ericsson-udm:udm/non_modeled/local[service-name=eric-udm-common]/remote[id=9448c0d3-6590-4e54-b90f-485353a1c1d1][service-name=nhss-uecm]	
specific-problem UDM Fail to Connect to HSS	
probable-cause 100505	
major-type 193	
minor-type 7798821	
last-event-time 2024-11-07T13:21:20.214000 PST	
additional-text UDM Fail to Connect to HSS	

```

udmNhssHssInstanceUnavailable
active-severity Critical
service-name eric-udm-common
event-type CommunicationsAlarm
expires 599
source /ericsson-udm:udm/non_modeled/local[service-name=eric-udm-common]/remote[id=9448c0d3-6590-4e54-b90f-485353a1c1d1][service-name=nhss-uecm]
specific-problem HSS Instance Unavailable for UDM
probable-cause 23
major-type 193
minor-type 7798822
last-event-time 2024-11-07T13:21:20.214000 PST
additional-text HSS Instance Unavailable for UDM

ccsmLmagentCcsmServicesNotDeployed
active-severity Major
service-name eric-ccsm-common
event-type OperationalViolation
expires 314
source /ericsson-ccsm:ccsm/non_modeled/local[service-name=eric-ccsm-lmagent]
specific-problem Mandatory service not deployed for licensed functionality
probable-cause 100506
major-type 193
minor-type 11993097
last-event-time 2024-11-07T13:48:25.905000 PST
additional-text Licensed by FAT1024210/2:eric-udm-iwk5g2g;FAT1024210/7:eric-udm-eapauth,eric-udm-eapprimeauth,eric-udm-gbaauth,eric-udm-imsauth is/are not
deployed

As per CPI:- we can see some configuration might have been missing for UDM & HSS alarm.

https://cpistore.internal.ericsson.com/elex?LI=EN/LZN7041198/1R1A&CL=EN/LZN7020558/1\*&FN=25\_1543-CSH109716\_1Uen.F.html&HT=nza1698219929747&DT=UDM+Fail+to+Connect+to+HSS

ccsmoam@ccdb#show running-config ccsm-common remote-nf-profile remote-nf-profile
% No entries found.
ccsmoam@ccdb#

ccsmoam@ccdb#show running-config udm remote-nf-profile remote-nf-profile 9448c0d3-6590-4e54-b90f-485353a1c1d2
udm remote-nf-profile remote-nf-profile 9448c0d3-6590-4e54-b90f-485353a1c1d2
type hss
fqdn hss-ccsm-tmouccb.5gc.mnc660.mcc311.3gppnetwork.org
hss-info-list 1
hss-info group-id 1
hss-info imsi-range 1
imsi-start 3116600000000000
imsi-end 3116609999999999
!
!
remote-nf-service nhss-uecm-0
name nhss-uecm
fqdn hss-ccsm-tmouccb.5gc.mnc660.mcc311.3gppnetwork.org
scheme http
ip-endpoint 1
port 80
!
version v1
api-full-version 1.R15.1.1
expiry 2050-10-23T09:45:12.438+00:00
!
!
!
ccsmoam@ccdb#

```

## Comments

Comment by Alvaro Martin [ 2024-12-05 ]

I think we can close this ticket:

- UCC1.0 CP1 has been updated to automatically remove port 8086 via CNAT, as last step in the vnf.yaml of ccsm deployment.
- The manual step which was described in UCC1.0 Installation Guide to remove 8086 port is deleted in Installation Guideline for CP1
- A known issue is added in CP1 Installation Guideline to update udm remote-nf-profile config (scheme and port) to secure ([https://cpistore.internal.ericsson.com/elex?LI=EN/LZN7041198/1R1A&CL=EN/LZN7020558/1\\*&FN=25\\_1543-CSH109716\\_1Uen.F.html&HT=nza1698219929747&DT=UDM+Fail+to+Connect+to+HSS](https://cpistore.internal.ericsson.com/elex?LI=EN/LZN7041198/1R1A&CL=EN/LZN7020558/1*&FN=25_1543-CSH109716_1Uen.F.html&HT=nza1698219929747&DT=UDM+Fail+to+Connect+to+HSS))

Comment by Rishi Shekhar [ 2024-12-05 ]

Issue for port 8086 block has been identified. Post deployment of CCSM- CU team applied a patch to remove port 8080 as per Software installation Guide from UCC 1.0 CPI.

[https://cpistore.internal.ericsson.com/elex?LI=EN/LZN7041198/1\\*](https://cpistore.internal.ericsson.com/elex?LI=EN/LZN7041198/1*)



UCC 1.0 CPI needs to be corrected accordingly & steps should be removed as its not applicable for UCC 1.0 release.

Comment by Rishi Shekhar [ 2024-12-03 ]

Hello Alvaro- Post redeployment of CCSM in two mana ucc1.0 setups udm & hss alarms not appearing.



But also we observing telnet to port 80 for hss-epc-traffic not working.

eccd@ucc-ccda:~> curl -v telnet://172.16.3.70:80

- Trying 172.16.3.70:80...
  - connect to 172.16.3.70 port 80 failed: Connection refused
  - Failed to connect to 172.16.3.70 port 80 after 0 ms: Couldn't connect to server
  - Closing connection 0  
curl: (7) Failed to connect to 172.16.3.70 port 80 after 0 ms: Couldn't connect to server
- eccd@ucc-ccda:~>  
eccd@ucc-ccda:~>  
eccd@ucc-ccda:~>  
eccd@ucc-ccda:~>  
eccd@ucc-ccda:~> curl -v telnet://172.16.3.70:443
- Trying 172.16.3.70:443...
  - Connected to 172.16.3.70 (172.16.3.70) port 443 (#0)  
^C
- eccd@ucc-ccda:~>

CCSM CNAT- installation logs looking clean- no pipeline or module present for port 80 block. [CNAT\\_install\\_20241128182341.log](#)

Comment by Alvaro Martin [ 2024-11-28 ]

Set to block till redeployment confirms the configuration

Comment by Alvaro Martin [ 2024-11-28 ]

MANA is using UCC1.0, where removal of port 8086 from gateway eric-ccsm-hss-epc-gateway is not implemented.

However the analysis shows that this port is actually removed.

This means someone has manually removed it in the gateway, as CCSM 1.13 includes that port as part of the deployment.

In fact, CPI describes how to delete it because the CCSM deployment keeps it open.

In order to confirm all this, please redeploy CCSM to verify that after deployment the port is there and therefore the connectivity from UDM to HSS through port 80 is working.

If right after deployment the port is removed, please check all the steps done in CNAT through cnat log to verify where it is being removed.

Comment by Alvaro Martin [ 2024-11-27 ]

This ticket is similar to [UCCXFT-155](#) UCC 1.0 CP1: CCSM alarms 'UDM Fail to Connect to HSS' is not cleared after connectivity is recovered - eTeamProject

Comment by Alvaro Martin [ 2024-11-27 ]

From UCC1.0 CP1 a new hardening configuration has been added to CCSM, in order to close the HSS cleartext port (targetPort=8086 for port 80 in svc eric-ingressgw-hss-epc-traffic):

- module: run-k8s-command  
name: Update hss-epc gateway  
cmd:  
patch gateways.networking.istio.io eric-ccsm-hss-epc-gateway --type=json -p="[{  
'op': 'remove', 'path': '/spec/servers/1'}]  
"-n ccsm

Configuration of the udm remote-nf-profile where hss connectivity data is defined with http scheme and port 80. This is not right, as this connectivity must be secured with mTLS. However, before CP1, as the HSS cleartext port was not closed, the configuration worked fine. After applying the hardening, this port cannot be reached and therefore UDM cannot reach HSS.

This udm remote-nf-profile configuration must be corrected to use mTLS, replacing http scheme by https and port 80 by 443. This information has been added in working copy of Deployment Guideline ([Ericsson Ultra Compact Core - Software Installation Guide.docx](#))

- New steps 5 and 9 in chapter 12.7 Deploy CCSM, in order to apply the required configuration change after deploying CCSM (replace http by https and 80 by 443)
- New known issue (chapter 21.8) describing the problem and the way to change the config.

[UCC\_PLM-170] MANA#UCC 1.0 : UCC installation guide missing steps for UCC without value package information Created: 2024-11-22 Updated: 2025-04-24 Resolved: 2025-04-24

Status:	Done
Project:	UCC_PLM
Component/s:	None
Affects Version/s:	UCC Appliance 1.0.0
Fix Version/s:	None

Type:	Bug	Priority:	Medium
Reporter:	Rajan Rajeshprasad Gupta	Assignee:	Unassigned
Resolution:	Closed	Votes:	0
Labels:	UCC_Appliance_1.1.0		
Remaining Estimate:	Not Specified		
Time Spent:	Not Specified		
Original Estimate:	Not Specified		

Issue Links:	<b>Dependent</b> depends on <a href="#">UCCXFT-774</a> <b>Problem/Incident</b> causes <a href="#">UCCXFT-1132</a>	UCC1.1, commercial license, Impact in... UCC Licensing: SWLT handling improvem...	Done To Do
Sprint:	UCC XFT1 Sprint 5, UCC XFT1 Sprint 6, UCC XFT1 Sprint 7, UCC XFT1 Sprint 8, UCC XFT1 Sprint 9		
Team/s:	UCC_XFT1		
Severity_qmt:	3- Medium		
Found in Build:	1.0.0		
Requirement Status:	UCC Appliance 0.2.1 - UNCOVERED		

#### Description

Hello,

As per UCC PPD (Product Package Description).

Commercial UCC has 2 types

- a. UCC with value pack which include CCPC+SC
- b. UCC without value pack which does not include CCPC/SC.

Raytheon has opted UCC without value pack.

I see no option/details mention in UCC Installation guide to support 2nd option ie skip or change configuration to send traffic on ccpc\*

Note\*

1. SMF to skip sending traffic to CCPC [ Change in APN configuration ] #
2. EP5G installation to skip installing CCPC
3. To avoid configuring CCPC Policies and Dataplan steps
4. Any other config not highlighted above etc.

Note#

Point1 is must to avoid customer using value CCPC value pack.

License control on CCPC is not a option as we have seen, CCPC without license reject call with 500 bad request ( It is not bypassing policies ).

```
{"version":"0.3.0", "timestamp":"2024-06-26T17:22:09.361431+02:00", "severity":"warning", "service_id":"eric-pcf-npcf-smppolicycontrol", "metadata":\{"category":"create", "groups":"business-policy-logs", "function":"PCF"}
```

, "message":"Unsuccessful Npcf\_SMPolicyControl response, SUPI: imsi-244990000000001, PEI: imeisv-123400000000101, GPSI: msisdn-86081000000001, TrafficId: 24499000000001, SubId: 24499000000001, **ErrorCause: No Base Package license available to handle N7 traffic**, SessionId: 5, SessionType: IPV4, DNN: internet, SliceInfo: {SST: 1, SD: 000001}, IpAddress: 10.23.0.2, SmPolicyId: 24499000000001|5|1719415329356880", "resp\_code":"500"}

Similar steps for SC should also reflect in UCC 1.1 as SC will be part of UCC 1.1.

## Comments

Comment by [Mats Persson](#) [ 2025-04-24 ]

CCPC/Policy button (enabling/disabling config requiring CCPC) delivered in LFD1.1

SEPP/Mobility button (enabling/disabling config requiring SEPP) delivered in LFD2

Comment by [Rajan Rajeshprasad Gupta](#) [ 2025-04-24 ]

Should we keep the ticket open, or has the solution already been delivered in version 1.1? Currently, we don't have access to a lab for SDU readiness testing, so I'm unsure of the status

Comment by [Mats Persson](#) [ 2025-04-24 ]

Problem not solved by updating document, but instead adding new deployment configuration parameters, see [UCCXFT-774](#).

Comment by [Åsa Preuss](#) [ 2025-04-24 ]

Shouldn't this ticket be labeled with Document?

We need it to make statistics.

BR Åsa

Comment by [Mats Persson](#) [ 2025-04-02 ]

Fix delivered in UCC 1.1 LFD1.1 delivery, [UCC 1.1 LFD1.1 - BCSS CNS-SE - Solutions and Ecosystem - EXPLORE, INVESTIGATE, PROVE - eTeamSpace](#).

Comment by [Mats Persson](#) [ 2025-03-21 ]

[UCCXFT-774](#) ticket now have provided a resolution "this will be controlled and propagated in SMF config automatically based on the feature\_tm\_pcf status from LLD."

This is planned to be delivered in UCC 1.1 LFD2 delivery.

Comment by [Mats Persson](#) [ 2025-03-11 ]

During test of this by UCC I&V the same issue had been reported by this ticket: [UCCXFT-774](#) UCC1.1, commercial license, Impact in epg gpw apn configuration in PCX

Resolution for UC 1.1 being discussed in this ticket.

Comment by [Mats Persson](#) [ 2025-01-29 ]

Current requirements for UC 1.0/1.1 are

- it should be possible to order a UCC commercial system without Traffic Management and Secure Mobility Value packs. The result if this is that the license keys for CCPC and SC/SEPP are not delivered.
- All CNFs shall always be installed, irrespective of if all value pack are ordered / license keys are available

What has been missed in UCC 1.0 is

- verifying behavior of UCC at installation and runtime if one or two or the value packs are not included and corresponding license keys in CCPC or SC are not installed. Verification is planned to UCC 1.1.
- describing in the installation guide how to at deployment and system health check handle the case where one or more VP is not ordered and corresponding license keys in CCPC or SC are not installed. This is what can be done for this TR (taking into account feedback from the verification activities on the point above).

Comment by [Maxime Mathieu](#) [ 2024-12-18 ]

As Rajan's experience with Raytheon has demonstrated, there is currently no option to install UCC without CCPC, even though, as per section 5.2 of the UCC Product Package Description document, the license for CCPC is part of a "UCC Value Package" that Raytheon has not bought.

This is most probably something that was overlooked when CCPC was introduced to UCC 1.0, but this needs to be fixed for UCC 1.1.

There needs to be a way to enable/disable the installation of CCPC, possibly from the CIQ, i.e. a way to be able to differentiate from the configuration of Base Package versus Value Package licensing.

This issue needs to be discussed further at the TR Board and/or at the Requirement Board; if indeed the strategy is to offer Value Packages, the proper licensing options need to be reflected in the installation procedure/tools.

Link to UCC Product Package Description document at the bottom of the following page:

[Ultra Compact Core - Ericsson](#)

Comment by [Rajan Rajeshprasad Gupta](#) [ 2024-12-17 ]

PI find information

UCC PPD (Product Package Description): Link from E/// Portfolio page

<https://erilink.internal.ericsson.com/eridoc/erl/objectId/09004cffd4957060?docno=1%2F22103-FGM101198%2F1&option=download&format=msw12>

Installation Guide : Link from UCC CPI

Ultra Compact Core (UCC) 1.1 - Preliminary, Ericsson Internal Support

Add on configuration on SMF to skip sending traffic to CCPC [ Change in APN configuration ]:

```
config;epg pgw apn internet;  
no sbi pcf-enabled-4g;  
no user-profile-selection n7-profile default n7-1;  
commit;
```

[UCC\_PLM-169] Wrong links to EDA library in B&R UG in UCC 1.0 CPI Created: 2024-11-21 Updated: 2025-04-24 Resolved: 2025-04-24

Status:	Done
Project:	UCC_PLM
Component/s:	None
Affects Version/s:	None
Fix Version/s:	UCC Appliance 1.0.1

Type:	Bug	Priority:	Medium
Reporter:	Eric Fenger	Assignee:	Andrea Maio
Resolution:	Closed	Votes:	0
Labels:	CPI, UCC_Appliance_1.0.1		
Remaining Estimate:	0h		
Time Spent:	2h		
Original Estimate:	2h		

Sprint:	UCC XFT3 Sprint 2
Team/s:	UCC_XFT3
Requirement Status:	UCC Appliance 0.2.1 - UNCOVERED

#### Description

In [https://cpistore.internal.ericsson.com/elex?LI=EN/LZN7041198/1R1A&FN=4\\_1553-HSC901198\\_1Uen.A.html&DT=UCC++Backup+and+Restore+User+Guide](https://cpistore.internal.ericsson.com/elex?LI=EN/LZN7041198/1R1A&FN=4_1553-HSC901198_1Uen.A.html&DT=UCC++Backup+and+Restore+User+Guide) all links to EDA library in chapter 2.5 refer to EDA 2.17 library. UCA for UCC 1.0 is based on EDA 2.18, see also EDA library being included in UCC 1.0 CPI library.

#### Comments

Comment by Åsa Preuss [ 2025-04-24 ]

Shouldn't this ticket be labeled with Document?

We need it to make statistics.

BR Åsa

[UCC\_PLM-168] Security and Privacy User Guide allows the use of self-signed certificates Created: 2024-11-20 Updated: 2025-04-24 Resolved: 2025-04-24

Status:	Done
Project:	UCC_PLM
Component/s:	None
Affects Version/s:	UCC Appliance 1.0.0, UCC Appliance 1.0.1-rc1
Fix Version/s:	None

Type:	Bug	Priority:	High
Reporter:	Fredrik Gustavsson	Assignee:	Unassigned

<b>Resolution:</b>	Closed	<b>Votes:</b>	0
<b>Labels:</b>	UCC_Appliance_1.0.1		
<b>Remaining Estimate:</b>	Not Specified		
<b>Time Spent:</b>	Not Specified		
<b>Original Estimate:</b>	Not Specified		

<b>Issue Links:</b>	<b>Association</b>		
	Associates with	<a href="#">UCC_SM-16</a>	Change of CA
<b>Detected in phase:</b>	PDU		Done
<b>Severity_qmt:</b>	2- High		
<b>Found in Build:</b>	UCC Appliance 1.0.0		
<b>Requirement Status:</b>	UCC Appliance 0.2.1 - UNCOVERED		

#### Description

In the Security and Privacy User Guide, Rev "", 2024-09-23, Chapter 3.1.5, it states:

"It is strongly recommended that UCC systems avoid using self-signed certificates ..."

This statement is in violation of the overall security design of UCC, where self-signed certificates are not allowed.

The text must be rephased to reflect this.

#### Comments

Comment by [Åsa Preuss](#) [ 2025-04-24 ]

Shouldn't this ticket be labeled with Document?

We need it to make statistics.

BR Åsa

Comment by [Mirac Günes](#) [ 2024-12-11 ]

[Daniel Smith C](#) this will have to be re-adjusted since we now fully remove all self-signed certificates.

The suggestion is to remove the annotation or rephrase it to state that we are delivering our products without certificates and expect the customer to **provide or populate** UCC with their own certificates.

The question is however, have we decided for whether we will ask the customer for certificates and pre-stage in the Ericsson premises or pre-stage in the customer premises until we create a proper strategy and related instructions on how to pre-stage at the Ericsson premises?

E.g.,

- 1) Ask the customer for dummy certificates
- 2) Pre-stage at Ericsson premises and deliver to customers
- 3) The customer follows our well defined and verified instructions to replace all of the dummy certs with their own <--- **doesn't exist as of today**

[UCC\_PLM-167] [Investigate cloning procedure for UCC for field replacement purposes](#) Created: 2024-11-19 Updated: 2025-04-24 Resolved: 2025-04-24

<b>Status:</b>	Rejected
<b>Project:</b>	<a href="#">UCC_PLM</a>
<b>Component/s:</b>	None
<b>Affects Version/s:</b>	None
<b>Fix Version/s:</b>	None

<b>Type:</b>	Task	<b>Priority:</b>	Low
<b>Reporter:</b>	<a href="#">Fredrik Gustavsson</a>	<b>Assignee:</b>	<a href="#">Cheng-Jun Li</a>
<b>Resolution:</b>	Rejected	<b>Votes:</b>	0
<b>Labels:</b>	None		
<b>Remaining Estimate:</b>	Not Specified		
<b>Time Spent:</b>	Not Specified		
<b>Original Estimate:</b>	Not Specified		

<b>Team/s:</b>	UCC_PLM
<b>Description</b>	
<p>The MELA team has raised some questions related to how to clone a UCC system to keep as a spare unit for replacement in the field.</p> <p>Further details will be shared after the next meeting with them by <a href="#">Reema Sidhwani</a>.</p> <p>The initial work related to this task is to:</p> <ul style="list-style-type: none"> <li>• Investigate the possible types of cloning/spare keeping. This involves:           <ul style="list-style-type: none"> <li>◦ Full system (router + 2 CCD servers)</li> <li>◦ Partial system (e.g. one server). Can it be used as either CCD-A or CCD-B?</li> </ul> </li> <li>• Procedure to set up the cloned system</li> <li>• Licensing needs</li> </ul>	

#### Comments

Comment by [Fredrik Gustavsson](#) [ 2024-12-09 ]

From Nov 27:

The procedure involves the following steps, starting with a healthy UCC installation on server 1 and licensing in autonomous mode:

1. Reboot server 1 using an in-memory image
2. Mount an external volume (we need ~4TB space) and copy out the OS and k8s disks
3. Shut down server 1
4. Transfer the network cables from server 1 to server 2
5. Boot server 2 using an in-memory image
6. Mount the external volume and overwrite the disks with the server 1 images
7. Reboot server 2 and validate that CCD, k8s, CNF, licenses works

We estimate that we need about 2 weeks of work for this.

Also, due to the recabling dependency, it would be optimal to run this in the Montreal Studio environment.

Alternatively, we need to add work orders for recabling and for the restore after the concluded test, that will add lead-time.

Comment by [Cheng-Jun Li](#) [ 2024-12-03 ]

We (PLM tteam) had a meeting to discuss the options.

An alternative to use one of the Montreal studio lab UCC systems might be considered.

Frederik is talking to Daniel to see if this is possible possible.

This option is would facilitate things given its location.

Comment by [Cheng-Jun Li](#) [ 2024-11-25 ]

#### PLM brainstorm minute on UCC cloning

Approach based on method presented in [Cloning in CNIS study\\_Nov 2024.pptx](#)

My understanding of the method/procedure:

#### Assumptions:

\*\*

1. We have an installed, functioning UCC 2-servers system (UCC-A and UCC-B), with UC provisioned.
2. HW requirement:
3. One Backup Server with enough disk space to store backup data of a UCC server
4. 2 Cloned Servers (UCC-A-Clone and UCC-B-Clone), each will contain the resulting cloned data of UCC-A and UCC-B

\*\*

#### Procedure:

\*\*

For each UCC server (UCC-A and UCC-B), do:

{ Step-1: Prepare the Backup Server (ref: slide 13, prepare backup server step) Step-2: Perform entire disk backup to the Backup Server using \*\_Linux dd command\_\* (ref: slide 13, step 2, 3) Step-3: Restore (Clone) the backup server's disk on to the corresponding Clone Server (UCC-A-Clone or UCC-B-Clone) using \*\_Linux dd command\_\* (ref: slide 15 steps) }

We now have UCC-A-Clone/UCC-B-Clone, ready to replace UCC-A/UCC-B in case of need.

**TBD:**

The approach needs to be experimented and validated, with stepped approach:

First, experiment on a CCD only system (i.e. CCD without any CNF)

Then experiment on a CCD + 1 CNF system without UE provisioning

Then experiment on a CCD + all CNF system without UE provisioning

Then experiment on a CCD + all CNF system with UE provisioning

**Question/Concerns:**

Q: It's not entirely clear to me how exactly the .iso, the .img, PXE boot work together. My current understanding (which could be wrong):

1. PXE boot requires the EricssonCCD.x86\_64-xxxxxx.iso.
2. After we run Step-2 (backup) above, we will have a ucc-a.img/ucc-b.img which contains everything, that would replace the node.img in the steps describe in step 2 on slide 5. And, since this ucc-a/b.img contains already everything, step 4 on slide 6 would be unnecessary in our scenario.

Q: What's the main purpose of the clone? For fast recovery from system failure, or for speeding up deployment? In the latter case, it would require a change of the UCC product so that it would support S/W and configuration separation, i.e. a cloneable installed UCC system with generic config values that can be cloned, on which site specific config can be injected.

Q/C: At this point, we are unsure whether a bit-by-bit clone would really work on a different server (e.g. would license be valid on different HW? On the flip side, if it works, then how does E// ensure proper license control/payment to prevent unauthorized cloning). This needs to be experimented and validate.

Q/C: Additional cost is obviously a concern + the additional H/W delivery required for this and other alternative approaches.

Q/C: The cloning process (cloned server generation): is this done at the SI level or at the field after delivery; current assumption is that it's at the SI stage, then the cloned server will be shipped to the field (this is also the way thru which we can ensure proper license control).

**Possible alternative approaches (based on PLM brainstorm):**

Have a copy of the jumphost shipped together with the UCC system. In case of failure, use the jumphost to reinstall the failed UCC server.

(Ideally, this approach shall work with a backup solution which backup the CNF data that allows facilitate and speedup data restore.)

Comment by [Fredrik Gustavsson](#) [ 2024-11-25 ]

In a meeting with MELA this issue was discussed.

The background is primarily to cover disaster recovery (HW replacement) but could be extended to also facilitate faster/simpler roll-out.

Also, the cloning should be done at the SI and a simple (adapted for the field) restore procedure should take place after the swap out of the HW.

The ask is for PLM to test if cloning is possible.

[\[UCC\\_PLM-166\] Investigate local backup procedure and possible improvements](#) Created: 2024-11-19 Updated: 2025-03-11 Resolved: 2025-03-11

Status:	Rejected
Project:	<a href="#">UCC_PLM</a>
Component/s:	None
Affects Version/s:	None
Fix Version/s:	None

Type:	Task	Priority:	Low
Reporter:	Fredrik Gustavsson	Assignee:	Ahmed Elkhouly
Resolution:	Rejected	Votes:	0
Labels:	None		
Remaining Estimate:	Not Specified		
Time Spent:	Not Specified		
Original Estimate:	Not Specified		

Team/s:	UCC_PLM
---------	---------

#### Description

The MELA team has raised some questions related to the backup procedure for a locally managed UCC, i.e. not ENM.

Further details will be shared after the next meeting with them by [Reema Sidhwani](#).

The initial work related to this task is to:

- Determine how to perform a UCC backup to a remote system.  
This may result in several alternative procedures.
- Determine the complexity/time needed for performing this/these procedure/s
- Investigate possible improvements via changes in the procedures, additional scripting, or new requirements

#### Comments

Comment by [Reema Sidhwani](#) [ 2025-03-11 ]

Hi Ahmed, rejecting this ticket for the moment for cleaning up PLM Jira. As discussed this will go through the FR process.

Comment by [Fredrik Gustavsson](#) [ 2024-11-25 ]

[Ahmed Elkhouly](#), will prepare a MOP for this. I will put the PLM task on hold

<a href="#">[UCC_PLM-165] Intermediately ccrc-dns is not resolving query in Aachen1a setup (UCC1.0_RC2)</a> <small>Created: 2024-11-19 Updated: 2025-03-11 Resolved: 2024-11-22</small>			
Status:	Done		
Project:	UCC_PLM		
Component/s:	None		
Affects Version/s:	UCC Appliance 1.0.0-rc2, UCC Appliance 1.0.0		
Fix Version/s:	None		

Type:	Bug	Priority:	High
Reporter:	<a href="#">Akshaya Avin Shetty</a>	Assignee:	Unassigned
Resolution:	Closed	Votes:	0
Labels:	None		
Remaining Estimate:	Not Specified		
Time Spent:	Not Specified		
Original Estimate:	Not Specified		

Attachments:	<a href="#"></a> dnslog.txt <a href="#"></a> image-2024-11-21-15-38-08-090.png <a href="#"></a> image-2024-11-21-15-38-54-544.png <a href="#"></a> logs_ccrc_2024-11-20-09-59-48.tgz <a href="#"></a> PM-165-nrf-dns-logs-2
Defect code_qmt:	1- Functional
Sprint:	UCC XFT2 Sprint 2
Team/s:	UCC_XFT2
Severity_qmt:	2- High
Found in Build:	UCC Appliance 1.0.0-rc2
Requirement Status:	UCC Appliance 0.2.1 - UNCOVERED

#### Description

We are observing out of 5 times, 3-4 times CCRC-DNS is unable to resolve the FQDN. Because of that calls are failing. Sometimes UDM FQDN resolution fails and sometimes PCF FQDN resolution fails

```
eccc@ucc-ccda:~> dig udm-ccsm-deacucc1a.5gc.mnc099.mcc244.3gppnetwork.org  
net.c:537: probing sendmsg() with IPV6_TCLASS=b8 failed: Network is unreachable
```

```
; <>> DiG 9.16.48 <>> udm-ccsm-deacucc1a.5gc.mnc099.mcc244.3gppnetwork.org  
; global options: +cmd  
; Got answer:  
;=>>HEADER<- opcode: QUERY, status: NXDOMAIN, id: 9329  
; flags: qr aa rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 1  
  
; OPT PSEUDOSECTION:  
; EDNS: version: 0, flags: udp: 4096  
; COOKIE: 4d066b9054a12048 (echoed)  
; QUESTION SECTION:  
;udm-ccsm-deacucc1a.5gc.mnc099.mcc244.3gppnetwork.org. IN A  
  
; AUTHORITY SECTION:  
5gc.mnc099.mcc244.3gppnetwork.org. 604800 IN SOA ns1.mnc099.mcc244.3gppnetwork.org. admin.mnc099.mcc244.3gppnetwork.org. 1 604800 604800 1209600 604800  
  
; Query time: 0 msec  
; SERVER: 10.96.0.10#53(10.96.0.10)  
; WHEN: Tue Nov 19 11:50:32 UTC 2024  
; MSG SIZE rcvd: 230
```

```
eccc@ucc-ccda:~> dig pcf-pcx-deacucc1a.5gc.mnc099.mcc244.3gppnetwork.org  
net.c:537: probing sendmsg() with IPV6_TCLASS=b8 failed: Network is unreachable
```

```
; <>> DiG 9.16.48 <>> pcf-pcx-deacucc1a.5gc.mnc099.mcc244.3gppnetwork.org  
; global options: +cmd  
; Got answer:  
;=>>HEADER<- opcode: QUERY, status: NXDOMAIN, id: 19717  
; flags: qr aa rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 1  
  
; OPT PSEUDOSECTION:  
; EDNS: version: 0, flags: udp: 4096  
; COOKIE: 964f86c24e4d81b8 (echoed)  
; QUESTION SECTION:  
;pcf-pcx-deacucc1a.5gc.mnc099.mcc244.3gppnetwork.org. IN A  
  
; AUTHORITY SECTION:  
5gc.mnc099.mcc244.3gppnetwork.org. 604800 IN SOA ns1.mnc099.mcc244.3gppnetwork.org. admin.mnc099.mcc244.3gppnetwork.org. 1 604800 604800 1209600 604800  
  
; Query time: 0 msec  
; SERVER: 10.96.0.10#53(10.96.0.10)  
; WHEN: Tue Nov 19 11:47:50 UTC 2024  
; MSG SIZE rcvd: 229
```

#### Comments

Comment by [Alvaro Martin](#) [ 2024-11-22 ]

I've updated our working Deployment Guideline to improve in chapter 15.2.1 the way to verify CCRC DNS data is properly replicated between CCRCs.

I close the ticket as the issue is fixed and clarified now.

Comment by [Alvaro Martin](#) [ 2024-11-21 ]

Hi Rajan,

now that you mentioned, I remember some time ago I did a manual re-sync in deacucc3, it failed also. Then I tried once more time and it worked, without any other interver mention.

Did you try to re-attempt the re-sync before cleaning+adding entries?

For the second point, yesterday I forgot to mention something I saw which was wrong but now it is corrected. The Match client IP in one of the views (I think it was ccdb view) was wrong: the network started by 72 instead of 172. Now I see it's corrected.

As the matching client network was wrong that view would never match (ccdb) so all the queries would go to ccda.

Comment by [Rajan Rajeshprasad Gupta](#) [2024-11-21]

Hello Alvaro,

Thank you for feedback.

you are right few entries of ccda was missing in ccdb ccrc-dns.

allow me to ask 2 more queries

1. I notice without adding entries manual re-sync failed. Is this normal?

see error as below;

```
ccrcoam@ccrc-ccdb#show nrf common geo-red progress-report 19699
Thu Nov 21 07:05:18.199 UTC+00:00
nrf common geo-red progress-report 19699
action-name      resync
additional-info   [ "action ID of TOUCHALL: 4b75ecba-68e4-4c01-93d1-63eb7bea8720\\nd != java.lang.String" ]
progress-info    "Synchronizing databases to other sites"
progress-percentage 100
result          failure
state            finished
time-action-started 2024-11-21T07:02:52.79038-00:00
time-action-completed 2024-11-21T07:04:10.253081-00:00
time-of-last-status-update 2024-11-21T07:04:10.253069-00:00
```

Only after cleaning+adding all entries re-sync started working in ccdb-ccrc.

```
ccrcoam@ccrc-ccdb#show nrf common geo-red progress-report 28697
nrf common geo-red progress-report 28697
action-name      resync
additional-info   [ "action ID of TOUCHALL: 80b71199-4b87-4f41-8d4b-8fd602c5fca3" ]
progress-info    "Synchronizing databases to other sites"
progress-percentage 100
result          success
state            finished
time-action-started 2024-11-21T08:21:32.793174-00:00
time-action-completed 2024-11-21T08:23:25.281878-00:00
time-of-last-status-update 2024-11-21T08:23:25.281863-00:00
ccrcoam@ccrc-ccdb#
ccrcoam@ccrc-ccdb#
```

2. I see from CCDA PCC-MME, NAPTR queries were always going to CCRC-DNS of CCDB. Is this expected(cross server).

Reasoning, I see In PCC-MME we dont have any priority so based on higher IP address, PCC-MME is sending all queries to CCDB CCRC-DNS. and as some DNS entries for CCDB selecting PGW/SGW of CCDB.

See below:

```
system-admin@pcx-ccda#mm gw test-gw-selection mobile-country-code 244 mobile-network-code 99 tracking-area-code 611 access-point-4.gprs
gw-selection-test {
  gw-selection-test-result
  sgw-ipv4-address 172.16.3.10
  pgw-ipv4-address 172.16.3.9
  s8-protocol gtp
  num-of-candidate-pairs 1
  sgw-pgw-candidate-pairs
  Sgw : topoff.s4s11.sgw-pcx-deacucc1b.nodes.epc.mnc099.mcc244.3gppnetwork.org.
  Pgw : topoff.s5.pgw-pcx-deacucc1b.nodes.epc.mnc099.mcc244.3gppnetwork.org.

  note The candidate list is sorted from the highest to the lowest priority. The gateway status are not considered here.
  To avoid too much printout, 30 pairs are displayed by default. To print more or less pairs, use option num-of-result.
}
```

After correcting entries: We started getting 4 candidate with correct PGW/SGW selection.

```

system_admin@pcx-ccda#mm toolbox dns-support clear-cache
system_admin@pcx-ccda#
system_admin@pcx-ccda#
system_admin@pcx-ccda#mm gw test-gw-selection mobile-country-code 244 mobile-network-code 99 tracking-area-code 611 access-poi
gprs
gw-selection-test {
    gw-selection-test-result
    sgw-ipv4-address 172.16.2.10
    pgw-ipv4-address 172.16.2.9
    s8-protocol gtp
    num-of-candidate-pairs 4
    sgw-pgw-candidate-pairs
    Sgw : topon.s4s11.sgw-pcx-deacuccla.nodes.epc.mnc099.mcc244.3gppnetwork.org.
    Pgw : topon.s5.pgw-pcx-deacuccla.nodes.epc.mnc099.mcc244.3gppnetwork.org.

    Sgw : topoff.s4s11.sgw-pcx-deacucclb.nodes.epc.mnc099.mcc244.3gppnetwork.org.
    Pgw : topoff.s5.pgw-pcx-deacucclb.nodes.epc.mnc099.mcc244.3gppnetwork.org.

    Sgw : topoff.s4s11.sgw-pcx-deacucclb.nodes.epc.mnc099.mcc244.3gppnetwork.org.
    Pgw : topon.s5.pgw-pcx-deacuccla.nodes.epc.mnc099.mcc244.3gppnetwork.org.

    Sgw : topon.s4s11.sgw-pcx-deacuccla.nodes.epc.mnc099.mcc244.3gppnetwork.org.
    Pgw : topoff.s5.pgw-pcx-deacucclb.nodes.epc.mnc099.mcc244.3gppnetwork.org.

note The candidate list is sorted from the highest to the lowest priority. The gateway status are not considered here.
      To avoid too much printout, 30 pairs are displayed by default. To print more or less pairs, use option num-of-result.
}

```

Comment by Alvaro Martin [2024-11-20]

Hi,

I've been checking status of both CCRCs in deacucc1 and I see CCRC DNS data is not synchronized between both NRFs and CCRC DNS in ccdb is missing ccda FQDNs.

This means that queries getting into CCRC-DNS in ccdb to resolve ccda FQDNs will fail.

As coredns is configured to send queries to both CCRC DNS, that's why:

- Some of the ccda FQDN queries are failing (the ones to be resolved by CCRC DNS ccdb)
- Some of the ccda FQDN queries are successful (the ones to be resolved by CCRC DNS ccda)
- All the ccdb FQDN queries are successful (all FQDNs are defined in both CCRC DNS)

coredns config:

```

5gc.mnc099.mcc244.3gppnetwork.org:53
{ errors loop forward . *172.16.2.73* *172.16.3.73* }
epc.mnc099.mcc244.3gppnetwork.org:53 { errors loop forward . *172.16.2.73* *172.16.3.73* }

```

Exporting A-Records from CNOM in both CCRC DNS you can see that CCRC-DNS ccdb only holds ccdb FQDNs while CCRC-DNS ccda holds both, ccda and ccdb FQDNs.

Also you can see that both CCRC do not hold same DNS info by running the step 4 in chapter 15.2.2 (Synchronize Data between sites) from Deployment guideline.

I'll add this procedure also in previous chapter so it's easier to verify the correct replication and take actions accordingly.

This is the summary of the execution of this procedure in CCRC ccda and ccdb:

ccda:

**nrf common kvdb-service show-status**

action-state running

action-id **29811**

**show nrf common kvdb-service progress-report 29811**

Command: `query --query="SELECT COUNT★ FROM /%s\"`

Output:

**ericsson-nrf-dns-address-groups: 11**

**ericsson-nrf-dns-nfprofiles: 12**

ericsson-nrf-dns-rootservers: 0

ericsson-nrf-dns-snssaiutinfo: 0

ericsson-nrf-dns-views: 2

ericsson-nrf-dns-zones: 3

ericsson-nrf-gpsigroupprofiles: 0

ericsson-nrf-gpsiprofiles: 0

ericsson-nrf-multisiteinfo: 2

ericsson-nrf-nfheartbeat: 12

ericsson-nrf-nfprofiles: 12

ericsson-nrf-nrfaddresses: 0

ericsson-nrf-nrfprofiles: 0

ericsson-nrf-policies: 0

ericsson-nrf-policylocators: 0

ericsson-nrf-regioncustommninfo: 0

```
ericsson-nrf-regionninfo: 0
ericsson-nrf-regionversion: 1
ericsson-nrf-rules: 0
ericsson-nrf-sic-subscriptions: 0
ericsson-nrf-subscriptions: 139
ericsson-nrf-supigroupprofiles: 0
ericsson-nrf-supiprofiles: 0
ericsson-nrf-witnessinfo: 0
```

ccdb:

**nrf common kvdb-service show-status**

action-state running  
action-id **780**

**show nrf common kvdb-service progress-report 780**

Command: 'query --query=\"SELECT COUNT★ FROM /%s\"'

Output:

**ericsson-nrf-dns-address-groups: 2**

**ericsson-nrf-dns-nfprofiles: 6**

ericsson-nrf-dns-rootservers: 0

ericsson-nrf-dns-snssaiutinfo: 0

ericsson-nrf-dns-views: 2

ericsson-nrf-dns-zones: 3

ericsson-nrf-gpsigroupprofiles: 0

ericsson-nrf-gpsiprofiles: 0

ericsson-nrf-multisiteinfo: 2

ericsson-nrf-nfheartbeat: 12

ericsson-nrf-nfprofiles: 12

ericsson-nrf-nraddresses: 0

ericsson-nrf-nfpprofiles: 0

ericsson-nrf-policies: 0

ericsson-nrf-policylocators: 0

ericsson-nrf-regioncustomninfo: 0

ericsson-nrf-regionninfo: 0

ericsson-nrf-regionversion: 1

ericsson-nrf-rules: 0

ericsson-nrf-sic-subscriptions: 0

ericsson-nrf-subscriptions: 139

ericsson-nrf-supigroupprofiles: 0

ericsson-nrf-supiprofiles: 0

ericsson-nrf-witnessinfo: 0

In order to fix this misalignment, please execute **15.2.2 Synchronize Data Between Sites** in Deployment Guideline.

---

Comment by [Akshaya Avin Shetty](#) [ 2024-11-20 ]

Data collector logs for ccrc and dns pods logs are attached for reference

---

Comment by [Fredrik Gustavsson](#) [ 2024-11-19 ]

This was reproduceable using other commands as well, e.g. ping, nslookup.

We will redirect the ticket to a design team.

---

[UCC\_PLM-163] UCC 1.0 : cCNOM 2.1 In the UE trace call flow, we see broken icons? Created: 2024-11-18 Updated: 2025-04-14 Resolved: 2025-04-14

Status:	Done
Project:	<a href="#">UCC_PLM</a>
Component/s:	None
Affects Version/s:	None
Fix Version/s:	None

Type:	Bug	Priority:	Medium
Reporter:	<a href="#">Rajan Rajeshprasad Gupta</a>	Assignee:	<a href="#">Christos Delis (EXT)</a>

<b>Resolution:</b>	Closed	<b>Votes:</b>	0
<b>Labels:</b>	UCC-CNOM		
<b>Remaining Estimate:</b>	Not Specified		
<b>Time Spent:</b>	Not Specified		
<b>Original Estimate:</b>	Not Specified		

<b>Attachments:</b>	
<b>Team/s:</b>	UCC_XFT3
<b>Severity_qmt:</b>	3- Medium
<b>Found in Build:</b>	UCC Appliance 1.0.0
<b>Requirement Status:</b>	UCC Appliance 0.2.1 - UNCOVERED

### Description

Hello,

Please refer ticket raise for general cCNOM problem reported during ATnT Customer Demo.

[cCNOM 2.1 In the UE trace call flow, we see broken icons? - ELS - Service project](#)

Fix from CNOM in CNOM Server 2.18.0 release.

Support needed to know which UCC release we can expect release inclusion of CNOM Server release.

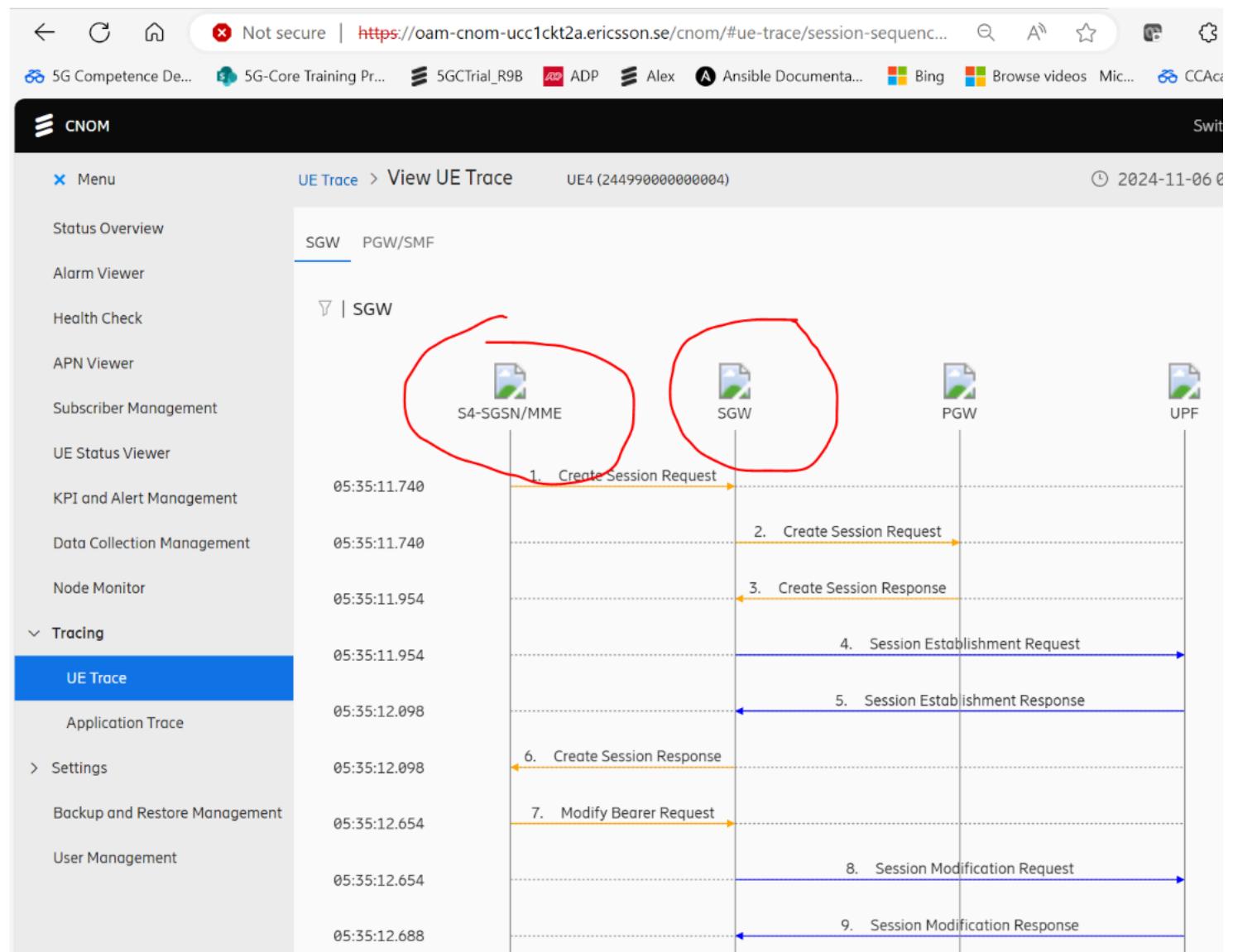


image.png

## Comments

Comment by [Rajan Rajeshprasad Gupta](#) [ 2025-04-14 ]

Thank you Christos Delis (EXT)

Please close ticket.

Comment by [Christos Delis \(EXT\)](#) [ 2025-04-14 ]

Hello [Rajan Rajeshprasad Gupta](#),

Yes on CNOM 2.2 is already resolved as it shown on below figures:



Am closing this ticket.

Thanks in advance.

Brs,

Christos

Comment by [Rajan Rajeshprasad Gupta](#) [ 2025-04-14 ]

Hello [Christos Delis \(EXT\)](#),

I dont have system to verify on CNOM 2.2 as we have not received software yet for UCC 1.1 for SDU service readiness testing.

Can you test on UCC 1.1 which will use CNOM 2.2? If you dont see problem, then we can close this ticket.

Comment by [Christos Delis \(EXT\)](#) [ 2025-04-14 ]

Hello,

Is it still ongoing? Could we close it?

Thanks in advance.

BRs,

Christos

Comment by [Rajan Rajeshprasad Gupta](#) [ 2024-11-27 ]

Perfect, Thank you Christos.

Comment by [Christos Delis \(EXT\)](#) [ 2024-11-27 ]

Hello Rajan,

Yes i saw that you invite me as a Participant.. i saw the last response.

From CNOM 2.2, from above screenshot which i shared looks that 2.18 version of cnom server is introduced.

Then we can verify and close it on CNOM 2.2 verification.

BRs,

Christos

Comment by [Rajan Rajeshprasad Gupta](#) [ 2024-11-27 ]

Hello Cristos,

Yes, I am not sure if you can open ELS ticket open to CNOM PDU. CNOM PDU analyzed case and come for software fix.

Pasting a snap here.

https://pdupc-jira.internal.ericsson.com/servicedesk/customer/portal/15/PCELS-33844

5G-Core Training Pr... 5GCTrial\_R9B ADP Alex Ansible Documenta... Bing Browse

Packet Core Service Center / ELS / PCELS-33844  
cCNOM 2.1 In the UE trace call flow, we see broken icons?

Comment on this request...

**CLOSED**  Don't notify me

Request participants

Rajan Rajeshprasad Gupta Creator

Christos Delis (EXT) Remove

Anchal Sharma A Remove

Matthew Gimlin Remove

Debajit Mitra Remove

Rishita Shankar Remove

MA 5GC Hubs Remove

Activity

Your request status changed to **Closed** with resolution **Done**. 2024-11-19 09:46 **LATEST**

Aram Rassool 2024-11-19 09:43  
Hi Rajan Rajeshprasad Gupta,

The fix will be added to cCNOM 2.2. I'll close this ticket now.

**FSA - Fault Slippage Analysis**

**Root Cause Analysis (RCA):**

The difference between my local environment and Rajan's hosted environment is how the image link is referenced in the code.

In my local environment, the HTML image tag references a *relative path* (note the "..../../."):

```
<image xlink:href="....../resources/sequenceDiagram/images/mme.png" x="-14" height="40" width="28"></image>
```

But in the hosted environment, the HTML tag uses an *absolute path* (without the "..../../.") and it can't find the image:

```
<image xlink:href="https:<URL>/resources/sequenceDiagram/images/mme.png" x="-14" height="40" width="28"></image>
```

This is likely due to the difference in the built CNOM package directory structure (compared to the local environment).

**Resolution details:** Changing the URL to an absolute path rather than a relative.

**Reason for Slippage / Should have been found in:** Code reviews and manual exploratory testing.

**Preventive action:** Not using relative paths and exploratory testing to ensure images load correctly.

BR,  
Aram

Comment by Christos Delis (EXT) [2024-11-27]

Hello Rajan,

Need to clarify some things about that ticket.

From description i see that this issue will be fixed in CNOM server 2.18.0 release. How did you get that info? Have you cross checked that info with CNOM PDU? Checking now the new release of CNOM 2.2 which will be applicable on UCC 1.1, see that the delivered version of CNOM server is 2.18.0:

```
productname: "CNOM Server Helm Chart"
productnumber: "CND 101 194"
images:
  server:
    productname: "CNOM Server Image"
    productnumber: "CND 101 1156"
    registrator: "cnom-server.nero.gic.ericsson.se"
    name: "proj-pc-cs-test"
    tag: "2.18.0-h20257ad"
```

BRs,  
Christos

[UCC\_PLM-162] UCC CP1 : II section 12.2.6 example CLI not working Created: 2024-11-15 Updated: 2025-04-23 Resolved: 2025-04-23

Status:	Done
Project:	UCC_PLM
Component/s:	None
Affects Version/s:	None
Fix Version/s:	None

Type:	Bug	Priority:	Low
Reporter:	Rajan Rajeshprasad Gupta	Assignee:	Unassigned
Resolution:	Closed	Votes:	0
Labels:	None		
Remaining Estimate:	Not Specified		
Time Spent:	Not Specified		
Original Estimate:	Not Specified		

Attachments:	
Team/s:	UCC_XFT2
Severity_qmt:	4-Low/Cosmetic
Found in Build:	UCC Appliance 1.0.1
Requirement Status:	UCC Appliance 0.2.1 - UNCOVERED

#### Description

Hello,
CP1 Installation Instruction section 12.2.6 example CLI not working
ucc@ucc-jumphost:~\$
ucc@ucc-jumphost:~\$
ucc@ucc-jumphost:~\$ export USER=eccd
export CLUSTER=ccdb
ssh -o ServerAliveInterval=60 \
\$USER@\$(cat \$config_dir/config/templates/site-global-ucc.yaml \
yq eval '.network.'\$CLUSTER'.ccd.ccd_oam.ipassignment \
.ccd_control_plane_external_vip' \
-)
Error: 1:40: invalid input text "\\\n
.ccd_control..."
ssh: Could not resolve hostname : Name or service not known
ucc@ucc-jumphost:~\$

#### Comments

Comment by Arron Kuang [ 2024-11-25 ]
Reported issue should be in section 10, step 3.
Updated the command.

[UCC\_PLM-161] UCC1.0 Netrunner subscriber view does not show APN Created: 2024-11-14 Updated: 2025-04-29 Resolved: 2025-04-29

Status:	Done
Project:	UCC_PLM
Component/s:	None
Affects Version/s:	UCC Appliance 1.0.0-rc2
Fix Version/s:	None

Type:	Bug	Priority:	Medium
Reporter:	Rishi Shekhar	Assignee:	Christos Delis (EXT)
Resolution:	Closed	Votes:	0

<b>Labels:</b>	UCC_Appliance_1.1.0
<b>Remaining Estimate:</b>	8h
<b>Time Spent:</b>	Not Specified
<b>Original Estimate:</b>	8h

<b>Attachments:</b>	
<b>Sprint:</b>	UCC XFT3 Sprint 2
<b>Detected in phase:</b>	Production
<b>Team/s:</b>	UCC_XFT3
<b>Severity_qmt:</b>	3- Medium
<b>Found in Build:</b>	UCC 1.0
<b>Requirement Status:</b>	UCC Appliance 0.2.1 - UNCOVERED

#### Description

UCC1.0 Netrunner & CNOM subscriber view does not show APN information.

#### Description

The Jason body of UE status viewer has an APN field, but shows empty string

```
{ "IMSI": "24499000000101", "Details status": "Not collected", "MSISDN": "86081000000101", "IMEI": "12340000005510", "Location": "244-99-50-12513024", "Radio access type": "5G", "Status": "Registered", "Name": "-", "APNs": "-" }
```

#### Component/s

UCC



#### Comments

Comment by Christos Delis (EXT) [ 2025-04-29 ]

Hello Jim Dumont,

Issue is related with the following one: <https://eteamproject-alpha.internal.ericsson.com/browse/CNOM-20298>, which will be fixed on next version of CNOM 2.3. Am setting current ticket with FIX AVAILABLE status.

BRs,  
Christos

Comment by Jim Dumont [ 2025-04-28 ]

Christos Delis (EXT) - is this bug still an issue or a CNOM fix was delivered? It's 'in progress' but perhaps it:

- 1) should be blocked if still waiting on fix, or
- 2) set to FIX AVAILABLE if finally there is a fix, or
- 3) cancelled if no longer reproducible for UCC 1.1?

Comment by Rajan Rajeshprasad Gupta [ 2025-01-16 ]

Update: Information shared to Qiang Zhang for required screen print to clarify.

Comment by Soner Mus [ 2024-12-12 ]

work is ongoing, it will be extend to Sprint #3.

Comment by Christos Delis (EXT) [ 2024-12-11 ]

Info has been shared with CNOM PDU via email.

Waiting for response.

Comment by Jim Dumont [ 2024-11-22 ]

Waiting for CNOM bug fix.

Comment by Mats Persson [ 2024-11-19 ]

Shouldn't this ticket be assigned to team XFT3 (Christos) or XFT2 (Rishi) instead of XFT1?

Comment by Rishi Shekhar [ 2024-11-14 ]

CU ticket for the same- <https://eteamproject.internal.ericsson.com/servicedesk/customer/portal/710/UCCSUPPORT-39>

<b>Status:</b>	Done
<b>Project:</b>	UCC_PLM
<b>Component/s:</b>	None
<b>Affects Version/s:</b>	UCC Appliance 0.2.2
<b>Fix Version/s:</b>	None

<b>Type:</b>	Bug	<b>Priority:</b>	Critical
<b>Reporter:</b>	Rishi Shekhar	<b>Assignee:</b>	Unassigned
<b>Resolution:</b>	Closed	<b>Votes:</b>	0
<b>Labels:</b>	None		
<b>Remaining Estimate:</b>	Not Specified		
<b>Time Spent:</b>	Not Specified		
<b>Original Estimate:</b>	Not Specified		

<b>Attachments:</b>	<a href="#">ECCD-A_ccdm_ccsm hc.txt</a>	<a href="#">ECCD-A_CCRC.txt</a>	<a href="#">ECCD-A_ccsm hc.txt</a>	<a href="#">ECCD-B_CCRC.txt</a>	<a href="#">EventLog_UCCA.csv</a>	<a href="#">EventLog_UCCB.csv</a>	<a href="#">image-2024-11-14-20-23-11-532.png</a>	<a href="#">image-2024-11-22-16-20-08-013.png</a>	<a href="#">show alarm history UCC-A.txt</a>	<a href="#">show alarm history UCC-B.txt</a>	<a href="#">Tef-Document-Database-doutput.csv</a>	<a href="#">uptime-ccda_12112024.JPG</a>	<a href="#">uptime-ccdb_12112024.JPG</a>
<b>Detected in phase:</b>	Production												
<b>Team/s:</b>	UCC_PLM												
<b>Severity_qmt:</b>	1- Critical												
<b>Found in Build:</b>	UCC Appliance 0.2.2												
<b>Requirement Status:</b>	UCC Appliance 0.2.1 - UNCOVERED												

#### Description

Hi Team,

Observed Issue:- All CCXX nodes lost LKFs in Autonomous mode.

Customer Telefonica  
UCC Release- 0.2.2  
Nels - Autonomous mode

4G calls working fine but all 5G calls impacted here.

Impact:- NRF management services & Discovery not working as functionailty disabled impacting 5G calls due to license issue.

Impacted Node:- CCRC, CCSM, CCDM

```

eccd@ucc-ucc1b:~> kubectl exec -it -n ccrc $(kubectl get po -n ccrc | grep -i eric-nrf-discovery | awk 'NR==1 {print $1}') -- curl -w "\n" --header "Content-Type: application/json" --request GET http://eric-lm-combined-server:8080/license-manager/api/v1/licenses --data '{"productType":"CCRC"}' | jq .
{
  "operationalStatusInfo": {
    "operationalMode": "AUTONOMOUS",
    "autonomousModeDuration": 1295660
  },
  * "licensesInfo": []
}

eccd@ucc-ucc1a:~> kubectl exec -it -n ccsn $(kubectl get po -n ccsn | grep -i eric-nrf-discovery | awk 'NR==1 {print $1}') -- curl -w "\n" --header "Content-Type: application/json" --request GET http://eric-lm-combined-server:8080/license-manager/api/v1/licenses --data '{"productType":"CCSN"}' | jq .
{
  "operationalStatusInfo": {
    "operationalMode": "AUTONOMOUS",
    "autonomousModeDuration": 1375018
  },
  * "licensesInfo": []
}

ccrcoam@ucc1a-ccrc#show alarm
nrfMngtNFsuspended
      active   severity       MinNon

```

Ungraceful reboot of cluster observed in both the cluster. Pls refer the attached snapshot. Checked with customer they don't know how this happened.

They insist this was not done from Power off since last 2-3 weeks.

From DB pod (eric-data-document-database-pg-0) in ccrc- we checked the license status from postgres dB & don't see any license being activated as well. Attached the same in csv file as well.

ADP logs for CCRC attached for detailed analysis.

Pls let me know if any other logs needed.

\*\*NOTE:- This is important from Telefonica Delivery perspective- as per CCXX CPI understanding once license is fetched from the Nels by LM-pods then this should be persistently stored in CCXX DBs. \*\*

## Comments

Comment by [Zhigang Han](#) [ 2024-12-10 ]

Hi team,

The root cause analysis has shared with the customer. We are closing the ticket.

Thanks,

BR/Zhigang

Comment by [Zhigang Han](#) [ 2024-12-05 ]

hi Rishi,

Please let us know if we could close the ticket soon?

Thanks,

BR/zhicang

Comment by [Zhigang Han](#) [ 2024-12-02 ]

hi Rishi,

Here is the procedure how to remove grace period alarm:

### Solution

1, Check if the License Manager Autonomous Mode Activated alarm is active.

The Alarm is... Action

Active Resolve the License Manager Autonomous Mode Activatedalarm before continuing with the next step.

Not Active Continue with the next step.

2, Contact NeLS to check if the license keys were attempted to be removed intentionally.

License Keys were Removed... Action

**Intentionally No further action is needed. Wait until the grace period ends, and the alarm clears automatically.**

**Unintentionally Continue with the next step.**

3, Order a new License Key File (LKF) from Ericsson that contains the missing license key data.

4, Contact NeLS to restore the LKF on NeLS.

5, Once the LKF is restored on NeLS, check the alarm again. If it is not cleared, restart the license management pods.

### Example

```
kubectl get pods --namespace <pod_namespace>
```

```
kubectl get pod <pod_name> --namespace <pod_namespace> -o yaml | kubectl replace --force -f -
```

6, If the alarm is not cleared, collect the logs related to license management, and contact the next level of support.

There will be one grace period alarm for each LKF, so please check the grace period alarm carefully. I do believe for Telefonica issue, some of grace period alarms are intentional LKFs, we should not have any grace period alarms. Unfortunately it is not the case for CCSM/CCRC. I believe CCDM has no grace period alarms for new LKFs or maybe the grace period for new LKFs was not expired on Nov 12th 2024, however for CCDM, 4 out of 5 LKFs were expired on Nov 9th, 2024 before the issue was reported.

thanks,

BR/Zhigang

Comment by [Zhigang Han](#) [ 2024-11-29 ]

hi Rishi,

From CCSM adp log, I could see there is grace period alarm activated and also on Nov 12th, the grace period alarm was expired:

```
{"version":"1.2.0","timestamp":"2024-11-12T12:48:20.814+00:00","severity":"info","service_id":"eric-lm-combined-server","message":"Deleted from cache: LicenseKey{id=31, productType=CCSM, licensId=FAT1024210/10, licenseType=2, start=2024-10-07 22:00:00 +0000 UTC, stop=2025-04-05 22:00:00 +0000 UTC, capacity=1000000, gracePeriodLength=9, periodStart=0, growOnly=false} slwtID=UME_TRIAL_CCSM2, customerID=941903, lastUpdateTime=1729597749176, description=[CCSM HSS-EPC mIoT Ba Package]}", "metadata":{"function":"gerrit.ericsson.se/adp-gs/adp-gs-lm/internal/persistence.(inMemoryCacheImpl).deleteLicenseKey","proc_id":"1","pod_name":"eric-lm-cc-license-consumer-handler-6b476d79drhgk!","container_name":"eric-lm-license-consumer-handler"}}
```

that is why CCSM behaved the similar situation as CCRC with no license keys.

From CCDM adp log, I donot see any grace period alarm was expired on Nov 12th, however I do see there were 5 license keys loading from repository (the only one license 20250405 and the remaining four license keys were expired on Nov 9th).

```
{"version":"1.2.0","timestamp":"2024-11-11T08:34:53.422+00:00","severity":"info","service_id":"eric-lm-combined-server","message":"[LicenseKeys]Trying to parse the row LicenseKey{id=343, productType=CCDM, licenseld=FAT1024200/56, licenseType=1, start=2024-05-13 22:00:00 +0000 UTC, stop=2024-11-09 23:00:00 +0000 UTC, capacity gracePeriod=1730807829562, periodLength=-1, periodStart=-1, growOnly=false} slwtID=, customerID=, lastUpdateTime=-1, description=[]}","metadata":{"function":"gerrit gs/adp-gs-lm/internal/persistence.(RepositoryImpl).FetchLicenseKeys(*)","proc_id":"1","pod_name":"eric-lm-combined-server-license-consumer-handler-5d8c94b8cs2rdw","container_name":"eric-lm-license-consumer-handler"}}
```

for CCDM, grace period alarm was not expired on Nov 12th, but 4 out 5 LFKs were expired on Nov 12th.

#### **conclusion from CCSM/CCDM is NeLS server activity was not succeed which caused license issue on UCC side**

Here is the root cause analysis about the issue:

- 1, NeLS server side activity did not succeed, which caused UCC-side raised grace period alarm
- 2, We should clear the grace period alarm before we continue with the NeLS server side activity. Unfortunately we completed the NeLS server side activity during the UCC-side alarm
- 3, The NeLS server was going on/off repeatedly for Telefonica UCC solution
- 4, Due to the NeLS server instability, the UCC-side was cycling in/out of autonomous mode all the time
- 5, On Nov 12th, the grace period expired, and CNFs deleted all license keys from the cache. On that day, the NeLS server was unreachable or unable to provide the correct license keys
- 6, Without valid licenses, traffic failed

the suggestions from PLM side:

- 1, Any activity from NeLS-side should not raise any alarm if it is done correctly. We need to check the alarms before and after any activity. If there is grace period alarm raise address the alarm before we close the activity.
- 2, The Telefonica NeLS server is really not stable. Here is one suggestion: Once the UCC CNFs have all valid license keys, we could disable the NeLS server connection and let it run in autonomous mode. We could activate NeLS service when we need to perform license upgrade or UCC upgrade etc.

if customer has no further questions, please let us know if we could close this ticket.

Thanks,

BR/Zhigang

---

Comment by [Rishi Shekhar](#) [ 2024-11-28 ]

Hi Zhigang Han Pls fine the SP link for CCSM & CCDM adp logs.

[https://ericsson-my.sharepoint.com/:u/p/rishi\\_shekhar/Ea2R3PlcpyNjtRnYx8KQKQQBmJuF81AEN\\_i11N09haAwdQ?e=SIGcS4](https://ericsson-my.sharepoint.com/:u/p/rishi_shekhar/Ea2R3PlcpyNjtRnYx8KQKQQBmJuF81AEN_i11N09haAwdQ?e=SIGcS4)

---

Comment by [Zhigang Han](#) [ 2024-11-22 ]

Thanks Rishi!

---

Comment by [Rishi Shekhar](#) [ 2024-11-22 ]

Hi Zhigang..

We didnt received any logs till now. Customer visit to Datacenter is not planned yet. Will soon share the logs once received it from telefonica,

---

Comment by [Zhigang Han](#) [ 2024-11-22 ]

Hi Rishi,

Could you also upload ccsm/ccdm ADP? I would like to see what is the issue for ccsm/ccdm.

Thanks,

BR/Zhigang

---

Comment by [Zhigang Han](#) [ 2024-11-22 ]

Thanks Rishi!

probably NeLs server activity was not done properly and also We didnot clear the grace period alarm before we moved to the next step.

The key is to make sure grace period alarm is cleared before we could continue the activity!

one thing: this NeLs server in Telefonica UCC solution was really not stable which caused license issues for UCC many times. Please ask CU to disable it and let ucc run in aut We could enable it when we perform upgrade/LFK update.

Thanks,

BR/Zhigang

---

Comment by [Rishi Shekhar](#) [ 2024-11-22 ]

FYR- I just got the graceful activation alarm from CCDM logs shared earlier to me. This mentions Graceful period activated on 22-10-2024.

LicenseManagerLicenseGracePeriodActivated  
active-severity Major  
service-name eric-lm-combined-server  
event-type CommunicationsAlarm  
source /x:product-type=CCDM/license-key-id=FAT1024200/51  
specific-problem License Manager License Grace Period Activated  
probable-cause 1  
major-type 193  
minor-type 17301511

- last-event-time 2024-10-22T11:57:09.664813 UTC\*  
additional-text License Key FAT1024200/51 belonging to License Domain CCDM,941903,UME\_TRIAL\_CCDM2 will be deleted

I checked the CCSM & CCRC alarm history as well but we dont have any logs before 30-10-2024, propably thos logs from alarm-history might have been rotated.

Attached logs for your reference as well. [ECCD-A\\_ccdm\\_ccsm\\_hc.txt](#)

---

Comment by [Zhigang Han](#) [ 2024-11-22 ]

hi Rajan,

"When the License Manager is informed by a Network License Server (NeLS) that a license currently in use has been removed from the NeLS inventory, the alarm [License Manager Grace Period Activated](#) will be raised." so UCC activated grace period alarm if NeLs server informed that a license in use has removed from NeLs server side.

grace period is 14 days however if UCC was in autonomous mode. The grace period will be delayed until UCC lm state is back to normal state from autonomous state.

**the key** is if there is any activity from NeLs and if there is grace period alarm generated from UCC side, it means NeLs server activity has not done correctly. From CPI, it mer make sure **grace period alarm is cleared** before we move to next step.

Yes we do not have the log before Oct 31, so we do not know what is going on before Oct 31st.

two things:

1, power on on Nov 12th did cause UCC deleted license keys, because after power on, NeLs server was back online which UCC lm state from autonomous mode to normal s same time grace period was expired on Nov 12th, however I am not sure when grace period alarm was activated. There is no log or alarm to show when UCC side raised gra could be on Oct 22nd or Oct 30th but not sure!

2, with these frequent power on/off, NeLs server might be corrupted which caused UCC raised grace period alarm also!!

as PLM suggested, after all LFK changes, disable license service from NeLs side ( there is one parameter to set to disable). After Nels engineer disabled this parameter, UCC autonomous mode so any changes from NeLs side will not impact UCC side.

hopefully this answers your question.

Thanks,

BR/Zhigang

---

Comment by [Rajan Rajeshprasad Gupta](#) [ 2024-11-22 ]

Hello Zhigang,

I spend time to analyze ADP logs in details to come for common root-cause of problem.

See below is event history collected from ILO events logs.

Date	Action	Status of Calls(4G/5G)
21-10-2024	NFs working with old LKFs	Ok
22-10-2024	NELS New License apply procedure	OK
24-10-2024	Change SWLT ID in change in CNFs	OK
30-10-2024	MM SWLT ID is not changed	Ok
31-10-2024	Power off	NA
31-10-2024	Power on	OK
8-11-2024	Power off	NA
11-11-2024	Power on	OK
12-11-2024	Power on	NOK
14-11-2024	Power off	NA
14-11-2024	Power on	NOK

Table indicate problem started after 12th Nov 2024(highlighted in red), Power restart is not a problem for deleting license as calls worked fine on 11th Nov 2024 after Power ADP logs for CCRC has unfortunately logs starting from 31st Oct 2024 (So we cant see before events).

See interesting logs:

```
{"version": "1.2.0", "timestamp": "2024-10-31T10:07:00.477Z", "severity": "info", "service_id": "eric-lm-combined-server", "metadata": {"container_name": "eric-lm-license-server", "pod_name": "eric-lm-combined-server-license-server-client-6b4bc9889f-6gmjd", "namespace": "ccrc"}, "message": "1@GracePeriodManager.java:scheduleAtDate:145@Sch GracePeriod callback for domain CCRC#UME_TRIAL_CCRC#963665 and key LicenseKey{id=562, productType='CCRC', swltId='UME_TRIAL_CCRC2', customerID='941903', licenseId='FAT1024199/10', licenseType=FEATURE, start=2024-10-07T22:00:00Z, stop=2025-04-05T22:00:00Z, capacity=null, gracePeriod=2024-11-12T12:48:20.987Z, per periodStart=null, growOnly=false, lastUpdateTime=2024-10-22T11:51:49.365Z, description=[NRF SW Probes] } in 1046480519 milliseconds"}
```

How I read it.

- last update @22-10-2024, ie Nels update happen by CCRC pod for license change/license refresh.
- During this update, nels has given graceperiod activation instruction on which is suppose to start @12-11-2024 (Future date apx. 20 days from change of last update )
- We see logs on 31-10-2024, It will be same logs from 22-10-2024 (Unfortunately logs are not available to confirm )
- Exactly on 12-11-2024 grace period expired and license is deleted from CCXX.

See logs for license deletion:

```
{"version": "1.2.0", "timestamp": "2024-11-12T12:48:21.076Z", "severity": "info", "service_id": "eric-lm-combined-server", "metadata": {"container_name": "eric-lm-license-server", "pod_name": "eric-lm-combined-server-license-server-client-6b4bc9889f-6gmjd", "namespace": "ccrc"}, "message": "23@Persistence.java::deleteLicenseKeyAtGracePeriodExpiration:1730@Triggered callback [ deleteLicenseKeyAtGracePeriodExpiration [ for domain CCRC#UME_TRIAL_CCRC#963665 and key LicenseKey{id=562, productType='CCRC', swltId='UME_TRIAL_CCRC2', customerID='941903', licenseId='FAT1024199/10|mailto:23@Persistence.java::deleteLicenseKeyAtGracePeriodExpiration:1730@Triggered%20callback%20deleteLicenseKeyAtGracePeriodExpiration%20for%20licenseManagement' ] ] in 1046480519 milliseconds"}
```

See statement from CPI:

[https://calstore.internal.ericsson.com/elex?LI=EN/LZN7020566/1R107B&FB=0\\_1&FN=19\\_1543-CSH109675\\_1Uen.C.html&HT=gws170730903139&DT=License+Manager+License+Grace+Period+Activated](https://calstore.internal.ericsson.com/elex?LI=EN/LZN7020566/1R107B&FB=0_1&FN=19_1543-CSH109675_1Uen.C.html&HT=gws170730903139&DT=License+Manager+License+Grace+Period+Activated)

"If a license key currently in use is attempted to be removed from the NeLS inventory during normal mode of operation, **a grace period is started for the removed license**. A grace period is set on a license, **license management retains its current status until the end of the grace period. The license key is removed after the grace period expires**".

So here conclusion:

1. Nels License key refresh happen on 22-10-2024
2. CNFs has updated license change request from Nels.
3. CNFs has activated grace-period of 20 days ie 12-11-2024 [ Instead of 14 days ], CNFs has not replaced new license immediately by waited for grace-period to end.
4. After grace-period expiry, CNF has deleted old license and tried contacting Nels to fetch new license.
5. However nels was not connected on 12-11-2024 and CNFs end up initial state with No-License & call fails.
6. Case is not related to power-restart by any means.

Please help to check with Nels and CNF behaviour.

In such case we should add dedicated statement in Installation guide of UCC "Procedure to change LKF in NeLS and Handing for UCC".

Good Option:

1. Force CNFs to fetch change in LKF immediately (Instead of activating grace period for delete and refresh operation) eg. restart of license-server-pod
2. Force Nels to install new LKF immediately (Instead of activating grace period for delete and refresh operation)

14 days or 20 days having nels always connected with UCC is not a good possible option.

Comment by Ahmed Elkhouly [ 2024-11-21 ]

Great analysis! Thanks Zhigang and Rishi

Comment by Zhigang Han [ 2024-11-21 ]

hi team,

here is the analysis from CCRC adp log:

1, NeLs server was on/off all the time

2, UCC ran in autonomous mode on/off all the time

3, there was grace period alarm activated from UCC side. clearly there was a change from NeLs server side.

"When the License Manager is informed by a Network License Server (NeLs) that a license currently in use has been removed from the NeLs inventory, the alarm [License Manager Grace Period Activated](#) will be raised."

4, on Nov 12th, NeLs server was back online and grace period expired, so CCRC deleted all license keys

```
{"version": "1.2.0", "timestamp": "2024-11-12T12:48:21.079+00:00", "severity": "info", "service_id": "eric-lm-combined-server", "message": "Deleted from cache: LicenseKey{id=51, productType=CCRC, licenseId=FAT1024199/10, licenseType=0, start=2024-10-07 22:00:00 +0000 UTC, stop=2025-04-05 22:00:00 +0000 UTC, capacity=-1, gracePeriod=173, periodLength=-1, periodStart=-1, growOnly=false} slwtID=UME_TRIAL_CCRC2, customerID=941903, lastUpdateTime=1729597909365, description=[NRF SW Probes]}", "metadata": {"function": "gerritt.ericsson.se/adp-gs/adp-gs-lm/internal/persistence.(inMemoryCacheImpl).deleteLicenseKey", "proc_id": "1", "pod_name": "eric-lm-combined-server-license-568645448fm7gw", "container_name": "eric-lm-license-consumer-handler"}}
```

here is another log which we could see grace period was expired:

```
{"version": "1.2.0", "timestamp": "2024-11-12T12:48:21.076Z", "severity": "info", "service_id": "eric-lm-combined-server", "metadata": {"container_name": "eric-lm-license-server", "pod_name": "eric-lm-combined-server-license-server-client-6b4bc9889f-6gmjd", "namespace": "ccrc"}, "message": "23@Persistence.java::deleteLicenseKeyAtGracePeriodExpiration:1730@Triggered callback deleteLicenseKeyAtGracePeriodExpiration for domain CCRC#UME_TRIAL_CCRC; FAT1024199/10"}
```

5, we saw CCRC generated one alarm about missing license on Nov 12th after CCRC deleted all license keys

nrfMngtLicenseAbsent active-severity Major service-name eric-nrf-nnrf-nfm event-type QualityOfServiceAlarm source /nrf:nrf/non\_modeled/nfmanagement specific-problem nnrf-nfm **License Absent probable-cause 418** major-type 193 minor-type 7929865 last-event-time **2024-11-12T12:48:36.000567** UTC alarm-update 0 additional-text Both and NRF mIoT BP License are Absent for The Configured SNSSAI

6, NeLs server was down so UCC was not able to connect to refresh the valid license keys.

without any valid license keys, that is why traffic was not working.

Here is the suggestion from PLM side:

1, fix NeLs server and allow UCC fetching all the correct license keys

2, make sure there is no any grace period alarm activated

3, create checkpoint for mm to save the valid license keys in case there is a reboot

4, disable license service from NeLs side which allow UCC running in autonomous mode all the time

once we receive CCSM/CCDM logs, we will continue checking if CCSM/CCDM ran into the similar situation or not?

Thanks,

BR/Zhigang

Comment by Rishi Shekhar [ 2024-11-21 ]

Regarding ADP logs from CCSM/CCDM already requested the requirements to Telefonica team. They mentioned once the next visit to site is planned Telefonica team will fetch for CCSM/CCDM.

From ILO logs captured earlier- it was observed multiple ungraceful cluster reboot happened due to power removal in both the nodes. Attached ILO logs for both the clusters [UCCA.csv](#) [EventLog\\_UCCB.csv](#)

Comment by Zhigang Han [ 2024-11-20 ]

Hi Ahmed,

I am waiting for the ADP of CCSM/CCDM from Rishi. one thing Ahmed: last time I checked the ilo log with Rishi, we identified that there were many power removed warning doesnot follow the official power on/off procedure, it could corrupt the UCC.

Thanks,

BR/Zhigang

Comment by [Ahmed Elkhouly](#) [ 2024-11-20 ]

Hi Zhigang,

We need to investigate why there was an issue in license keys in the first place.

UCC is supposed to be connected to NeLS during pre-staging phase or for upgrades.

was there anything suspicious from the logs provided by Rishi?

Comment by [Zhigang Han](#) [ 2024-11-19 ]

hi Rishi,

Please request CU to fix NeLs server as soon as possible. NeLs is mandatory in UCC solution when there is an issue with license keys in this situation.

Thanks,

BR/Zhigang

Comment by [Zhigang Han](#) [ 2024-11-18 ]

hi Rishi,

Could you collect ccsm ADP logs also?

Thanks,

BR/Zhigang

Comment by [Rishi Shekhar](#) [ 2024-11-14 ]

CCRC ADP logs sharepoint link for analysysis:-

[https://ericsson-my.sharepoint.com/:u/r/personal/rishi\\_shekhar\\_ericsson\\_com/Documents/Desktop/Tef-CCXX-License%20issue/wetransfer\\_untitled-transfer\\_2024-11-14\\_0831/ADP\\_logs\\_ccrc\\_2024-11-13-17-13-29-UCCA.7z?csf=1&web=1&e=A81DJz](https://ericsson-my.sharepoint.com/:u/r/personal/rishi_shekhar_ericsson_com/Documents/Desktop/Tef-CCXX-License%20issue/wetransfer_untitled-transfer_2024-11-14_0831/ADP_logs_ccrc_2024-11-13-17-13-29-UCCA.7z?csf=1&web=1&e=A81DJz)

#### [UCC\_PLM-159] UCC CP1 : CCD version is upgraded to 2.29.4 in correction package Created: 2024-11-14 Updated: 2025-04-24 Resolved: 2025-04-24

Status:	Done
Project:	<a href="#">UCC_PLM</a>
Component/s:	None
Affects Version/s:	None
Fix Version/s:	None

Type:	Bug	Priority:	Medium
Reporter:	<a href="#">Rajan Rajeshprasad Gupta</a>	Assignee:	Unassigned
Resolution:	Closed	Votes:	0
Labels:	None		
Remaining Estimate:	Not Specified		
Time Spent:	Not Specified		
Original Estimate:	Not Specified		

Severity_qmt:	3- Medium
Found in Build:	1.0.CP1
Requirement Status:	UCC Appliance 0.2.1 - UNCOVERED

#### Description

Hello,

As per understanding CP1 is correction package.

I dont see any specific bug in CCD 2.29.1 solved as part of CP1.

1. May we know reason to upgrade CCD software in correction package from 2.29.1 to 2.29.4?

2. Why we have not upgraded software for all other NFs like EP5G,CCRC etc?

Questions will be asked by all MAs and SDUs. So we want to know reason to be in common information to be shared to all.

Note: Any new change in software, needs download of software from software gateway and push to jumphost on remote location.

#### Comments

Comment by [Reema Sidhwani](#) [ 2024-11-17 ]

The reason for upgrading to CCD 2.29.4 is that several critical vulnerabilities have been closed in this version compared to 2.29.1. The list of vulnerabilities will be mentioned in the release notes for CP1.

There was no similar reason or any critical reported bugs on any other CNF so no other CNF upgrade has been included in CP1.

#### [UCC\_PLM-158] UCC CP1 : LLD still show 2 diameter IP for rx and gx for CCPC

Created: 2024-11-14 Updated: 2024-11-25 Resolved: 2024-11-25

Status:	Rejected
Project:	<a href="#">UCC_PLM</a>
Component/s:	None
Affects Version/s:	None
Fix Version/s:	None

Type:	Bug	Priority:	Medium
Reporter:	<a href="#">Rajan Rajeshprasad Gupta</a>	Assignee:	<a href="#">Kamal Ait Hammou</a>
Resolution:	Rejected	Votes:	0
Labels:	None		
Remaining Estimate:	Not Specified		
Time Spent:	Not Specified		
Original Estimate:	Not Specified		

Attachments:	
Defect code_qmt:	1- Functional
Team/s:	UCC_XFT2
Severity_qmt:	2- High
Found in Build:	UCC Appliance 1.0.1-rc1
Requirement Status:	UCC Appliance 0.2.1 - UNCOVERED

#### Description

Hello,

refer ticket raised for ccpc support single diameter vip.

[https://eteamproject.internal.ericsson.com/browse/UCC\\_PLM-114](https://eteamproject.internal.ericsson.com/browse/UCC_PLM-114)

however we still see 2 diameter vips in CP1 lld for diameter.

is it typo? or purposely designed?

VIP	TYPE		Network Instance		SUBNET	
ecfe_sig_vips	ecfe-vip		Sig		172.16.2.64/32	smf
					172.16.2.65/32	smf
					172.16.2.66/32	udr
					172.16.2.67/32	udr
					172.16.2.68/32	ausf
					172.16.2.69/32	dia
					172.16.2.70/32	hss
					172.16.2.71/32	udm
					172.16.2.72/32	ccrc
					172.16.2.73/32	ccrc
					172.16.2.74/32	ccpc
					172.16.2.75/32	ccpc
ecfe_oam_vips	ecfe-vip		oam		10.92.238.64/32	pcx
ecfe_sig_data_vips			sig_data		10.92.238.65/32	pcx
ecfe_sig_ext_vips			sig_ext		10.92.238.66/32	ccdr
					10.92.238.67/32	ccdr
					10.92.238.68/32	ccdr
					10.92.238.69/32	ccsn
					10.92.238.70/32	ccrc
					10.92.238.71/32	ccrc
					10.92.238.72/32	eda
					10.92.238.73/32	cno
					10.92.238.74/32	cno
					10.92.238.75/32	ccd
					172.16.2.97/32	smg
					172.16.2.98/32	creg
					172.16.2.99/32	ccpc
					172.16.2.100/32	ccdr
					10.92.238.216/32	ccpc
					172.16.2.61/32	ccrf

#### Comments

Comment by Kamal Ait Hammou [2024-11-25]

Hi Rajan,

In fact we have two Diameter IPs :

- One on the VRV Sig\_Ext : that will be used by any application outside UCC ( like MCPTT)
- second VIP on the VRF Sig : is reserved for future use for internal traffic ( like NEF implementation)

Please describe in solution description that the Vip that will used externally is ccpc\_rx.

Best regards,

Kamal

[UCC\_PLM-157] UCC1.0 Netrunner add user fails and crashes internally UCC provisioning feature Created: 2024-11-12 Updated: 2025-03-11 Resolved: 2025-02-17

Status:	Done
Project:	UCC_PLM
Component/s:	None
Affects Version/s:	UCC Appliance 1.0.0-rc2
Fix Version/s:	None

Type:	Bug	Priority:	Critical
Reporter:	Rishi Shekhar	Assignee:	Unassigned
Resolution:	Closed	Votes:	0
Labels:	None		
Remaining Estimate:	0h		
Time Spent:	8h		
Original Estimate:	Not Specified		

Attachments:	Deac-2_PLM-157-Shared-License-erroe.txt  Netrunner-UE Prov Error.png
Other Assignees:	Rishi Shekhar
Detected in phase:	Production
Epic Link:	Bug Backlog for UCC1.1
Team/s:	UCC_XFT2, UCC_XFT3
Severity_qmt:	1- Critical
Found in Build:	1.0
Requirement Status:	UCC Appliance 0.2.1 - UNCOVERED

#### Description

##### Description:-

Netrunner add user fails and causes subscriber management page to go out of sync.

Issue reproduced in two setups- Mana- Experience Center UCC setup & TMO setup in UCC 1.0 release.

Single UE provisioning fails in Netrunner. Whenever the issue happens it impacts the subscriber management in CNOM.

Components:- UCC-CNOM

Manual Curl query to UDR for UE status:- Auth profile present but UDM profile missing.

```
eccd@ucc-ccda:~> curl -v -s -X GET -H "Content-Type: application/json; charset=utf-8" --header "Authorization: Bearer $ACCESS_TOKEN"
https://10.145.7.67:443/mapi/v1/users/imsi-311660000000055 --insecure | jq
```

```
{
  "identities": [
    { "idType": "imsi", "idValue": "311660000000055" }
  ],
  "auth": {
    "authSubscription": {
      "imsi-311660000000055": {
        "ueIdList": [
          { "idType": "imsi", "idValue": "311660000000055" }
        ],
        "authenticationMethod": "5G_AKA",
        "encPermanentKey": "04b6ba6e362dfca54baae164488dad1",
        "authenticationManagementField": "725C",
        "algorithmId": "0",
        "a4KeyInd": "1",
        "a4Ind": "2"
      }
    }
  }
}
```

#### Work Around to fix the issue:-

Do a UE provisioning with UCA batch job.

#### Comments

Comment by Christos Delis (EXT) [ 2024-12-20 ]

Hello,

Am closing this ticket as issue has been resolved on new CNOM 2.2 release.

BRs,

Christos

Comment by Rishi Shekhar [ 2024-12-05 ]

Based on PDU confirmation from Christos- issue is identified & going to fix with next CNOM version.

Comment by Jim Dumont [ 2024-11-22 ]

Blocked on waiting for response from PDU

Comment by [Rishi Shekhar](#) [ 2024-11-21 ]

I am able to reproduce the shared license issue in Deacucc2 setup as well.

Attached complete logs for reference. [Deac-2\\_PLM-157-Shared-License-erroe.txt](#)

eccc@ucc-ccda:~/esheris>

eccc@ucc-ccda:~/esheris> curl -v -s -X POST -H "Content-Type: application/json; charset=utf-8" --header "Authorization: Bearer \$TOKEN" -d

@Create\_Data\_Subscription\_Data.json <https://prov.eda-deacucc2a.deac.ericsson.se/aapi/v1/eps-udm/data-subscription?userId=imsi-244990000018000> --cert tls.crt --key tls.key --cacert ca.crt

- Trying 10.92.239.72:443...
- Connected to prov.eda-deacucc2a.deac.ericsson.se (10.92.239.72) port 443 (#0)
- ALPN: offers h2,http/1.1
- TLSv1.3 (OUT), TLS handshake, Client hello (1):

<

- Connection #0 to host prov.eda-deacucc2a.deac.ericsson.se left intact {"faultcode":1099,"faultreason":"System error.","faultdetails":"Shared Networks license is not installed.\*"}

eccc@ucc-ccda:~/esheris>

eccc@ucc-ccda:~/esheris>

eccc@ucc-ccda:~/esheris>

Comment by [Zhigang Han](#) [ 2024-11-18 ]

Hi Rishi,

using CNOM netrunner to perform the subscriber provisioning, CNOM will do curl post towards to UCA not directly towards to CCDM, so Could you check UCA log to see if we could see the license issue?

Thanks,

BR/Zhigang

Comment by [Zhigang Han](#) [ 2024-11-18 ]

Hi Rishi,

The site which we performed the test is also having the same license keys as MANA site:

```
bash-4.4$ curl -w "\n" --header "Content-Type: application/json" --request GET http://eric-lm-combined-server:8080/license-manager/api/v1/licenses --data '{"productType":"CCDM"}' | jq . | jq . | grep -i FAT
% Total % Received % Xferd Average Speed Time Time Current
          Dload Upload Total Spent Left Speed
100  688 100  666 100  22 214k  7246 0:0:0:0:0:0 0:0:0:0 335k
  "keyId": "FAT1024213/6",
  "keyId": "FAT1024213/9",
  "keyId": "FAT1024213/1",
  "keyId": "FAT1024200/51",
bash-4.4$
```

we are also facing the provisioning issue with netrunner from cnom gui. It is possible that the issue is related to the missing license but I will check other site to see if we could perform this license test.

Thanks,

BR/Zhigang

Comment by [Rishi Shekhar](#) [ 2024-11-18 ]

I reproduced the issue today in TMO Mana setup.

Manual UE provisioning from CLI on "A-API (this way CNOM use to do UE provisioning) " towards UDR gives license error.

```
eccc@ucc-ccda:~/prov> curl -v -s -X POST -H "Content-Type: application/json; charset=utf-8" --header "Authorization: Bearer $TOKEN" -d
@Create_Data_Subscription_Data.json https://prov.eda-tmoucca.tmuucc.internal.ericsson.com/aapi/v1/eps-udm/data-subscription?userId=imsi-311660000000030 --cert
tls.crt --key tls.key --cacert ca.crt
```

- Connection #0 to host prov.eda-tmoucca.tmuucc.internal.ericsson.com left intact {"faultcode":1099,"faultreason":"System error.","faultdetails":"Shared Networks license is not installed.\*"}

eccc@ucc-ccda:~/prov>

License comarison Mana TMO v/s Aachen Deacucc1a:-

```
eccc@ucc-ccda:~/prov> kubectl exec -it -n ccdm $(kubectl get po -n ccdm | grep -i eric-nrf-discovery | awk 'NR==1
```

```
{print $1}) - curl -w "\n" --header "Content-Type: application/json" --request GET http://eric-lm-combined-server:8080/license-manager/api/v1/licenses --data
'{"productType":"CCDM"}' | jq . | jq . | grep -i FAT
"keyId": "FAT1024213/6",
"keyId": "FAT1024213/9",
"keyId": "FAT1024213/1",
"keyId": "FAT1024200/51",

deacucc1@ucc-jumphost:~$ kubectl exec -it -n ccdm $(kubectl get po -n ccdm | grep -i eric-nrf-discovery | awk 'NR==1 {print $1}
') - curl -w "\n" --header "Content-Type: application/json" --request GET http://eric-lm-combined-server:8080/license-manager/api/v1/licenses --data
'{"productType":"CCDM"}'
' | jq . | jq . | grep -i FAT
• "keyId": "FAT1024200/56",
"keyId": "FAT1024213/2",
"keyId": "FAT1024200/51",
• "keyId": "FAT1024200/52",
"keyId": "FAT1024200/55",*
```

As now we have used Shared license in GA version but earlier with PoC 0.2.2 release in Telefonica we had the similar experience during UE provisioning & same was fixed by adding the feature license key- \* **FAT1024200/52**, **FAT1024200/55**, "FAT1024200/56",\*\*

Comment by [Zhigang Han](#) [2024-11-15]

Hi Rishi,

Christos mentioned two points :

- a user was not added/deleting correctly - as only Auth Data has been created CNOM is not able to fetch subs. By fully deleted the subscriber, CNOM can fetch subs.
- hss validator was not installed.

Could you verify these two points from MANA site which you are facing the issue?

For me, the first point is actually the real issue, but could you use UCA to delete the subscriber then perform the subscriber provisioning via NetRunner to see if the issue is still there or not??

Thanks,

BR/Zhigang

Comment by [Christos Delis \(EXT\)](#) [2024-11-15]

Hi Zhigang,

From my experience as we have already encountered, as it seems from the logs the same issue, the two main reasons which we have identified, as wrote on previous comment, were:

- a user was not added/deleting correctly - as only Auth Data has been created CNOM is not able to fetch subs. By fully deleted the subscriber, CNOM can fetch subs.
- hss validator was not installed.

In our case by fixing above bullets, process of provision was okay.

In any case, lets have a try to provision a subscriber via NetRunner when PLM system will be back (on an empty UDR database), to see the outcome and according to the result we can continue the investigation, and we could also get feedback from CNOM PDU.

BRs,

Christos.

Comment by [Zhigang Han](#) [2024-11-15]

Hi Christos,

PLM system is under the redeployment right now. Once it is done, we will perform the test again on PLM system. here is my question:

after supporting Rishi, are you able to identify the root cause of the issue?

Thanks,

BR/Zhigang

Comment by [Christos Delis \(EXT\)](#) [2024-11-15]

Good morning Zhigang,

I had a discussion with Rishi and we were trying to check/fix the issue but we couldn't find the solution.

In our verification activities, when we were trying to execute this activity, we didn't face this issue:

<https://eteamproject.internal.ericsson.com/browse/UCCPOCDEV-293>

Please check test cases ([UCC\\_PRODIV-332-333](#), [UCC\\_PRODIV-574-575](#)).

I remember that in the past we have encountered this issue as Rishi shared with me from the logs:

```
{"version":"1.2.0","timestamp":"2024-11-13T00:34:25.450-08:00","severity":"error","service_id":"eric-cnom-server","message":"Error: PrivateNetworkSubscriber validation failed: imsi: Path `imsi` is required.\n at ValidationError.inspect (/cnom/node_modules/mongoose/lib/error/validation.js:50:26)\n at formatValue\n(node:internal/util/inspect:805:19)\n at inspect (node:internal/util/inspect:364:10)\n at formatWithOptionsInternal (node:internal/util/inspect:2298:40)\n at Object.format"
```

There was a discussion with CNOM PDU where if Data Auth is not able to be created for the specific user, Auth Data must be also discarded. This issue will be covered on new CNOM version cNOM 2.1 (<https://eteamproject.internal.ericsson.com/browse/CNOM-17965>)

From the description of the issue, looks the same. In our case when we faced this issue the main two reasons were:

- a user was not added/deleting correctly - as only Auth Data has been created CNOM is not able to fetch subs. By fully deleted the subscriber, CNOM can fetch subs.
- hss validator was not installed.

Have you tried to provision a first subscriber only from Network Runner, by having an empty UDR database?

If not, could you please try this to check the status of CNOM.

BRs,  
Christos

Comment by [Zhigang Han](#) [ 2024-11-14 ]

hi Christos,

Rishi and I were able to duplicate the issue on another site with UCC 1.0 release. we were not able to find any useful information from the log of eric-cnom-ingester pod.

Thanks,

BR/Zhigang

#### [UCC\_PLM-156] HLD feedback Created: 2024-11-12 Updated: 2025-03-11 Resolved: 2025-03-11

Status:	Completed
Project:	<a href="#">UCC_PLM</a>
Component/s:	None
Affects Version/s:	None
Fix Version/s:	None

Type:	Story	Priority:	Low
Reporter:	<a href="#">Ashok Gumpu</a>	Assignee:	<a href="#">Marija Skrekovski</a>
Resolution:	Complete	Votes:	0
Labels:	UCC_Appliance_1.0.1		
Remaining Estimate:	Not Specified		
Time Spent:	Not Specified		
Original Estimate:	Not Specified		

Requirement Status:	UCC Appliance 0.2.1 - UNCOVERED
Team/s:	<a href="#">UCC_SM</a>

#### Description

Hello Team,

This is regarding HLD feedback on UCC traffic Scenario.

**In HLD its mention UCC-Server 1 should handle 99% traffic and UCC-Server 2 will handle rest**

but the relative Node capacity mention in HLD needs update

#### Existing information in HLD

Relative capacity for MME pool:

- MME1 =1
- MME2=255

Relative capacity for AMF pool:

- AMF1=1
- AMF2=255

## It Should be

Relative capacity for MME pool:

- MME1 =255
- MME2=1

Relative capacity for AMF pool:

- AMF1=255
- AMF2=1

Thanks

Ashok Gumpu

## Comments

Comment by [Marija Skrekovski](#) [ 2024-11-13 ]

The text is updated in the UCC Redundancy description document. The new version (PB1) is available in EriDoc.

## [UCC\_PLM-152] Relative path used for UCA CSAR Package Preparation Created: 2024-11-08 Updated: 2025-04-23 Resolved: 2025-04-23

Status:	Done
Project:	<a href="#">UCC_PLM</a>
Component/s:	None
Affects Version/s:	<a href="#">UCC Appliance 1.0.1-rc1</a>
Fix Version/s:	None

Type:	Bug	Priority:	Low
Reporter:	<a href="#">Fredrik Gustavsson</a>	Assignee:	Unassigned
Resolution:	Closed	Votes:	0
Labels:	None		
Remaining Estimate:	Not Specified		
Time Spent:	Not Specified		
Original Estimate:	Not Specified		

Defect code_qmt:	3- Usability
Sprint:	UCC XFT2 Sprint 2
Detected in phase:	PDU
Team/s:	UCC_XFT2
Severity_qmt:	4-Low/Cosmetic
Found in Build:	<a href="#">UCC Appliance 1.0.1-rc1</a>
Requirement Status:	UCC Appliance 0.2.1 - UNCOVERED

## Description

In UCC - Software Installation Guide, 2024-09-06, Rev "", part of UCC 1.0.1 (CP1) release candidate 1 (2024-11-08), chapter 12.1 UCA CSAR Package Preparation, bullet 4 and 6 use relative paths:

```
zip -g $software_dir/EDA/eric-act-uca-1.63.128.csar \
Definitions/TOSCA.yaml
```

```
unzip -j /data/software/EDA/eric-act-uca-1.63.128.csar \
Definitions/OtherTemplates/eric-act-cna-1.63.128-6.tgz
```

The commands fail unless the user converts them to absolute paths or changes directory.

## Comments

Comment by [Arron Kuang](#) [ 2024-11-27 ]

Hi,