



# Release Notes for *Cisco Policy Suite* for Release 6.1

---

**First Published: May 1, 2014**

**Last Updated: July 10, 2015**

**Release: 6.1**

## Contents

This document describes the new features, feature versions and limitations for Cisco Policy Suite. Use this document in combination with documents listed in the “[Related Documentation](#)” section on page 23.

This document includes the following sections:

- [Introduction, page 1](#)
- [New and Changed Information, page 2](#)
- [Installation Notes, page 5](#)
- [Limitations and Restrictions, page 12](#)
- [Caveats, page 12](#)
- [Related Documentation, page 23](#)

## Introduction

Cisco Policy Suite (CPS) is a comprehensive policy, charging, and subscriber data management solution that allows service providers to control and monetize their networks and to profit from personalized services. CPS has the following components:

- Cisco Policy Server (PS)
- Cisco Charging Server (CS)
- Cisco Application Gateway (AGW)



- Cisco Unified Subscriber Manager (USuM)
- Cisco Subscriber Analytics

CPS provides an intelligent control plane solution, including southbound interfaces to various policy control enforcement functions (PCEFs) in the network, and northbound interfaces to OSS/BSS and subscriber applications, IMSs, and web applications. The CPS modules are enabled individually or deployed as an integrated end-to-end policy, charging, and service creation solution.

### Competitive Benefits

The new CPS solution provides these benefits over competitive solutions.

- CPS architecture allows simultaneous sessions and transactions per second (TPS) capacity to be independently scaled. This allows CPS to be efficiently sized for both high simultaneous sessions with low TPS or low sessions with high TPS, resulting in lower total cost of ownership when compared to traditional PCRF models. As soon as sessions are bound to a given processing node, the ability to handle traffic spikes is reduced.
- CPS virtual architecture supports flexible and cost-effective carrier grade strategies. Virtual instances are spread across multiple blade serves for full hardware and software redundancy within a CPS cluster.
- The flexible nature of the CPS lets a service provider go beyond standard policy definition to add new, customized functionality. It provides a comprehensive open policy software development kit (SDK) using industry-standard languages and frameworks. Customized or vendor scripting is not needed, which allows service providers to create plug-ins within the existing policy server and automatically exposes the new services to the policy engine.

## New and Changed Information

This section describes the new and changed features for the CPS Release 6.1.

### New Software Features in Release 6.1

#### Content Filtering Policy

Content Filtering Policy is implemented by CPS on the ASR 5000 platform. The Policies are defined by the service provider on the ASR 5000 platform through the CPS, by using the Credit Control Access (CCA) and the Re-authorization Request (RAR) messages of the Diameter Gx component. Content Filtering is provided by the ASR 5000 by specifying the Policy ID through the Gx interface. Diameter Gx is the existing component in the CPS which supports AVP's for the Content Filtering in the CCA and RAR messages.

When a user initiates a session, the ASR 5000 communicates with the CPS to initialize the defined policies. CPS provides the Policy ID to the ASR 5000 to provide the necessary Content Filtering services for the user. Policy IDs need to be configured by the subscriber on the ASR 5000 through the CPS.

#### Diameter Configurable AVP Dictionary

To enhance the QoE, CPS supports configuring custom AVP's across interfaces of the PCRF. CPS supports the following:

- Capability to define a wide range of Vendor Specific AVP.

- Copy/replicate an AVP from one interface to another.
- Ability to store value contained in standard/3GPP defined AVP to send it over a Vendor specific AVP.

## Conversational Video Service

IMS conversational video services builds on VoLTE to support the addition of GSM IR.94 video capability, providing users with synchronized full-duplex voice and video calls. Using conversational video services, users can make one-to-one or multi-party video calls, switch to video at any point during a call, and drop video at any point to continue with just voice. With this feature, the CPS supports policy control for conversational video services authorizing dedicated QoS Bearers (video and audio) within a subscriber's IP-CAN session.

## Default Bearer Modification Triggered by Rx (HTTP REST API)

CPS provides capability to modify a session's default bearer QoS and AMBR, which is triggered through Rx interface. This capability is achieved by integrating the Monarch system through the Rx interface.

## Enhanced Multi-Media Priority Services

CPS provides Enhanced Multi-Media Priority Services (eMPS) subscription data for priority subscribers. CPS supports VoLTE/IMS calls for priority subscribers. Diameter Gx is the existing component in CPS, which supports a new service configuration for provisioning eMPS data. CPS provides the ability to determine priority subscribers to provide priority services.

## Gx Race Conditioning Handling

CPS supports the Cisco ASR5500 for race condition elimination on the Gx interface ensuring QoE for subscribers.

During the processing of a Gx request, if there is another request that is received at the Gx interface, a new error indication "DIAMETER PENDING TRANSACTION" is sent to the transaction originator to determine if a re-attempt of the transaction at a later time if required.

## HTTP REST API or Rx Trigger

There are three use cases where the Subscriber session parameters are modified either over the Rx interface or with REST API. The HTTP REST API is alternate method to modify subscriber QoS as a part of use cases:

- QoS Uplift on Default Bearer
- Venue Throttling (Network Congestion Control)
- Creation of Dedicated Bearer on Subscriber Session (with or without Sponsored Data)

## Network Congestion Level

Congestion Control Levels and corresponding QoS values (Apn-Aggregate-Max-BitRate-UL and APN-Aggregate-Max-BitRate-DL) are defined by the operator via Customer Reference Data tables. The congestion level is the key column. The application function via Rx interface and AAR message

indicates the congestion level to the PCRF. The PCRF looks up Customer Reference Data table to find appropriate values of APN-Agg-Bit rate values and initiates a RAR message on the session towards the PCRF to either upgrade or downgrade the QoS.

## Service Group QoS

ASR5K supports handling of Service Group QoS and defines new Gx AVPs which are exchanged between PCEF and PCRF. These new vendor-specific AVPs define parameters like Rule Name, specific QoS Information and precedence values. Additionally CPS (PCRF) supports various use cases related to PCC Rules provisioning and usage monitoring control as defined in 3GPP specification 29.212.

## Single Radio Voice Call Continuity (SRVCC) Handover Notification

Single Radio Voice Call Continuity (SRVCC) solution seamlessly maintains voice calls as mobile users move from LTE to non-LTE coverage areas. This solution transfers VoLTE calls in progress from LTE to legacy voice networks. Without SRVCC, a VoLTE call on a device moving out of LTE coverage will be dropped.

CPS (PCRF) interfaces with PCEF over the Gx interface and towards the AF via the Rx interface. To support SRVCC, CPS supports to notify AF (IMS System) when dynamic rules (created for Rx) on Gx fails because of handover from packet switched (PS) to Circuit Switched (CS).

## Small-scale Deployment Configuration

The small scale deployment project is a scaled down PCRF configuration that includes one PCRF in a 2 blade configuration in each deployed location. All the VMs in the blade are distributed in these 2 blades which requires Most of World (MOW) Project to provide for a more seamless user experience when roaming internationally.

This scaled down version is easy to install and can be accommodated at places which have hardware limitations.

## SNMP Enhancements

CPS supports new SNMP traps. The following is the list of new traps implemented:

- QPS Process Down - This traps gets generated when any QNS process is down on any VM types: perfclient, lb and qns.
- Admin/root User Logs in - This traps gets generated if admin/root user logs in to any VM.
- License Usage threshold exceeded - This traps gets generated whenever Session usage has exceeded the configured threshold value.

## SSL Support

Default HAProxy configuration does not have SSL support for any port. To enable/add the SSL configuration for any port in HAProxy.cfg, it has to be done manually. Moreover, the same changes has to be done on all LB VMs. Under this feature, a script (setupSSL) is added.

setupSSL is a script which adds or deletes the SSL Configuration into/from HAProxy.cfg file. It does this change on all LB VMs present into the system.

## Upgrade Automation

The automated upgrade supported in 6.1 release does a seamless upgrade to CPS system. It supports upgrades from 5.3.4 release onwards. It requires minimal user intervention while doing upgrade.

It upgrades the whole system including the RPMs, OS related configuration and 3rd party configuration. It preserve the files which are customer centric. The full upgrade procedure is logged so that it can be referred if needed. It can also be used to upgrade the portal software, feature files and QNS software on all VMs.

## Installation Notes

This section describes the installation notes in Release 6.1.



**Note**

Currently, direct upgrading of CPS from version 5.3.5 to 6.1 is not supported. Customer first needs to upgrade CPS to 5.5 and then can upgrade the system to 6.1.



**Note**

Customer must download the latest software package available from the link <http://software.cisco.com/download/type.html?mdfid=284883882&catid=null>.

## Feature Versions

The following table mentions the component version for CPS 6.1 Release:

Component	Version
Core	6.1.0
Audit	1.3.0
Balance	3.3.0
Control Center	3.3.0
Congestion Reference Data	1.1.0
Customer Reference Data	2.3.0
DHCP	1.3.1
Diameter2	3.3.0
ISG Prepaid	1.7.0
LDAP	1.4.0
Notifications	5.7.0
Policy Intel	2.1.0
POP-3 Authentication	1.3.0
Radius	3.2.0
SCE	2.0.8
Scheduled Events	1.2.0

Component	Version
SPR	2.2.0
Unified API	2.2.0
Web Services	1.4.0
Recharge Wallet	1.1.0
Installer	No version
RPMS	No version

## Applying Hotfix

This hot fix can only be installed with 6.1.0 CCO releases. To check the release, the service provider needs to verify the installed features by running `/opt/broadhop/qns-1/bin/features.sh` and confirming that the `policy.feature=6.1.0.release` has a “.release” extension and not a “.r#####”.

If a deployment has a non-released version (.r#####) then the service provider must contact their Cisco technical representative to have a patch created that works with their version.

This hotfix must be installed to ensure that the Policy Builder works properly with the newer versions of Firefox (v29+) and Chrome (v33+).

**Step 1** Download `Hotfix_Patch1_6.1.0.tar.gz` from <http://software.cisco.com/download/release.html?i=y&mdfid=284883910&softwareid=284980034&release=6.1&os=> along with your CPS 6.1.0 software or get the hotfix from your Cisco technical representative and extract it in `/var/broadhop/repositories` directory as a root user.

**Step 2** After extraction, find directory `Hotfix_Patch1_6.1.0` in `/var/broadhop/repositories` directory.

**Step 3** Add entry of extracted directory into `/etc/broadhop/repositories` file.

Entry Name:

```
file:///var/broadhop/repositories/Hotfix_Patch1_6.1.0
```



### Note

- Do not delete old entries from `/etc/broadhop/repositories` file.
- `QNS_6.1.0.release` entry in `/var/broadhop/repositories` needs to be left uncommented while applying the patch (updating qns).

**Step 4** Go to `/opt/broadhop/installer/` directory in `pcrfclient01` and run the commands:

```
cd /opt/broadhop/installer/
run su qns -c "./update_qns.sh"
```

**Step 5** Run `restartall.sh` from `pcrfclient01` to apply the patch.

## Portal Patch Installation

Portal Patch Name: `SSP_Patch_6.1.tar.gz`

- 
- Step 1** Place the new portal tar.gz in /var/www.
- Step 2** Unzip/Untar the portal file by: tar xzf ssp\_prod-6.1.tar.gz. This creates an archive directory.
- Step 3** Rename the archive directory:
- ```
mv archive portal
```
- Step 4** Change directory back to /var/www/portal.
- Step 5** Initialize:./init.sh
- Step 6** Run setup and answer configuration questions.
- ```
./setup.sh
```
- Step 7** Restart portal:
- ```
service httpd restart
```



**Note** The above mentioned steps must be run for every portal installation/upgradation on each portal server.

---

## Removing MySQL JDBC Connectors from Standard Load Line-up

---

- Step 1** Add the following entry to `qns.conf` file on all the CPS boxes.
- ```
-DmysqlDriver=file:///var/broadhop/jdbc/jdbc_5_1_6.jar
```
- Step 2** Download MySQL jdbc 5.1.6 binary jar from <http://ebr.springsource.com> (search for com.springsource.com.mysql.jdbc and download version 5.1.6 from the link).
- Step 3** Rename the downloaded jar file to `jdbc_5_1_6.jar` and copy the jar file to `/var/broadhop/jdbc/` directory on all CPS boxes.
- Step 4** Synchronize all the boxes and then restart CPS.

## Deployment Management Console

Deployment Management Console feature is released as patch over 6.1 release build. Patch release covers instructions to install the feature in the setup environment.

- 
- Step 1** Download `qps_mgmt_console.zip` to `/tmp` directory.
- Step 2** Unzip `qps_mgmt_console.zip` to `/tmp` directory.
- Step 3** Run `update_console.sh` from `/tmp` directory.
- Step 4** Execute the command `qps_management_console` to check management console is installed or not.

## RAR Fix for GR Setup

The following configuration changes need to be done:

- 
- Step 1** Add SiteId and RemoteSiteId VM arguments in all `qns.conf` files mentioned below, so that all outbound messages get processed by RemoteSite when GGSN link failure occurs on Site.

```
-DSiteId=Site1
```

```
-DRemoteSiteId=Site2
```

Files that need to be updated:

```
/etc/broadhop/diameter_endpoint/qns.conf, /etc/broadhop/diameter_endpoint_stby/qns.conf,
```

```
/etc/broadhop/iomanager01/qns.conf,
```

```
/etc/broadhop/iomanager02/qns.conf,
```

```
/etc/broadhop/iomanager_stby_01/qns.conf,
```

```
/etc/broadhop/iomanager_stby_02/qns.conf,
```

```
/etc/broadhop/pcrf/qns.conf,
```

```
/etc/broadhop/pcrf_stby/qns.conf,
```

```
/etc/broadhop/qns.conf,
```

- Step 2** Similarly, the user needs to configure the following VM arguments in the above mentioned files in other sites.

```
-DSiteId=Site2 (should be same as RemoteSiteId of other site)
```

```
-DRemoteSiteId=Site1 (should be same as SiteId of other site)
```



**Note**

-DSiteId and -DRemoteSiteId values can be custom names. The purpose of the naming conversion is useful in finding out from which site CPS is sending outbound messages.

---

## Upgrade Portal DB Arbiter from pcrfclient01 to sessionmgr01

---

- Step 1** Login to pcrfclient01.

- Step 2** Stop portal DB arbiter on pcrfclient01.

```
[root@pcrfclient01 ~]# /etc/init.d/portalDB-27749 stop
```

```
[root@pcrfclient01 ~]# chkconfig --del portalDB-27749
```

- Step 3** Start portal DB arbiter on sessionmgr01.

```
[root@sessionmgr01 ~]# /etc/init.d/portalDB-27749 start
```

If it fails to start, then create a directory called `portal.1` in `/data` on sessionmgr01 and start it.

```
[root@sessionmgr01 ~]# chkconfig --add portalDB-27749
```



**Step 4** On pcrfclient01, execute the command.

```
scp /etc/init.d/portalDB-27749 sessionmgr01://etc/init.d/
```

**Step 5** Modify portal replication set (add sessionmgr01 arbiter and remove pcrfclient01 arbiter).

```
[root@pcrfclient01 ~]# mongo portal01:27749
```

```
portal01:PRIMARY> rs.addArb("sessionmgr01:27749") output is:
```

```
{ "down" : [ "sessionmgr01:27749" ], "ok" : 1 }
```

```
portal01:PRIMARY> rs.remove("pcrfclient01:27749")
```

output is:

```
Wed Apr 2 03:33:16.371 DBClientCursor::init call() failed Wed Apr 2 03:33:16.372 Error: error
doing query: failed at src/mongo/shell/query.js:78 Wed Apr 2 03:33:16.373 trying reconnect to
portal01:27749 Wed Apr 2 03:33:16.374 reconnect portal01:27749 ok
```

**Step 6** Verify portal replica set.

```
[root@pcrfclient01 ~]# diagnostics.sh --get_replica_status
```

## Peer Connection with GGSN not Coming UP on new OVF for AIO Setup

**Problem** In Policy builder we observe that Diameter stack definition is given at two places i.e. under system-1 as well as under cluster. Hence the configuration defined under System is not being applied and so the peer connection with GGSN is not established.

**Configuration:** It comes as default when we deploy OVF for AIO.

**Explanation** CER/CEA is not exchanged. Hence the configuration defined under System is not being applied and so the peer connection with GGSN is not established.

**Recommended Action** Remove the Diameter Stack configuration from Cluster.

## Generate Certificate for SSL and CA

Generate a key and a certificate using openssl and concatenate them in a file, the certificate first, then the key.

**Step 1** Go to directory `/etc/pki/tls/certs`.

**Step 2** Create the following directories under certs directory as follows:

1. `mkdir Certificates`
2. `mkdir Keys`
3. `mkdir CSR`

**Step 3** Create file `index.txt` under certs directory:

```
touch index.txt
```

**Step 4** Create file serial under certs directory:

```
cat "01" > serial
```

**Step 5** Create a private key of CA.

```
openssl genrsa -des3 -out Keys/RootCA.key 2048.
```

**Step 6** Create self-signed certificate of CA.

```
openssl req -config /etc/pki/tls/openssl.cnf -new -x509 -days 360 -key Keys/RootCA.key -out
Certificates/RootCA.crt
```

**Step 7** Create private key for the server.

```
openssl genrsa -des3 -out Keys/server.key 2048
```

**Step 8** Create CSR for the server.

```
openssl req -config /etc/pki/tls/openssl.cnf -new -key Keys/server.key -out CSR/server.csr
```

**Step 9** Create server certificate.

```
openssl ca -config /etc/pki/tls/openssl.cnf -days 360 -in CSR/server.csr -out Certificates/server.crt
-keyfile Keys/RootCA.key -cert Certificates/RootCA.crt -policy policy_anything
```

**Step 10** Remove passphrase from private key so that while starting/restarting the HA proxy it won't ask for passphrase.

```
cp RootCA.key RootCA.key.orig
openssl rsa -in RootCA.key.orig -out RootCA.key
cp server.key server.key.orig
openssl rsa -in server.key.orig -out server.key
```

**Step 11** Copy and paste the RootCA and server certificate and key as certificate first and then the key to a file; For example

```
vi /etc/pki/tls/certs/haproxy.pem
-----BEGIN CERTIFICATE-----
MIIBrzCCARgCCQCfMsCGwq31yzANBjkqhkiG9w0BAQUFADAcMR0wGAYDVQQDExF3
d3cuZXhjZWxpYW5jZS5mcjAeFw0xMjA5MDQwODU3MzNaFw0xMzA5MDQwODU3MzNa
MBwxGjAYBgNVBAMTEXd3dy5leGNlbG1hbmNlLmZyMIGfMA0GCSqGSIb3DQEBAQUA
A4GNADCBiQKBgQDFxSTUwX5RD4AL2Ya5t5PAaAjcwPa3Km40uaPKSH1U8AMydxCl
wB4L0k3Ms9uh98R+kIJS+TxdfDaYxk/GdDYI1CMm4TM+BLHGAVA2DeNf2hBhBRkb
TAgxCxXwORJQSB/B+1r0/ZiQ2ig5Jzr8xGHZ+tBsHYZ+t+RmjZPQFjnlewIDAQAB
MA0GCSqGSIb3DQEBBQUAA4GBABqVuloGWHReSGLY1yAs20uhJ3j/9SvtoueyFBag
z5jX4BNO/4yhpKEpCGmzYtjr7us3v/s0mKoIVvAgah778rCZW3kF1Y6xR6TYqZna
```

```

1ryKB50/MJg9PC4LNL+sAu+WSslof6+6Ru5N3JjhIZST8edJsGDi6/5HTKogyvkp
wOMn
-----END CERTIFICATE-----
-----BEGIN RSA PRIVATE KEY-----
MIICXgIBAAKBgQDFxSTUwX5RD4AL2Ya5t5PAaNjcwPa3Km40uaPKSHlU8AMydxCl
wB4L0k3Ms9uh98R+kIJS+TxdfDaYxk/GdDYI1CMm4TM+BLHGAVA2DeNf2hBhBRkb
TAGxCxXwORJQSB/B+lR0/ZiQ2ig5Jzr8xGHZ+tBsHYZ+t+RmjZPQFjnlewIDAQAB
AoGBALUeVhuuVLOB4X94qGSe1eZpXunUol2esy0AMhtIAi4iXJsz5Y69sgabg/qL
YQJVOZO7Xk8EyB7JaerB+z9BIFWbZwS9HirqR/sKjjbhu/rAQDgjVWw2Y9sjPhEr
CEAvqmQskT4mY+RW4qz2k8pe4HKq8NAFwbe8iNP7AySP3K4BAkEA4ZPBagt1JzrU
7T4BvQJhBmvNYEFviMScipHBlpwzfw+79xvZhTtxtsSBHAM9KLBqO33VmJ3C/L/t
xukW8S06ewJBAOBxU0TfS0EzcRQJ4sn78G6hTjjLwJM2q4xuSwLQDVaWwtXDI6HE
jb7HePaGBGnOrlXxEOfQZCVdDaLhX0zceQECQQDHcvc+phioGRKPOAFp1HhdfsA2
FIBZX3U90DfAXFMFKFXMiyFMJxSZPyHQ/OQkjaaJN3eWW1c+Vw0MJkGoskLlAkeA
h8xpqoFEgkXCxHIa00VpuzZEIt89PJVWhJhzMFd7yolbh4UTeRx4+xashNUHtJFG
MF+0a+990JIt3wBn7hQ1AQJACScT3p6zJ4llm59xTPeOYpSXy1lR4GMilsGIRNZT
RGYxcvqR775RkAgE+5DHmAksW7TBaxcO6+C1+LJEwFRxw==
-----END RSA PRIVATE KEY-----

```

**Step 12** Save and close the file haproxy.pem and edit the configuration file /etc/haproxy/haproxy.cfg.

**Step 13** Go to section listen controlcenter\_proxy and add the following lines:

```

listen andsf_proxy

bind *:8071 ssl crt /etc/pki/tls/certs/haproxy.pem ca-file /etc/pki/tls/certs/Certificates/RootCA.crt
    verify optional

default_backend andsf_server

backend andsf_server

option httpchk GET /Security.html

server srv1 qns01:9091 check inter 30s

server srv2 qns02:9092 check inter 30s

```

A sample configuration section of haproxy.cfg for ssl looks as follows;

```
listen andsf_sproxy
    bind *:8071 ssl crt /etc/pki/tls/certs/haproxy.pem ca-file
    /etc/pki/tls/certs/Certificates/RootCA.crt verify required

    default_backend andsf_server

backend andsf_server
    server srv1 qns01:9191 check inter 30s
    server srv1 qns02:9191 check inter 30s
```

## Limitations and Restrictions

CPS has the following limitations and restrictions:

- After database role change for multiple sessionMgrs, CPS is unable to stabilize the calls and timeouts happen constantly.
- On receiving Accounting Stop message, the Radius call is not disconnected and the session is also present in mongo database.
- Session viewing capability in Policy builder is deprecated and will not be available in future versions.
- It is recommend to use Control Center for viewing the session details.

## Caveats

The following sections lists Open Caveats and Resolved Caveats for CPS. For your convenience in locating caveats in Cisco's Bug Toolkit, the caveat titles listed in this section are drawn directly from the Bug Toolkit database. These caveat titles are not intended to be read as complete sentences because the title field length is limited. In the caveat titles, some truncation of wording or punctuation might be necessary to provide the most complete and concise description.



### Note

If you are a registered cisco.com user, view Bug Toolkit on cisco.com at the following website:

<https://tools.cisco.com/bugsearch>

To become a registered cisco.com user, go to the following website:

[https://tools.cisco.com/RPF/register/register.do?exit\\_url=](https://tools.cisco.com/RPF/register/register.do?exit_url=)

## Open Caveats

Table 1 lists the open caveats in the CPS 6.1 release.

**Table 1** Open Caveats

CDET ID	Status	Headline
<a href="#">CSCuo51335</a>	A	QPS: Peer connection with GGSN not coming up on new OVF for QPS_6.1_AIO
<a href="#">CSCug21376</a>	A	QNS: Displaying wrong value of rule in services in policy builder.
<a href="#">CSCug39309</a>	A	RADIUS: [QNS-1530] Integration of Control Center and ISG query isn't working
<a href="#">CSCui00922</a>	A	QNS_HA: Exception error seen in logs on service startup on lb nodes
<a href="#">CSCui78870</a>	A	Amount field is not required for Quota Template
<a href="#">CSCuj34878</a>	A	GR: Fallback of qps-vip-standby to qps-vip not taking place
<a href="#">CSCul20601</a>	A	Radius Disconnect message is not logged in Engine log.
<a href="#">CSCul20931</a>	A	PortalProxyExternalCurrentsessions SNMP KPI cannot be retrieved
<a href="#">CSCul34049</a>	A	Not all KPIs available via SNMP in default deployment
<a href="#">CSCul71020</a>	A	CSCul64768,CSCul49223 Review Comments - Refactoring of \"addAVPs\" method
<a href="#">CSCum11515</a>	A	no web redirection to original web-page after successful authentication on QPS
<a href="#">CSCum15366</a>	A	Policy Builder: Switching between profile sources in PB not working
<a href="#">CSCum48808</a>	A	Policy Builder Usability Enhancements
<a href="#">CSCum65906</a>	A	QNS: Exception observed when manually add CRD in CC
<a href="#">CSCum68136</a>	A	Deployment Management Console has display issues
<a href="#">CSCum73214</a>	A	OSGi container should take latest version jar, but it is not happening.
<a href="#">CSCum74721</a>	A	QNS[Sys-Test]: typo error observed for SNMP traps for following logs
<a href="#">CSCum77036</a>	A	OneTimeUsageCharge error on RadiusAccountingTotalBytesRetriever
<a href="#">CSCum86397</a>	A	Address Diameter related FindBugs warnings reported by Jenkins
<a href="#">CSCun01704</a>	A	QPS-org.springframework.security.access.event.AuthorizationFailureEvent
<a href="#">CSCun23514</a>	A	Proper check needed for RESOURCEGROUP value in esx.conf
<a href="#">CSCun25939</a>	A	Incorrect error when a invalid VSWITCH entry is in esx.conf
<a href="#">CSCun28546</a>	A	Validation failed when any config has DEVICE assigned/n in network.conf
<a href="#">CSCun28576</a>	A	Validation failed when any config entry has invalid IP in network.conf
<a href="#">CSCun28671</a>	A	Validate format of each config entry in network.conf
<a href="#">CSCun28846</a>	A	Validation needed when QNS, PORTAL and PCRFCLIENT entries has same IP
<a href="#">CSCun28895</a>	A	Validation required to check uniqueness of host names in network.conf
<a href="#">CSCun31441</a>	A	Validate if datastore is valid in qns.conf
<a href="#">CSCun31456</a>	A	Validate incorrect Disk Format Option in qns.conf

**Table 1**      **Open Caveats**

<b>CDET ID</b>	<b>Status</b>	<b>Headline</b>
<a href="#">CSCun31481</a>	A	Display correct error message when quotes are missing in qns.conf
<a href="#">CSCun31513</a>	A	Validate format of CC_ASSIGN and QS_ASSIGN
<a href="#">CSCun34068</a>	A	Deploy_qns.sh should check RAM assigned in CC_CONFIG & QS_CONFIG
<a href="#">CSCun34156</a>	A	Deploy_qns.sh should check CPU's assigned in CC_CONFIG & QS_CONFIG
<a href="#">CSCun34212</a>	A	Check syntax and format of CC & QS CONFIG in qns.conf
<a href="#">CSCun34332</a>	A	[QPS.6.0.1] QPS Policy builder Errors out after "\"restartall.sh\""
<a href="#">CSCun45498</a>	A	QNS[Sys-Test]: JmsDestinationStatus warning
<a href="#">CSCun57296</a>	A	Need to handle warnings during OVF install.
<a href="#">CSCun57593</a>	A	ESXiHOST does not recognize is_resourcegroup checking.
<a href="#">CSCun59674</a>	A	QPS 6.1 SNMP: RadiusConnectionError traps not being sent
<a href="#">CSCun60571</a>	A	QPS 6.1 SNMP: Unable to produce MemcachedInternalError traps
<a href="#">CSCun70637</a>	A	QNS: While creating a service offer in portal, no service is displayed.
<a href="#">CSCun73319</a>	A	QNS: proper err msg should be displayed while mongo authentication failed
<a href="#">CSCun83797</a>	A	wrong release number displayed on OVF distribution VM's login screen.
<a href="#">CSCun99695</a>	A	False DB Alarms generated on GR setup
<a href="#">CSCuo00338</a>	A	6.0.1 upgrade script not removing old jar files
<a href="#">CSCuo04093</a>	A	QNS Sec: Direct Access to Admin Pg security issues observed QPS 6.1 PB
<a href="#">CSCuo04514</a>	A	QPS upgrade: After upgrade DIAMETER_UNABLE_TO_COMPLY.
<a href="#">CSCuo04540</a>	A	QPS upgrade: bugs in upgrade from 5.3.5 to 6.1
<a href="#">CSCuo04636</a>	A	QNS: QNS updates both BganMonthlyFapVolume and LastFAPVolume in CC.
<a href="#">CSCuo04686</a>	A	PCRF LB01/02 internal IPs advertised in Host-IP-Address in CEA
<a href="#">CSCuo08815</a>	A	Gx TCP sessions take >90s to re-establish upon lb switchover
<a href="#">CSCuo11071</a>	A	QPS:pcrfclient01 crashed due to high CPU usage on idle system
<a href="#">CSCuo11893</a>	A	QPS VRoGx Bandwidth Monitoring - RAR un-throttles a high usage sub
<a href="#">CSCuo12900</a>	A	QNS[Sys-Test]: Blueprint Error observed when LDAP feature is enabled on
<a href="#">CSCuo14378</a>	A	PB Copy UCT and create fresh UCT exhibit different behaviors
<a href="#">CSCuo15288</a>	A	QPS Internal OCS using Gx and Gy improperly handles Quota depletion.
<a href="#">CSCuo16673</a>	A	QNS: QNS auto provision the balance with unit bytes irrespective of ABT
<a href="#">CSCuo20926</a>	A	QPS: startall.sh not working
<a href="#">CSCuo21365</a>	A	Radius WLC: Blank Access Accept sent for WLC when template configured
<a href="#">CSCuo22996</a>	A	OpenSSL Heartbeat Extension Vulnerability in QPS
<a href="#">CSCuo24180</a>	A	Test Case Failure due to Service Missing in regression

**Table 1**      **Open Caveats**

<b>CDET ID</b>	<b>Status</b>	<b>Headline</b>
<a href="#">CSCuo27076</a>	A	QPS responds with Diameter_Unable_to_Comply (5012) for CCR-U
<a href="#">CSCuo27897</a>	A	ISG Prepaid use case fails with AutoProvisionQuota service configuration
<a href="#">CSCuo30008</a>	A	Usage monitoring disables bandwidth monitoring when quota is depleted
<a href="#">CSCuo30305</a>	A	AppScan VT test found low severity issue in PB
<a href="#">CSCuo31963</a>	A	SNMP trap is not being generated when application is down on AIO
<a href="#">CSCuo33194</a>	A	QPS is running as root instead of a non-privileged user
<a href="#">CSCuo33328</a>	A	update_sys_files.sh has no roll-back options
<a href="#">CSCuo36066</a>	A	QPS replying late to CCR-U message when both balance_DB ports are down.
<a href="#">CSCuo36305</a>	A	Update PAX-WEB
<a href="#">CSCuo40940</a>	A	QPS: Modified \"QoS-Information. Bearer-Identifier\" not present in CCA-U
<a href="#">CSCuo41255</a>	A	QPS: QPS is unable to forward Gy CCA-I when CDR table enabled
<a href="#">CSCuo42594</a>	A	QNS[Sys-Test]: Discrepancy found in Device protocol in Gx/Gy Proxy mixcal
<a href="#">CSCuo43750</a>	A	6.1:GR_SysTst:EDR is not properly generating for rule name add/remove
<a href="#">CSCuo46067</a>	A	QPS: Disk Space usage on AIO
<a href="#">CSCuo47785</a>	A	6.1:GR_SysTst: Java process down with SIGSEGV on qns06 of standby site
<a href="#">CSCuo48146</a>	A	6.1:GR_SysTst:No RAR is sending by QPS after recurring quota code refresh
<a href="#">CSCze10322</a>	A	Multiple Prepaid - Change From Stackable to Not Stackable - no en...
<a href="#">CSCze10335</a>	A	Multiple Prepaid - Edge Case - handling of activating 2nd quota w...
<a href="#">CSCum40321</a>	N	QNS[Sys-Test]: Site1 chassis sessionmgr02 slow resp lots Time outs seen
<a href="#">CSCum85913</a>	N	QNS[Sys-Test]: Site1+Site1Arbiter+Site2Arbiter dwn err on site2 diagnostic
<a href="#">CSCun54620</a>	N	No guidance in set_config.sh 4 config dir values: general general_mobile
<a href="#">CSCun63619</a>	N	Hybrid service: 2 DPIs, 1 PCRF
<a href="#">CSCun82249</a>	N	TAC: snmp KPI sessioncount shows double count seen in session_cache db
<a href="#">CSCuo04132</a>	N	QNS Sec: \"Information leakage\" issues observed with QPS 6.1 PB
<a href="#">CSCuo04142</a>	N	QNS Sec: \"TRACE and TRACK HTTP Methods Enabled\" issues in QPS 6.1 PB
<a href="#">CSCuo04147</a>	N	QNS Sec: \"Application Test Script Detected\" issues in QPS 6.1 PB
<a href="#">CSCuo16723</a>	N	QPS_mgmt_console providing misleading message after script execution
<a href="#">CSCuo23197</a>	N	QPS did not generate consolidate logs after upgrade to 6.0.1
<a href="#">CSCuo23928</a>	N	QNS: Console is getting closed after resized TUI window if no logs found.
<a href="#">CSCuo26402</a>	N	QNS: pcrf_A/pcrf_B is not present in configurations in TUI window
<a href="#">CSCuo27610</a>	N	Wrong QPS version is displayed on the deployment VM's login banner

**Table 1**      **Open Caveats**

<b>CDET ID</b>	<b>Status</b>	<b>Headline</b>
<a href="#">CSCuo28811</a>	N	QPS upgrade: documentation: Update_qns failing without set_permission.sh
<a href="#">CSCuo29451</a>	N	6.1: QPS upgrade failed using bin file
<a href="#">CSCuo30088</a>	N	QPS_6.1_SPRINT6 OVF's have extra repository in /var/broadhop/repositories
<a href="#">CSCuo31251</a>	N	QCI/priority values of default bearer are not applying as expected
<a href="#">CSCuo31259</a>	N	AVP Substitution for Sub Account in 5.5.3
<a href="#">CSCuo31728</a>	N	Cell-Congestion Provisioning SNMP trap forwarding issue
<a href="#">CSCuo31836</a>	N	CI: Gx Dictionary is not aligned with QPS dictionary
<a href="#">CSCuo35130</a>	N	"Service qns stop" is taking forever to stop qns service.
<a href="#">CSCuo35140</a>	N	restartall.sh does not work after system upgrade using .bin
<a href="#">CSCuo35198</a>	N	AN-GW_Address option for CRD
<a href="#">CSCuo35240</a>	N	QPS_6.1 SNMP: LicensedSessionCreation traps not being sent
<a href="#">CSCuo36244</a>	N	629937353: QPS v5.3.4 JMS Errors
<a href="#">CSCuo36253</a>	N	EPN3.0: Null-pointer exception in UpdateSubscriberResponse
<a href="#">CSCuo36722</a>	N	QPS_6.1 VM sizing is too small
<a href="#">CSCuo38774</a>	N	IP Central security issue found with Spring Framework 3.0.5 in QPS5.5.MR3
<a href="#">CSCuo39589</a>	N	Two blade configuration needs to support failover
<a href="#">CSCuo41046</a>	N	QPS: wrong errormessage with error code=2 UpdateSubscriberResponse
<a href="#">CSCuo41080</a>	N	QPS: unable to search subscriber using networkId as filter
<a href="#">CSCuo41504</a>	N	Upgrade: Question after size reqs. defaulting to "yes" should be "no"
<a href="#">CSCuo43096</a>	N	Modify BROADHOP-QNS-MIB.txt file to remove unsupported KPIs
<a href="#">CSCuo44008</a>	N	6.1: GR_SysTst: Getting error for Policy Reporting Policy Cdrs EventRecords
<a href="#">CSCuo46183</a>	N	QNS: SNMP trap exception is observed in QNS log in HA setup.
<a href="#">CSCuo46858</a>	N	Gy 3GPP-SGSN-MCC-MNC AVP is not supported as a Initiator or condition
<a href="#">CSCuo47875</a>	N	QPS: need to reduce log severity level for some case
<a href="#">CSCuo48615</a>	N	QNS: For wrong session ID QNS does not send diameter result code 5002
<a href="#">CSCug45709</a>	O	QNS: Not able to edit or remove the values in service option once we save
<a href="#">CSCui30480</a>	O	QNS SEP: No log for offln evnt notif record change to "NOFITY" in MongoDB
<a href="#">CSCuj85200</a>	O	QNS[Sys-Test]: qns01 /var partition full due to java_pid20885.hprof dump
<a href="#">CSCun11405</a>	O	Check for affected flow returns wrong value
<a href="#">CSCuo00524</a>	O	QPS_6.1_SPRINT5 OVF's: Network configuration fails
<a href="#">CSCun34299</a>	O	QPS_6.1_SPRINT3 OVF's have extra filesystems in snmpd.conf



**Table 1** Open Caveats

CDET ID	Status	Headline
<a href="#">CSCun83125</a>	O	BufferLimit HaspMap exception err observe in 72hr longevity
<a href="#">CSCuo28831</a>	O	QPS upgrade: remove step synconfig from manual steps after upgrade.

A - Assigned

N - New

O - Opened

## Resolved/Verified Caveats

[Table 2](#) lists the resolved/verified caveats in the QPS 6.1 release.

**Table 2** Resolved/Verified Caveats

CDET ID	Status	Headline
<a href="#">CSCuo18403</a>	C	6.1[GR-sys-test]: Continuous timeouts during plain longevity post 14 hrs
<a href="#">CSCuo09710</a>	C	6.1:GR_SystemTest: Plain Longevity failed due to hprof dump on lb01 site1
<a href="#">CSCun24663</a>	C	QNS[Opt-Sys]: Cache data is out of date errors seen in qns logs
<a href="#">CSCum35656</a>	C	create_policy_builder_user.sh creates same user in users-access-file
<a href="#">CSCum41384</a>	C	Use of \"Realtime Notifications\" is not correct in PB
<a href="#">CSCum60141</a>	C	Customer reference data is not displaying checkboxex
<a href="#">CSCum70763</a>	C	qns consolidated logging doesn't worked after upgrade from 6.0 to 6.1
<a href="#">CSCum79055</a>	C	Dummy Test Bug to check TEACAT is generated for customer found issues
<a href="#">CSCum84102</a>	C	Gy provisioning for SessionWallet fails.
<a href="#">CSCun13921</a>	C	Log rotate failing on hourly run
<a href="#">CSCun18317</a>	C	FAILURE IN Gx PROXY CALL FLOW
<a href="#">CSCun18595</a>	C	Proxy: Sy Proxy not sending error to the client received from Server
<a href="#">CSCun42783</a>	C	Session removed due to no service associated.
<a href="#">CSCun44542</a>	C	QNS[Opt-Sys]: Getting timeout inSite1 after sesn adm db recove manual
<a href="#">CSCun53396</a>	C	qps routing policy not enabled for outgoing packets
<a href="#">CSCun60509</a>	C	SVN repo on perfclient01 and perfclient02 are not in sync.
<a href="#">CSCun92292</a>	C	Rollback 6.1 to 5.5.1 -- CC fails: 503 Svc Unavail
<a href="#">CSCuo00672</a>	C	Add new logger to logback is not persistent after upgrade...
<a href="#">CSCuo06520</a>	C	Sanity Failed for 6.1.0 and 6.0.1
<a href="#">CSCuo19325</a>	C	QPS: NPE for TraceDatabase (TraceDatabase.java:194)
<a href="#">CSCuo24375</a>	C	Test Case Failure due to Script damage in regression
<a href="#">CSCuo31634</a>	C	Test case failure due to rule name was missing, Wrong Qos Value in PB.
<a href="#">CSCuo22017</a>	R	On Debit No RAR for Quota depletion, balance amount as Use Case Initiator
<a href="#">CSCuo18517</a>	R	6.1:GR_SysTst:Balance not associating for few subs during provisioning

**Table 2**      **Resolved/Verified Caveats**

<b>CDET ID</b>	<b>Status</b>	<b>Headline</b>
CSCuo15570	R	SPR subscriber search failing due to reg_expr by default enabled in PB
CSCuo13470	R	QPS: QPS not sending resultcode 5065 in Rx AAA when no Gx session
CSCun47094	R	QPS did NOT send RAR in the condition of congestion change
CSCum24873	R	Interface Integra/PCRF for resolving IP address to MSISDN
CSCum25266	R	Package-ID AVP for SIG
CSCum35454	R	Request usage report when Gx usage monitoring key is disabled
CSCum35467	R	Request usage report when bandwidth monitoring is removed
CSCum41506	R	Control Center Import Progress Dialog not centered
CSCum46216	R	Import should not allow duplicate rows
CSCum46301	R	PB should not allow duplicates in Static Valid Values for Cust Ref Data
CSCum53235	R	QueryBalanceRequest Unified API response is not proper.
CSCum53694	R	Chart windows not resizing correctly in Monitoring Dashboards
CSCum54049	R	ISG Prepaid balance reservation error
CSCum55551	R	Update the Policy Builder /welcome URL to automatically redirect to /pb
CSCum63351	R	Some AVPs are missing in Sy STA response
CSCum65042	R	SPR Database encryption step missing in QPS 6.0
CSCum65054	R	Undefined domain created after QPS 6.0 upgrade
CSCum67372	R	TM - EDR Configuration Caused Traffic Issue, Help Configuring needed
CSCum67913	R	Missing details of severity 8 and 9 in SNMP Guide
CSCum68117	R	Deployment Management Console missing the functions mentioned in 6.0 RN
CSCum71743	R	Multi Site SPR Key generation
CSCum72052	R	As a service provider, I need take into account the user's time zone
CSCum75668	R	Policy Reporting config did not get update post QPS upgrade
CSCum76695	R	haproxy version 1.5 not available in QPS 6.0 lb VMs
CSCum80483	R	Eliminate unnecessary pausing to recompile policy rules
CSCum86508	R	add diagnostic for the shardinterface to send traps
CSCum89186	R	QPS: Null Pointer Exception on null network device manager
CSCun00369	R	TAC: no SNMP trap is generated with a qns process dies
CSCun02406	R	QNS: The balance is not created properly in CC.
CSCun13748	R	CiscoContentFilterPolicyId value stored in the session all the time
CSCun19500	R	UNKNOWN hostname (26878.100.1.1.7) & ComponentID (26878.100.1.1.9) Found
CSCun19662	R	Bearer-id AVP must be present & NON-ZERO within QoS-Information in CCA-U
CSCun20742	R	Enhancement to report error on provisioning new balance...
CSCun21967	R	QPS: LAB1-Traffic coming on lb01 is getting distributed
CSCun22043	R	OCSThreshold Breach and Status not triggering state change with ALU

**Table 2** *Resolved/Verified Caveats*

<b>CDET ID</b>	<b>Status</b>	<b>Headline</b>
CSCun29749	R	QPS does not send DPR in case of LB reboot or shutdown
CSCun29928	R	License alarm enhancement with additional detailed requirement
CSCun35362	R	update build_set.sh so that it wont ask for usr input for default operat
CSCun49023	R	JMX connection issue prevents flow control of messages
CSCun49431	R	QPS: URLs in about.sh are static
CSCun53390	R	QPS 6.1: diagnostics.sh doesn't check if replica sets are configured
CSCun54556	R	need to check license manager service as part of installing license
CSCun60576	R	pcrfclient01 and portal01 on same host breaks redundancy.
CSCun60602	R	Redundancy issue when two specific blades goes down.
CSCun60866	R	Allow control center monitoring to be disabled from the qns.conf
CSCun65135	R	getExternalProfile() is called multiple times on external profile update
CSCun66318	R	UsageMonitoringKey sends incorrect Monitoring Key
CSCun66412	R	Portals need to have Gateway assigned in network.conf
CSCun76981	R	SessionDuration field needs to be changed in blueprint.
CSCun77738	R	GR diameter failover for the mid call -- CCRu not processed by QPS
CSCun79941	R	PolicyIntel PostgreSql Integration
CSCun84309	R	!isNull matches empty field in CRD table
CSCun97087	R	Ports that need to be opened on production
CSCun97867	R	QPS: Policy Builder doesn't respect -DcheckReadOnlyUser= false
CSCuo00481	R	Gy CDRs
CSCuo03690	R	Upgrade AIO from 5.5 to 6.1: getting error when collectd service start
CSCuo03740	R	Automate Upgrade: Update disk space warning with new calculation
CSCuo16563	R	QPS: NPE is observed when qns receives decreased FAPVOL for existing acc
CSCun64063	R	Charge against reservation does not work with 2 Gy sessions.
CSCun69972	R	Duplicate EDR Data
CSCuo09537	R	CRD data not mapping into Access-Accept Packet
CSCun43000	R	QPS_6.1_SPRINT3 SNMP: JMSSConnectionError traps not being sent
CSCuo16450	R	QNS: QPS doesn't update FAPVolume on receiving null FAPVolume in STD.
CSCuo24339	R	GY Message Structure should be proper in automated scripts
CSCuo29155	R	QPS: Multiple duplicate messages.
CSCuo30783	R	Mongo arbiter processes do not start on SPRINT6 OVFs
CSCuo44876	R	QPS_6.1_SPRINT7 deployment echoes root password back in cleartext
CSCuo09693	V	Upgrade: Process should NOT overwrite /etc/broadhop/portal/broadhop.php
CSCun98736	V	stopall.sh not stopping qns on lb and qns VMs on 6.1 build on GR
CSCun98085	V	GR - Need to run qns as root to overcome firewall and network issues
CSCun96799	V	QPS: Stage update failed with collectd and license issues on AIO

**Table 2**      **Resolved/Verified Caveats**

<b>CDET ID</b>	<b>Status</b>	<b>Headline</b>
CSCun93929	V	QNS[Sys-Test]: Unable to Proxy Request
CSCun27279	V	QPS: Sy Proxy not sending the Failure cause when server is Down
CSCun20726	V	QNS: User able to create duplicate diameter agents
CSCum58287	V	Not able to add policies when start from scratch
CSCuo11955	V	QPS returning 'Diameter_too_busy' error with Createbalance API
CSCuo11524	V	QPS:QPS throws error when User-Equipment-Info AVP configured in CRD
CSCuo06508	V	QPS: New Update Method_Mongo_RPM
CSCuo04552	V	QPS upgrade: After upgrade from 5.3.5 to 6.1 synconfig failing.
CSCuo04358	V	QPS:RAR not being sent on 6.0.1 release build
CSCuo04239	V	QPS: New update method_Target Version
CSCuo04034	V	QNS Sec: VT noticed Path Traversal issue with 6.1 QPS Policy Builder
CSCuo02514	V	QNS[Sys-Test]: sessionmgr failover results in diameter peer flap
CSCun99735	V	RPM Dependency check failed while doing upgrade on AIO.
CSCun99625	V	QPS upgrade: Upgrade failing on AIO using release-train-6.1.0_42.bin
CSCun97490	V	diagnostics showing wrong error message for sessionmgr01
CSCun97073	V	QPS: After upgrade to 6.1.0.r058576 by bin update pb config are wiped out
CSCun94237	V	QPS upgrade: Manual steps for 5.3.5 upgrade should be same as 5.3.4
CSCun92650	V	Upgrade: Installer incorrectly requesting sessionmgr ports for portal
CSCun89155	V	QPS upgrade: space wasted on qns VMs.
CSCun86866	V	Upgrade: Documentation needs to include note about overwriting files
CSCun86805	V	ISG Prepaid cannot charge the last dosage
CSCun78915	V	QNS: QPS CreateSubscriberRequest with balance autoprovisioned service
CSCun78687	V	QPS upgrade: PB is not opening.
CSCun78100	V	QNS: QPS does not send RAR after Rx emergency session termination
CSCun76960	V	Service Change Not Reflected on WLC
CSCun72850	V	QPS upgrade: CCA is not coming.
CSCun70851	V	QPS upgrade: collectD is consuming too much space.
CSCun66392	V	Wrong QPS version number is displayed by the deployment VM.
CSCun62908	V	No charging information in Gx-RAR for sponsor data
CSCun61988	V	set_config.sh missing general_mobile entry when run without arguments
CSCun60558	V	qns and engine are not logging consolidated logs on perflclient02
CSCun60553	V	qns user does not have the correct password on lb02.
CSCun60545	V	Key authentication is not configured on lb02
CSCun52939	V	QPS does not send Gx RAR when get Rx AAR with Dynamic-PCC-Requested-QoS
CSCun52358	V	Application should create the tmp dir if it is not present.

**Table 2**      **Resolved/Verified Caveats**

<b>CDET ID</b>	<b>Status</b>	<b>Headline</b>
CSCun48752	V	QPS: LB's default memory of 2GB is not enough when installing diameter
CSCun48740	V	QPS: Install script doesn't assign enough memory to pcrlclient01
CSCun43062	V	QPS_6.1_SPRINT3 OVF's: bad haresources file on portalLBs
CSCun40889	V	QPS_6.1_SPRINT3 OVF's: incorrect name/severity for InvalidLicense traps
CSCun40775	V	QPS_6.1_SPRINT3 OVF's: SNMP - filesystems not monitored on portal VMs
CSCun40164	V	QPS_6.1_SPRINT3 OVF's have issues in diagnostics.ini
CSCun39746	V	QPS: QNS VM's trying to connect to 127.0.0.1:27017
CSCun39202	V	Diameter Failure due to GX QoS Issue
CSCun34531	V	QPS_6.1_SPRINT3 SNMP: blank uptime not handled by component_trap_convert
CSCun32196	V	SNMP: QPS_6.1_SPRINT3 OVF's do not monitor /data on sessionmgr VMs
CSCun30760	V	Mongo failover exception in Add service API performance Testing
CSCun31439	V	QPS 6.1 SNMP - PortalProxyExternalCurrentSessions KPI is incorrect
CSCun26548	V	SNMP: QPS 6.1_SPRINT3 OVF's have bad swap/memory/load average thresholds
CSCun26327	V	QPS 6.1 - multiple collectd restart jobs in root's crontab
CSCun23540	V	configure_esx.sh overwrites RESOURCEGROUP that already exists.
CSCum92048	V	QNS[Sys-Test]: getting error message after executing synconfig.sh script
CSCum90472	V	Stale session and session timer expiration RAR not wkg correctly (AIO)
CSCum80656	V	TAC: service-qns-x.log files do not archive
CSCum21082	V	Session wallet is not recharging once the quota is less than the dosage
CSCum30305	V	Session Wallet Enhancement
CSCum42709	V	uncontrolled generation of logs in pcrlclient01
CSCum56765	V	Copying installer files of /etc/broadhop from general to general_mobile
CSCum60330	V	QPS Upgrade from 5.5.1 to 5.5.3 failed on HA setup
CSCum72401	V	Issues with Lab Demo
CSCum74705	V	Gx session is not removed from QPS when the CCRt is received
CSCum75040	V	CC is showing No Subscribers found exists some times
CSCum77292	V	QPS sending faulty session timeout after voucher authentication
CSCum81130	V	need SNMP Trap alarm when configured license threshold is reached
CSCum85557	V	QNS: Cyrillic characters are not decoded for sms at receiver's end.
CSCum88517	V	Unified API 2.1.0 Release Notes ua.version.2.0.compatible prop
CSCum91182	V	Diameter Gx Initiator is not working - A Gx charge request exists
CSCum92829	V	create_policy_builder_user.sh updates wrong file in multi policy builder
CSCum93478	V	Invalid xml generated by QPS, not compatible with SOAP standard
CSCum93612	V	PCRF always uses the same RB as it chose first ever for an End User
CSCum96345	V	RADIUS not responding on correct IO Manager

**Table 2**      **Resolved/Verified Caveats**

<b>CDET ID</b>	<b>Status</b>	<b>Headline</b>
CSCun00316	V	Error 'invalid arithmetic operator' using bulkstat_collection.sh script
CSCun05662	V	Authorized QoS-Info Fields in EDRs
CSCun12088	V	HTTPS wsdI for UnifiedAPI unable to accessed from the SOAP UI
CSCun13673	V	Upgrade failed: QPS6.0(release) to 6.1(latest, 2/13/2014)
CSCun18337	V	QNS[Opt-Sys]: Balance TPS is very low and observing errors in tailcon log
CSCun20327	V	QPS: Unable to search subscriber with credential in CC
CSCun23123	V	QPS: management_console binaries not present in 6.1.0.r056254
CSCun23589	V	configure_esx.sh does not create a resource group when part of it exists
CSCun23665	V	Incorrect validation of parameters of VSWITCH in esx.conf
CSCun24161	V	control center username & password in cleartext
CSCun24199	V	configure_esx.sh aborted abruptly when Portal VSWITCH doesn't exits
CSCun28019	V	parameter missing on 6.0.1.r057255
CSCun29725	V	Basic GR Site outage GR failure trigger is failing
CSCun31151	V	CDR/EDRs fields of CCA-t Qos-Info are similar with CCA-i/CCA-u CDR/EDRs
CSCun37269	V	QPS_6.1_SPRINT3 OVFs: some files have bad permissions in /etc/broadhop
CSCun43205	V	QPS_6.1_SPRINT3 OVFs: LBs have developer mode enabled
CSCun44534	V	Site1 recovery is failing due to session admin db fail
CSCun54367	V	installer.bin writing to '/' -- saw '/' volume go to 0 bytes remaining
CSCun61739	V	Need changes Power ON sequence in MOP during site recovery
CSCun72719	V	QPS: PCRf doesn't send CCA-U upon receiving Charging-Rule-Report update
CSCun86088	V	QPS: Value of dedicated bearer QoS priority level is incorrectly derived QPS: about.sh shows junk output
CSCun94880	V	Upgrade from 5.5.MR1 to 6.1 with Valid License -- fails installing RPMs
CSCun95619	V	5.5.1 > 6.1 fails w/ diags: 'Error creating bean...
CSCun97507	V	GR_MOP execution on 6.1 profile refresh configuration throws errors
CSCun97541	V	pSessionMgr aliases addition should be supported in automated scripts
CSCun99511	V	Bandwidth Boost Service Activation without balance
CSCun99861	V	QPS: Issue with new upgrade method
CSCuo04159	V	QPS: about.sh shows junk output
CSCuo12011	V	Opt RAR for multiple GGSN is RAR is failing to send through standby peer
CSCuo13094	V	QNS Sec: Disable weak installation credentials after install
CSCuo13095	V	QNS Sec: Log startup and shutdown of logging/auditing
CSCuo36274	V	Upgrade: AIO Installation is not upgrading to the new portal

R - Resolved

V - Verified

C - Closed

## Related Documentation

This section contains information about the documentation available for CPS.

### Release-Specific Documents

Refer to the following documents for better understanding of Cisco Policy Suite.

- *Cisco Policy Suite 6.1 Alarming and SNMP Guide*
- *Cisco Policy Suite 6.1 Backup and Restore Guide*
- *Cisco Policy Suite 6.1 Installation Guide*
- *Cisco Policy Suite 6.1 Mobile Configuration Guide*
- *Cisco Policy Suite 6.1 Operations Guide*
- *Cisco Policy Suite 6.1 Policy Reporting Guide*
- *Cisco Policy Suite 6.1 Troubleshooting Guide*
- *Cisco Policy Suite 6.1 Wi-Fi/BNG Configuration Guide*
- *Cisco Policy Suite Control Center 3.3 Interface Guide for Full Privilege Administrators*
- *Cisco Policy Suite Control Center 3.3 Interface Guide for View Only Administrators*
- *Cisco Subscriber Services Portal 6.1 Interface Guide for Administrators*
- *Cisco Subscriber Services Portal 6.1 Interface Guide for Managers*
- *Cisco Subscriber Services Portal 6.1 Interface Guide for Front Desk Personnel*

The documents can be downloaded from the following links:

- Common Guides:  
<http://www.cisco.com/c/en/us/support/wireless/quantum-policy-suite-bng/products-installation-and-configuration-guides-list.html>
- Mobile Configuration Guide + Common Guides:  
<http://www.cisco.com/c/en/us/support/wireless/quantum-policy-suite-mobile/products-installation-and-configuration-guides-list.html>
- Wi-Fi Configuration Guide + Common Guides:  
<http://www.cisco.com/c/en/us/support/wireless/quantum-policy-suite-wi-fi/products-installation-and-configuration-guides-list.html>

## Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, using the Cisco Bug Search Tool (BST), submitting a service request, and gathering additional information, see *What's New in Cisco Product Documentation* at: <http://www.cisco.com/c/en/us/td/docs/general/whatsnew/whatsnew.html>.

Subscribe to *What's New in Cisco Product Documentation*, which lists all new and revised Cisco technical documentation as an RSS feed and delivers content directly to your desktop using a reader application. The RSS feeds are a free service.

---

This document is to be used in conjunction with the documents listed in the “[Related Documentation](#)” section.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: [www.cisco.com/go/trademarks](http://www.cisco.com/go/trademarks). Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

© 2015 Cisco Systems, Inc. All rights reserved.