



CPS UDC MoP for Session Migration, Release 18.2.0 (Restricted Release)

First Published: 2018-05-11

Last Modified: 2018-05-11

Americas Headquarters

Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
<http://www.cisco.com>
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Cisco and the Cisco Logo are trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at 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.

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.

© 2018 Cisco Systems, Inc. All rights reserved.

CONTENTS

RESTRICTED RELEASE	5
UDC SESSION MIGRATION	6
MIGRATE UDC VMs	7
CONFIGURE SESSION MIGRATION	10
<i>Domain Configuration</i>	10
<i>Policy Configuration</i>	12
VERIFY SESSION MIGRATION	14

RESTRICTED RELEASE

IMPORTANT: This is a Short Term Support (STS) release with availability and use restrictions. Contact your Cisco Account or Support representatives for more information.

UDC Session Migration

This guide describes UDC Session Migration procedures and includes the following topics:

- Migrate UDC VMs
- Configure Session Migration
- Verify Session Migration

Migrate UDC VMs

Perform the following steps to migrate UDC VMs:

Step 1 Migrate existing CPS setup to CPS 13.x ISO.

Step 2 Initialize new UDC VMs.

For more information about initializing new UDC VMs, see *CPS User Data Convergence Migration MoP for VMWare* or *CPS User Data Convergence Migration MoP for OpenStack*.

Step 3 Restart the qns processes on `pcrfclient01` and `pcrfclient02`.

Step 4 Add the following UDC Systems Configuration in Policy Builder and publish the configuration:

If you are using `systems.json` configuration, update the file with the following configurations:

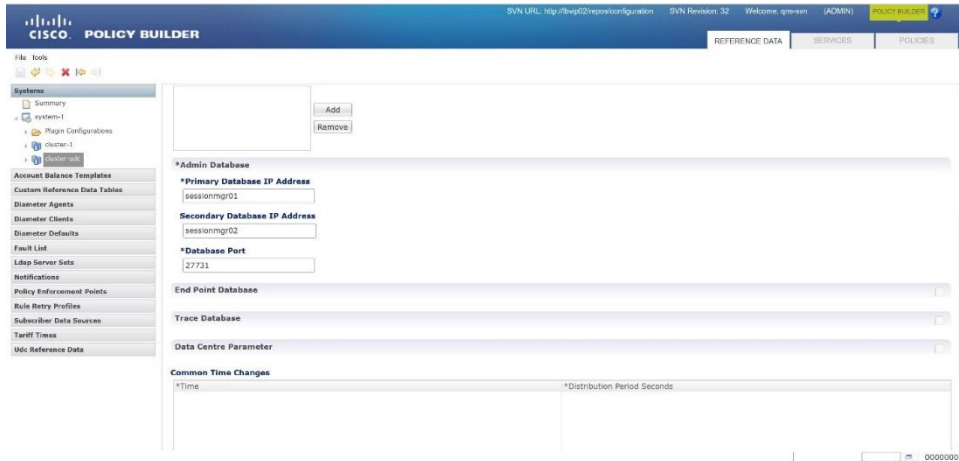
1. Log in to Policy Builder.
2. Add a new cluster under **system-1**.
3. Navigate to **Systems**.
4. Click **Create Child: Cluster**.

A new screen is displayed as follows:

The screenshot shows the Cisco Policy Builder interface. The left sidebar contains a navigation menu with categories like Systems, Plugins Configurations, Account Balance Templates, Custom Reference Data Tables, Diameter Agents, Diameter Clients, Diameter Defaults, Fault List, LDAP Server Sets, Notifications, Policy Enforcement Points, Rule Retry Profiles, Subscriber Data Sources, Swift Times, and IMC Reference Data. The main area is titled 'Cluster' and contains the following configuration fields:

- Name:** cluster-udc
- Description:** (empty)
- *Ds Write Concern:** DefaultInstanceSafe
- *Replication Wait Time:** 100
- *Min Key Cache Time Min:** 240
- *Re-evaluation diffusion buckets:** 50
- *Broadcast Msg Wait Timer Ms:** 50
- *Lookaside Key Prefixes:** (empty list with Add and Remove buttons)
- *Failover Site Ms:** 0
- *Trace Db Size Mb:** 512
- *Max Timer T P S:** 2000
- *Re-evaluation diffusion interval (in milli seconds):** 20
- *Max Sessions Per Shard:** 0
- *Admin Database:**
 - *Primary Database IP Address:** sessionmg01

5. Add the name **cluster-udc**.
6. Add the database IP and port address that are configured in `mongoConfig.cfg` for the Admin Database.



7. Add the remaining Policy Builder Systems Configuration for UDC.

For information about systems configuration, see *CPS UDC Guide*.

1. UD Interface Configuration
2. cluster-udc Configurations
 - i. UDC FE Configuration
 - ii. Diameter Configuration
 - iii. Ldap Server Configuration

NOTE: In order to configure Ldap Server Configuration, Ldap Server Sets have to be configured. To configure Ldap Server Sets, see *CPS Mobile Configuration Guide*.

Step 5 Publish Policy Builder configurations.

Step 6 Run `restartall.sh`.

Step 7 From Installer, log in to UDC Admin DB using `mongo sessionmgr01:xxxxx`.

Where `xxxxx` is the port number of the new UDC Admin DB.

Verify if the values for `seed_1`, `seed_2`, and `port` corresponds to the values that is in the `session.db.init` parameters in `/etc/broadhop/udc/qns.conf` by running the following command from the MongoDB shell:

```
set06:PRIMARY> db.shards.findOne()
{
  "_id" : 1,
  "seed_1" : "sessionmgr01",
```



```
"seed_2" : "sessionmgr02",  
"port" : 27727,  
"db" : "session_cache",  
"online" : true,  
"count" : NumberLong(5),  
"lockTime" : ISODate("2017-06-29T20:47:43.690Z"),  
"isLocked" : false,  
"lockedBy" : null  
}
```

Step 8 Verify that processes on each UDC VM are up and running by running the following command:

```
ssh udc<xx> service qns status
```

Step 9 Verify that QNS UDC Client is up and running by running the following command:

```
diagnostics.sh
```

The following clean diagnostics.sh output indicates that the QNS UDC Client is up and running:

```
(all [PASS])
```

Configure Session Migration

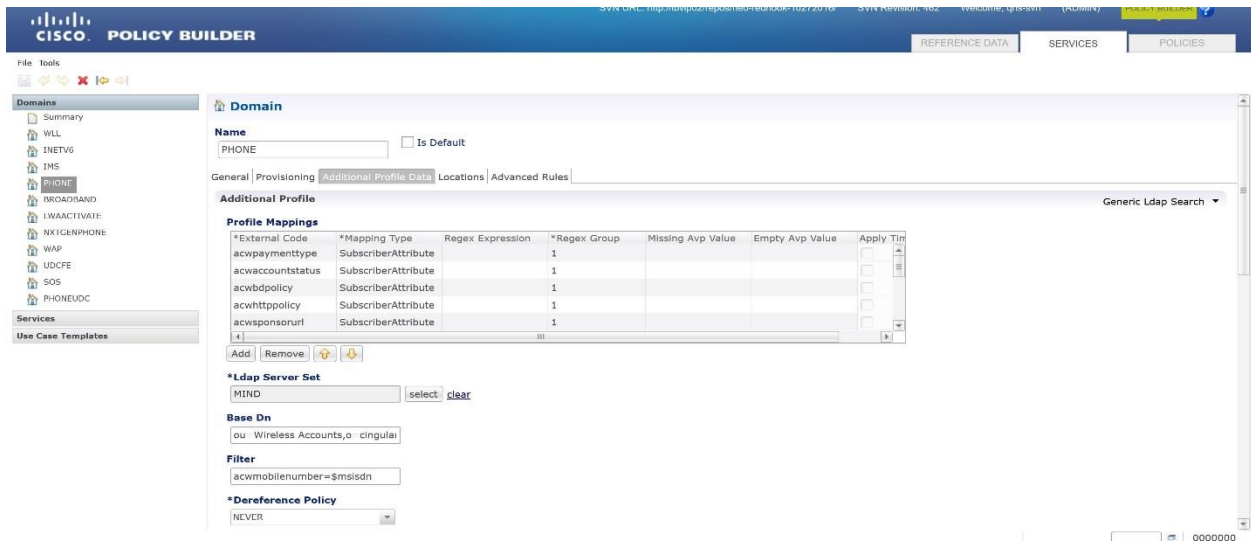
Configuring session migration includes the following tasks:

- Domain Configuration
- Policy Configuration

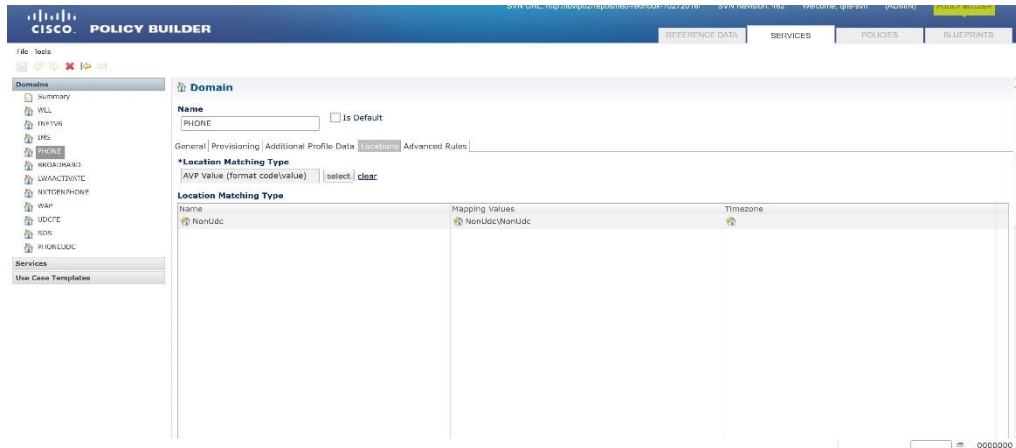
Domain Configuration

- Step 1** In Policy Builder, navigate to Services.
- Step 2** Select Domain.
- Step 3** Configure existing domains to work with the UDC deployment.

For example, the domain “PHONE” has **Generic Ldap Search** under the **Additional Profile Data** tab. Another corresponding domain called “PHONEUDC” with UDC Profile in it has to be created to be used by the UDC Client on the QNS VM.



- Step 4** Ensure that in the **Locations** tab of the “PHONE” domain, in the **Location Matching Type** table, the entry has the **Mapping Values** as “NonUdc\NonUdc.”



Step 5 Add a corresponding UDC-specific domain, for each existing domain that has **Generic Ldap Search** under **Additional Profile Data**.

Step 6 Create a new domain named **PHONEUDC**.

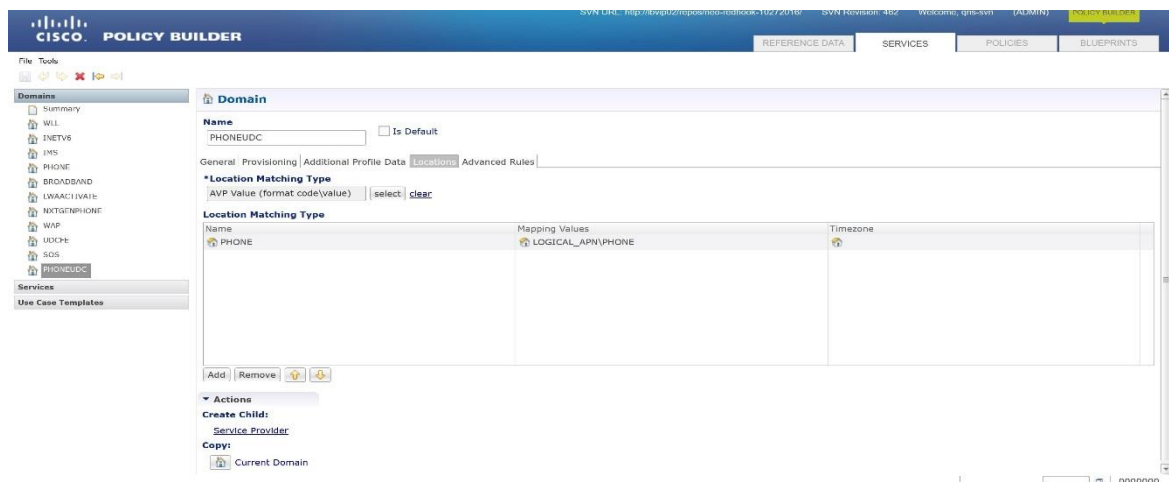
Step 7 In the “PHONEUDC” domain, under the **General** tab, in the **Authorization** section, select **Allow All Users**.

Step 8 In the “PHONEUDC” domain, under the **Additional Profile Data** tab, select **UDC Profile**.

For more information about configuring UDC Profile, refer to *CPS UDC Guide*.

Step 9 Under **Locations** tab in “PHONEUDC” domain, select “AVP Value (format code\value)” for **Location Matching Type**.

Step 10 Add a new entry in the **Location Matching Type** table with the **Name** as “PHONE” and the **Mapping Values** as “LOGICAL_APN\PHONE”

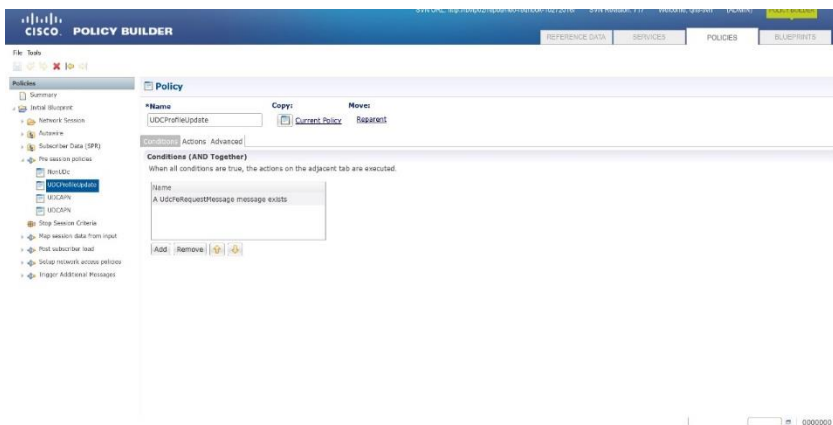


- Step 11** Under **Advanced Rules** tab, select **Default Service** as the service that is used by the **PHONE** domain.
- Step 12** Create a new domain named “UDCFE.”
- Step 13** Navigate to the **Authorization** section under **General tab** in the “UDCFE” domain.
- Step 14** Select **Allow All Users**.
- Step 15** Under the **Additional Profile Data** tab, select **Generic Ldap Search** and enter all possible attributes from all domains.
- Step 16** Under **Locations** tab in “UDCFE” domain, select “AVP Value (format code\value)” for **Location Matching Type**.
- Step 17** Add a new entry in the **Location Matching Type** table with the **Name** as “UDCFE” and the Mapping Values as “UDCFE\UDCFE”.
- Step 18** Under the Advanced Rules tab, select the Default Service as the service that is used by the “PHONE” domain.

Policy Configuration

- Step 1** Navigate to **Policy** tab.
- Step 2** Under **Policies** navigate to **Initial Blueprint**.
- Step 3** Add the section if there is no existing **Pre session policies** section.
- Step 4** Select **Configured Extension Point**.

The dialog box is displayed.
- Step 5** Expand **Initial Blueprint**.
- Step 6** Select **Pre session policies**.
- Step 7** Click **ok**.
- Step 8** Under **Pre session policies**, add another policy named “UDCProfileUpdate”.
- Step 9** Under **Conditions** tab, add a new condition **A UdcFeRequestMessage message exists**.



Step 10 Under **Actions** tab, add a new action **Add a policy derived AVP**.

Step 11 Under **Input Variables**, add **code** with the following details:

Type: Literal

Operator: =

Value: UDCFE

Step 12 Add **string** with the following details:

Type: Literal

Operator: =

Value: UDCFE

The screenshot shows the Cisco Policy Builder interface. The main window displays the configuration for a policy named "UDCProfileUpdate". The "Actions" tab is selected, showing a list of actions. The "Input Variables (AND Together)" table is visible below the actions, containing two rows:

Input Variables (AND Together)	Type	Operator	Value	
code (String)	Literal	=	UDCFE	Remove
value (String)	Literal	=	UDCFE	Remove

Step 13 Publish Policy Builder configuration.

Verify Session Migration

After migration, you need to monitor the increase in the number of sessions on UDC session cache to verify if all subscribers are migrated to the UDC cache.