



About CPS DRA

- [DRA Overview, on page 1](#)
- [DRA Architecture, on page 1](#)
- [DRA Users And Roles, on page 2](#)
- [Access CPS DRA, on page 3](#)
- [Manage Users, on page 4](#)
- [Supported Browsers, on page 5](#)

DRA Overview

Cisco Policy Suite DRA (Diameter Routing Agent) is a GUI platform that enables you to perform CPS vDRA related operations and launch the following applications and utilities:

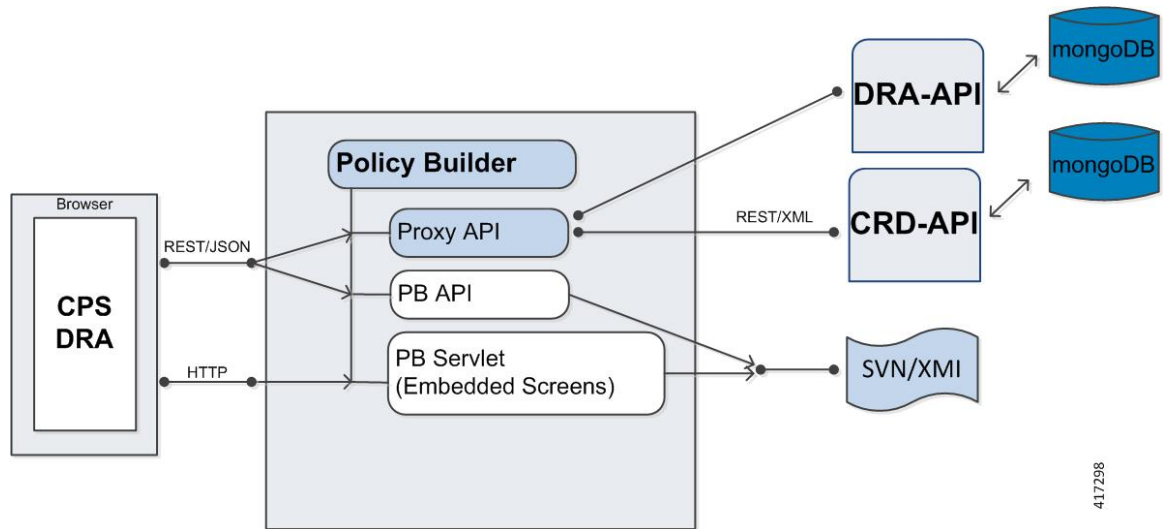
- Policy Builder - CPS Policy Builder with CPS vDRA specific options to customize and optimize CPS vDRA. For more information, see *Chapter 2 Configuring CPS DRA*.
- Custom Reference Data - Interface for service providers to create and populate data tables. For more information, see *Chapter 3 Managing Custom Reference Data*.
- Operations
 - DRA Monitoring - Interfaces to monitor the CPS vDRA related operations such as DRA Peer Monitoring, DRA Binding Monitoring, DRA SLF Bindings, and Grafana.
 - DRA API Information - Provides vPAS API and SLF API Documentation.

For more information, see *Managing DRA Operations* chapter in this guide.

DRA Architecture

DRA GUI is compliant with CPS Central functional structure.

Figure 1: DRA Architecture



The following section describes different layers of the DRA GUI:

- PB API layer - Manages PB API requests and interfaces with other CPS APIs. The PB API layer is one unified CPS API layer.
- PB servlet layer - Manages requests and responses between DRA GUI and the embedded PB screens.
- DRA GUI client layer - DRA GUI which reuses PB2 modularity and implements CPS vDRA specific GUI.

DRA System Flow

The following section describes the DRA system flow:

1. DRA GUI initiates active/inactive peers in the PB Proxy API.
2. PB Proxy API invokes DRA API end points to retrieve CPS vDRA data.
3. DRA API returns data back to the PB Proxy API.
4. PB Proxy API returns data back to the DRA GUI.
5. DRA GUI renders the data.

DRA Users And Roles

The following types of users/roles are supported in CPS DRA:

- Admin: User with create, read, update, and delete (CRUD) access to CPS DRA.
- Read Only: Restricted to read access only.

Access CPS DRA

You can access CPS DRA on the same port as Policy Builder with `/central/dra` and `/central/dra/` context.

You can enter `/central` or `/central/` in the browser, the application server redirects you to either CPS Central or CPS DRA depending on the install type you have selected during installation.

To access the CPS DRA Interface, use the supported URLs as described in the following table:

Table 1: Supported URLs

| Install Type | Entered URLs | Redirected URLs |
|--------------|--|--|
| DRA | <code>https:// <ip-address>/</code> | <code>https:// <ip-address>:7443/central/dra/</code> |
| | <code>https:// <ip-address>:7443/central</code> | <code>https:// <ip-address>:7443/central/dra/</code> |
| | <code>https:// <ip-address>:7443/central/</code> | <code>https:// <ip-address>:7443/central/dra/</code> |
| | <code>https:// <ip-address>:7443/central/dra</code> | <code>https:// <ip-address>:7443/central/dra/</code> |
| | <code>https:// <ip-address>:7443/central/dra/</code> | <code>https:// <ip-address>:7443/central/dra/</code> |
| | <code>https:// <ip-address>:443/central</code> | <code>https:// <ip-address>:7443/central/dra/</code> |
| | <code>https:// <ip-address>:443/central/</code> | <code>https:// <ip-address>:7443/central/dra/</code> |
| | <code>https:// <ip-address>:443/central/dra</code> | <code>https:// <ip-address>:7443/central/dra/</code> |
| | <code>https:// <ip-address>:443/central/dra/</code> | <code>https:// <ip-address>:7443/central/dra/</code> |
| Mobile | <code>https:// <ip-address>/</code> | <code>https:// <ip-address>:7443/central/</code> |
| | <code>https:// <ip-address>:7443/central</code> | <code>https:// <ip-address>:7443/central/</code> |
| | <code>https:// <ip-address>:7443/central/</code> | <code>https:// <ip-address>:7443/central/</code> |
| | <code>https:// <ip-address>:7443/central/dra</code> | HTTP ERROR 404 |
| | <code>https:// <ip-address>:7443/central/dra/</code> | HTTP ERROR 404 |
| | <code>https:// <ip-address>:443/central</code> | <code>https:// <ip-address>:443/central/</code> |
| | <code>https:// <ip-address>:443/central/</code> | <code>https:// <ip-address>:443/central/</code> |
| | <code>https:// <ip-address>:443/central/dra</code> | HTTP ERROR 404 (As the installed system is not DRA) |

The hostname is displayed in the login dialog box and system banner to differentiate between open windows while performing any operation of the CPS system. It indicates which system is being modified and prevents any errors or misconfigurations.

The hostname is displayed when the parameter `-Dhostname=lab` is configured in `pb/qns.conf` files. If it is not configured in the `qns.conf` file, it is displayed as a result of the command "hostname" on the server.

The hostname is displayed in the login panel only when the following argument is set to true:

```
-DshowSitenameLogin
```

Manage Users

Perform the following steps to add a new user:

1. Enter CONFIG mode as shown:

```
scheduler# config
Entering configuration mode terminal
scheduler(config)#
```

2. Use the **aaa authentication** command to create the user:

```
scheduler(config)# aaa authentication users user test2 gid 100 uid 9000 homedir / password
testpassword ssh_keydir /
scheduler(config-user-test2)# commit
scheduler(config-user-test2)# exit
```



Note The **gid**, **uid**, **homedir** and **ssh_keydir** are required but not used by the application.

Add User To A Viewer Operational Group

In CONFIG mode, add the user to the “oper” group and commit the change as shown:

```
scheduler(config)# nacm groups group oper user-name test2
scheduler(config-group-oper)# commit
```

Add User To An Editor Group

In CONFIG mode, add the user to the “editor” group and commit the change as shown:

```
scheduler(config)# nacm groups group editor user-name test2
scheduler(config-group-editor)# commit
```

Add User To An Admin Group

In config mode, add the user to the “admin” group and commit the change as shown:

```
scheduler(config)# nacm groups group admin user-name test2
scheduler(config-group-admin)# commit
```



Note To provide a user with Admin CRUD access to CPS DRA Central, add the user to the “policy-admin” group.

Change A User's Password

In the Management CLI, use the **aaa authentication users user change-password** command as shown:

```
scheduler# aaa authentication users user test2 change-password
Value for 'old-password' (<string>): *****
Value for 'new-password' (<string>): *****
Value for 'confirm-password' (<string>): *****
scheduler#
System message at 2017-03-08 21:17:18...
Commit performed by system via system using system.
```

Supported Browsers

CPS DRA supports the most recent versions of the following browsers:

- Apple Safari
- Google Chrome
- Microsoft IE
- Mozilla Firefox

