# Managing Custom Reference Data


- Feature Summary and Revision History, on page 1
- Feature Description, on page 1
- Configuration Support for Importing CRD, on page 2


# Feature Summary and Revision History

## Summary Data

***Table 1: Summary Data***

| | |
|---|---|
| Applicable Products or Functional Area | PCF |
| Applicable Platform(s) | SMI |
| Feature Default Setting | Enabled – Always-on |
| Related Documentation | Not Applicable |

## Revision History

***Table 2: Revision History***

| Revision Details | Release |
|---|---|
| First introduced. | 2020.05.0 |

# Feature Description

The Custom Reference Data (CRD) is the reference data specific to a service provider, such as their networks or cell sites' names and characteristics. This data is required to operate the policy engine but not used for evaluating the policies. The CRD is represented in the table format. The service providers have the flexibility to create custom data tables and manage them as per their requirements.

**Note** Make sure to start all the policy servers after a CRD table schema is modified (for example, column added/removed).

CRD supports the pagination component, which controls the data displayed according to the number of rows configured for each page. You can change the number of rows to be displayed per page. Once you set the value for rows per page, the same value is used across the Central unless you change it. Also, you can navigate to other pages using the arrows.

# Configuration Support for Importing CRD

This section describes the procedure to import CRD when the CRD schema is modified.

Importing of CRD involves the following steps:

- Backing Up the Existing SVN Repository
- Backing Up the Existing CRD
- Removing the Existing CRD from MongoDB
- Importing and Publishing the New CRD Schema
- Importing the New CRD Table

## Backing Up the Existing SVN Repository

This section describes how to import the SVN repository when the CRD schema is modified.

To take a backup of the existing SVN repository and store it on another environment, use the following configuration:

1. Log in to the PCF Central GUI.
2. On the **Cisco Policy Suite Central** page, navigate to **Policy Builder** and click the **Import/Export** link.

   The **Import/Export** form opens.
3. In the **Export** tab, select the **All data** option to configure the export type.

   The following table describes the export/import options:

***Table 3: Export and Import Options***

| Parameters | Description |
|---|---|
| All data | Exports service configuration with environment data, which acts as a complete backup of both service configurations and environmental data. |

| Parameters | Description |
|---|---|
| Exclude Environment | Exports without environment data, which allows exporting configuration from a lab and into another environment without destroying the new system's environment-specific data. |
| Only Environment | Exports only environment data, which provides a way to back up the system-specific environmental information. |
| Export URL | The URL can be accessed from the Policy Builder or viewed directly in Subversion. |
| Export File Prefix | Provide a name (prefix) for the export file.<br>**Note** The exported filename automatically includes the date and time when the export was performed. |

4. If you want to export the file in the compressed format, select the **Use 'zip' file extension** check box.
5. Click **Export**.
6. Navigate to the file and save it to your local machine. The file must include the cluster name and date.

# Backing Up the Existing CRD

This section describes how to import an existing CRD when the CRD schema is modified.

To take a backup of the configured CRD and store it to another environment, use the following configuration:

1. Log in to the PCF Central GUI.
2. On the **Cisco Policy Suite Central** page, navigate to **Custom Reference Data** and click the **Custom Reference Data** link.

   The **Import/Export CRD data** form opens.
3. Under **Export Custom Reference Data**, the following options are displayed:

   ***Table 4: Export Custom Reference Data Options***

| Options | Description |
|---|---|
| Use 'zip' file extension | Enables easier viewing of the exported contents for the advanced users. |
| Export CRD to Golden Repository | When the system is in a BAD state, the CRD cache is built using the golden-crd data. |

4. Click **Export**.

# Removing the Existing CRD from MongoDB

This section describes how to remove the existing CRD tables that have schema change from MongoDB.

To remove a configured CRD schema change, use the following configuration:

1. Log in to the admin-db pod that has the CRD (cust_ref_data) database.
2. Access the cust_ref_data using the following command:

   ```
   use cust_ref_data
   ```

3. Delete the data from one or more existing CRD tables using the following command:

   ```
   db.table_name.remove({})
   ```

4. Exit the admin-db pod.

# Importing and Publishing the New CRD Schema

This section describes how to import and publish the new CRD schema.

To import and publish the CRD schema, use the following configuration:

1. Log in to the PCF Central GUI.
2. On the **Cisco Policy Suite Central** page, navigate to **Policy Builder** and click the **Import/Export** link.

   The **Import/Export** form opens.
3. In the **Import** tab, browse to the file that you want to import.
4. In the **Import URL** field, enter the URL where the file must be imported. We recommend importing a new URL and verify it using the Policy Builder.
5. In the **Commit Message** field, enter the appropriate information.
6. To enforce import in situations where the checksums don't match, select the **Force import even if checksums don't match** check box.
7. Click **Import**.

### Importing the New CRD

To import the new CRD, use the following configuration:

1. Access the Policy Builder URL and add a new repository.
   a. In the **Choose Policy Builder data reposiorty...** window, select **<Add New Repository>** from the drop-down.

      The **Repository** dialog box appears.

      The following parameters can be configured under **Repository**:

      Configure the parameters according to the network requirements.

*Table 5: Repository Parameters*

| Parameter | Description |
|---|---|
| Name | This is a mandatory field. Ensure that you specify a unique value to identify your repository's site.<br>**Note** We recommend the following format for naming the repositories: customername_project_date, where underscores are used to separate customer name, project, and date. Date can be entered in the MMDDYYYY format. |
| Username and Password | Enter a username that is configured to view the Policy Builder data. The password can be saved for faster access, but it is less secure. A password, used with the Username, permits, or denies access to make changes to the repository. |
| Save Password | Select this check box to save the password on the local hard drive. This password is encrypted and saved as a cookie on the server. |
| Url | You can have several branches in the version control software to save different versions of configuration data. Create a branch in the version control software before assigning the URL in this screen.<br>Enter the URL of the branch of the version control software server that is used to check in this version of the data. |

| Parameter | Description |
|---|---|
| Local Directory | Do not modify the value in this field.<br>This is the location on the hard drive where the Policy Builder configuration objects are stored in the version control.<br>When you click either Publish or Save to Repository, the data is saved from this directory to the version control application specified in the Url text field.<br>The field supports the following characters:<br>• Uppercase: A to Z<br>• Lowercase: a to z<br>• Digits: 1–9<br>• Nonalphanumeric: /<br>**Note** The user must use only the supported characters. |
| Validate on Close | Select this check box to see if the values for Username, Password, or the URL are legitimate and unique. If not, the screen displays an error message and provides a chance to correct the errors. |
| Remove | Removes the display of the repository in Cisco Policy Builder.<br>**Note** The remove link here does not delete any data at that URL. The local directory is deleted. |

**b.** Click **OK** to save your work to the local directory.

**Note** When you change screens, the Policy Builder automatically saves your work. We recommend saving your work to the local directory by clicking on the diskette icon on the Policy Builder GUI or CTRL-S on the keyboard.

**c.** If you are ready to commit these changes to the version control software, choose **File > Save to Client Repository** on the Policy Builder home screen.

2. Log in to the new repository.
3. Verify the new CRD table schema and publish the changes.

4. Review the crd-api pod logs for any exception or error related to the duplicate key or duplicate index. If there are no errors, then the CRD is successfully imported.

# Importing the New CRD Table

This section describes how to import the CRD table.

To import new CRD tables, use the following configuration:

Before importing the CRD table, ensure that the CRD data archive is saved as dot (.) crd or dot (.) zip.

1. Log in to the PCF Central.
2. Click **Custom Reference Data**.
3. Click **Import/Export CRD Data**.
4. Under **Export Custom Reference Data**, the following options are displayed:
   - Select the **Use 'zip' file extension** check box to enable easier viewing of export contents for advanced users.
   - Select the **Export CRD to Golden Repository** check box to export CRD to golden repository which is used to restore cust_ref_data in case of error scenarios. A new input text box is displayed.
5. Add a valid SVN server hostname or IP address to push CRD to repository. You can add multiple hostnames or IP addresses by clicking on the plus sign.
6. Click **Export**.

### Verifying the Successful Export of CRD Table to Golden Repository

To verify of the export of the custom CRD table to the golden repository is successful, use the following configuration:

1. Log in to the PCF Central.
2. Click **Custom Reference Data**.
3. Click **Import/Export CRD Data**.
4. In **Import Custom Reference Data**, click **Field to Import field and browse for the CRD archive**.
5. Click the **Import** button to import the CRD data.
6. On successful import, verify that you receive a "Data imported" message on the PCF Central GUI.
7. Review crd-api pod logs for any exception or error related to duplicate key or duplicate index. If there are no errors, then the CRD is successfully imported.