

## **Configuring Data Collection**

# Contents



<b>Chapter 2. My overview for the processing scheme.....</b>	<b>3</b>
<b>Chapter 3. Configuring Data Collection: DataPower SOA Appliance.....</b>	<b>4</b>
<b>Chapter 4. The DataPower data collector as a proxy.....</b>	<b>5</b>
<b>Chapter 5. Planning for deployment.....</b>	<b>6</b>
Deploying the Data Power Data Collector.....	7
Unconfiguration steps.....	7
<b>Chapter 6. Configuring the DataPower SOA appliance for monitoring.....</b>	<b>8</b>
Configuring a user account on the DataPower SOA appliance.....	8
Configuring the XML Management Interface.....	8
<b>Chapter 7. Enabling data collection.....</b>	<b>10</b>
The DataPower configuration file.....	10
Enabling data collection using the Data Collector Configuration utility.....	11
Enabling data collection using the KD4configDC command.....	13
Specifying KD4configDC parameters.....	13
<b>Chapter 8. Disabling data collection.....</b>	<b>16</b>
Upgrading the data collector.....	16
Disabling the data collector using the Data Collector Configuration utility.....	16
<b>Chapter 9. Additional topics.....</b>	<b>17</b>
Starting and stopping the data collector.....	17
Optimizing performance.....	17
Creating node names in Tivoli Enterprise Portal.....	17
Required software.....	17
Integrating with ITCAM for transactions.....	17
Running the data collector configuration utility.....	17
Considerations for enabling data collection for DataPower monitoring.....	17
Running the DataPower data collector as a Windows service or UNIX daemon.....	17

# Chapter 1. My overview for the processing scheme

---

I have created a processing scheme based on the brand of the document.

I decided to use the brand of the document as the processing scheme because I feel that this is a relevant and real-world example of how processing is used in documentation. Often similar products created by the same company will change the name of the product in a document, and replace with another product. I wanted to recreate this for my assignment so that I get a real understanding of how processing works in a document. Anywhere that the product name 'SOA' appeared, I replaced with the keydef of 'Brand'. I created a fake product name, 'SIH', which will appear whenever I change the product in the Attributes list.

In terms of flagging, I have also applied a 'New' and 'Deleted' status to the Attributes list. This is to indicate whenever a new piece of text has been added to the document version, and when a piece of text has been deleted from the document version. I also feel that this is a good opportunity to use real-world examples of how conditionalising works in DITA. I include in my assignment file, a PDF version of both the SOA and SIH processing schemes and parts of texts that are flagged as both New and Deleted.

## Chapter 2. Configuring Data Collection: DataPower SOA Appliance

This section describes the support for monitoring of service flows through an IBM® WebSphere® DataPower® SOA appliance, where the ITCAM for SOA data collector acts as a proxy between the services clients and servers.

The list of versions of the DataPower SOA appliance supported by ITCAM for SOA 7.2 Fix Pack 1 is available from the Software product compatibility reports website. For information about accessing reports from this website, see Required software.

The DataPower data collector can be integrated with ITCAM for Transactions. If configured, transaction events are sent to a Transaction Collector which stores and aggregates transaction data from multiple data collectors. For more information about configuring the interface to ITCAM for Transactions, see Integrating with ITCAM for Transactions.

IBM WebSphere DataPower SOA appliances are used for processing XML messages, and providing message transformation, services acceleration, and security functions. A DataPower appliance is typically used to improve the security and performance of services by offloading functions from the application server that is hosting the target service to a DataPower SOA appliance. Typical functions that are off-loaded include; authentication and authorization, XML schema validation, and services encryption and decryption.

ITCAM for SOA provides a DataPower data collector that operates as a proxy and monitors services flows through a DataPower SOA appliance, providing similar services management and availability information that ITCAM for SOA currently provides for application server runtime environments. This information is displayed in the Tivoli® Enterprise Portal using the usual predefined or user-defined workspaces and views. DataPower supports two proxy types that can process SOA messages:

**The Web Services Proxy** You configure a Web Services Proxy by importing one or more WSDL files and then telling the appliance where to direct those messages. Thus, the Web Services Proxy receives only SOAP messages. The Multi-Protocol Gateway The Multi-Protocol Gateway is more versatile than the Web Services Proxy. You can use it to process nearly any type of message, including SOAP, non-SOAP XML, text, or binary. For XML messages (including SOAP), XSL transforms are used to manipulate the message. For non-XML messages, similar transform actions can be built using IBM WebSphere Transformation Extender (for more information about this product, see <http://www-306.ibm.com/software/integration/wdatastagetx/>).



### HAZARD

#### Firmware

**Before using the DataPower data collector proxy, you must upgrade the firmware on DataPower SOA appliances that you want to monitor, to include the necessary monitoring and data transformation capabilities.**

**Upgrade your firmware to at least version 3.7.1 or later to monitor traffic through the Web Services Proxy.**

**Upgrade your firmware to at least version 3.7.1 Fix Pack 4 or later to monitor traffic through a Multi-Protocol Gateway.**

**Consult your DataPower Appliance documentation for information about upgrading your firmware level.**

## Chapter 3. The DataPower data collector as a proxy

---

Data collector provided with ITCAM for SOA are usually installed directly into the application server runtime environment hosting the services being monitored. The DataPower SOA appliance, however, does not support the installation of additional software, such as a data collector.

Unlike other application server runtime environments, the ITCAM for SOA data collector for the DataPower environment is installed on a separate computer system and uses a special communication mechanism that allows external software applications to receive data from its internal transaction log.

This communication mechanism is used to retrieve monitoring data about services requests flowing through one or more DataPower SOA appliances, and to convert the data into a format that ITCAM for SOA can process. In this way, the DataPower data collector acts as a proxy between the DataPower SOA appliances and the ITCAM for SOA monitoring agent.

The DataPower data collector can be installed on a dedicated computer system, or it can run on a computer that is also hosting data collectors for other application server runtime environments.



**Important:** IBM supports only one instance of the DataPower data collector running on any computer system. This one data collector instance, however, can monitor any number of domains on any number of appliances, subject to available resources.

When data collection is enabled for the DataPower environment, the data collector subscribes to each monitored DataPower SOA appliance and then polls the appliance for monitoring data at the specified interval. The data that is retrieved from the DataPower SOA appliance is written to metric log files in the format used by ITCAM for SOA. When this data is later displayed in the Tivoli Enterprise Portal, nodes are displayed in the Tivoli Enterprise Portal Navigator view that represent the DataPower SOA appliances that are being monitored. You can select workspaces under these nodes and view the services management data for the service requests flowing through the monitored DataPower SOA appliances.

The DataPower data collector can subscribe to multiple DataPower SOA appliances, and retrieve and manage data from multiple domains. This data can then be separated by DataPower domain or aggregated across multiple domains and appliances, depending on how you configure the data collector. The DataPower data collector uses a configuration file that contains information about which DataPower SOA appliances are being monitored and information needed to establish communication with each monitored appliance.

## Chapter 4. Planning for deployment

---

DataPower proxies are defined within *application domains*, and DataPower users can be restricted to access some or all domains.

When configuring the DataPower data collector, you must understand how the domains and users are defined on the monitored DataPower SOA appliances, to ensure that the data collector uses valid authentication credentials. This refers to user IDs and passwords that have access to the DataPower domains containing the services proxies to be monitored. In addition, you must decide how you want to aggregate or separate the data collected from those domains for display in the Tivoli Enterprise Portal.

You can use DataPower SOA appliances in several typical configurations:

### **Single appliance, single domain**

The data collector monitors a single DataPower SOA appliance, with all of the monitored resources that are defined in a single domain on the appliance.

### **Single appliance, multiple domains**

The data collector monitors a single DataPower SOA appliance, but that appliance has monitored resources that are defined in more than one domain on the appliance.

### **Multiple appliances with different configurations**

The data collector monitors multiple DataPower SOA appliances, and each appliance has a different configuration of resources to be monitored. Each appliance is configured for a particular job, with no intention of load-balancing or fail-over between appliances.

### **Multiple appliances with identical configurations**

The data collector monitors multiple DataPower SOA appliances, and all of the appliances have an identical configuration of resources being monitored. All of the appliances are configured for the same job, taking advantage of load-balancing, and fail-over capabilities between appliances.

Given these typical configurations, the DataPower data collector provides a great deal of flexibility in defining how the collected monitoring data should be separated or aggregated, across a single appliance or multiple appliances, for display in the Tivoli Enterprise Portal. The following examples illustrate how data can be separated or aggregated for managing the data from various domains and appliances:

### **Separation of data at the domain**

You can view the services management data for the resources in a single domain, separate from the data for resources in other domains.

### **Aggregation of data across domains**

You can view the services management data for the resources in several domains (for example, all of the domains on a DataPower SOA appliance) in an aggregated form, with no regard for the domain in which individual resources are defined.

### **Separation of data at the appliance**

You can view the services management data for resources on a single DataPower SOA appliance, separate from the data for resources on other appliances.

### **Aggregation of data across appliances**

You can view the services management data for the resources on several DataPower SOA appliances (for example, all of the appliances in a Configuring data collection: DataPower SOA Appliance 3 load-balancing *cluster*) in an aggregated form, with no regard for what activity occurs on each individual appliance.

By default, the DataPower data collector aggregates data for all of the monitored domains on a single DataPower SOA appliance (even if the domains are accessed using different credentials), and keeps the data from each DataPower SOA appliance separated. See [Enabling data collection \(page 10\)](#) for more information. However, operational flow data is collected only by individual domains. Refer to [Creating node names in Tivoli Enterprise Portal \(page 17\)](#) for additional details.

A single instance of the DataPower data collector can monitor any number of DataPower SOA appliances, limited only by the memory, CPU power, and other resources available to it.



**Important:** IBM supports running only a single instance of the data collector on any computer system.

## Deploying the DataPower Data Collector

---

How to deploy the DataPower data collector in your environment.

Before using the DataPower data collector proxy, you must upgrade the firmware on DataPower SOA appliances that you want to monitor, to include the necessary monitoring and data transformation capabilities.

1. Configure your DataPower SOA appliances for monitoring (see [Configuring the DataPower SOA appliance for monitoring \(page 8\)](#) for details).
2. Enable the DataPower data collector (see [Enabling data collection \(page 10\)](#) for details).
3. Run the `startDC` script to start the data collector (see [Starting and stopping the data collector \(page 17\)](#) for details), or configure the data collector to run in the background and start the background task.

## Unconfiguration steps

---

To unconfigure the DataPower Data Collector in your environment, complete the following general steps:

1. Run the `stopDC` script to stop the Data Collector (see [Starting and stopping the data collector \(page 17\)](#) for details) when the DataPower proxy is started as a background task, or run the **stop**, **quit**, or **exit** command from the console to initiate an orderly shutdown of the DataPower Data Collector.
2. Disable the DataPower Data Collector (see [Disabling data collection \(page 16\)](#) for details).

## Chapter 5. Configuring the DataPower SOA appliance for monitoring

---

Before a DataPower SOA appliance can be monitored by the DataPower data collector, configure the DataPower SOA appliance by completing these tasks, described in more detail in the sections that follow:

- Upgrade your DataPower firmware to the minimum supported version.
- Configure a user account on the DataPower SOA appliance for use with the DataPower data collector.
- Enable the XML Management Interface on the appliance.
- Check additional optional settings for each domain to be monitored.
- Enable the ITCAM for SOA transforms for the Web Services Proxy gateways and the Multi-Protocol gateways as needed.
- Configure the AAA policy for the Web Services Proxy gateways and the Multi-Protocol gateways if you plan to monitor Web service requesters by user ID.

### Configuring a user account on the DataPower SOA appliance

---

The DataPower user ID used by the data collector must belong to a user group with the following permissions:

- *Read* permission on the Login XML-Mgmt Resource Type in the default domain.
- *Read* permission on the XML-Mgmt Resource Type in each domain to be monitored using this user ID.
- *Read* permission on the (any) Resource Type in each domain to be monitored using this user ID.

See your *DataPower WebGUI Guide* or *DataPower CLI Reference Guide* for details on configuring user group permissions.

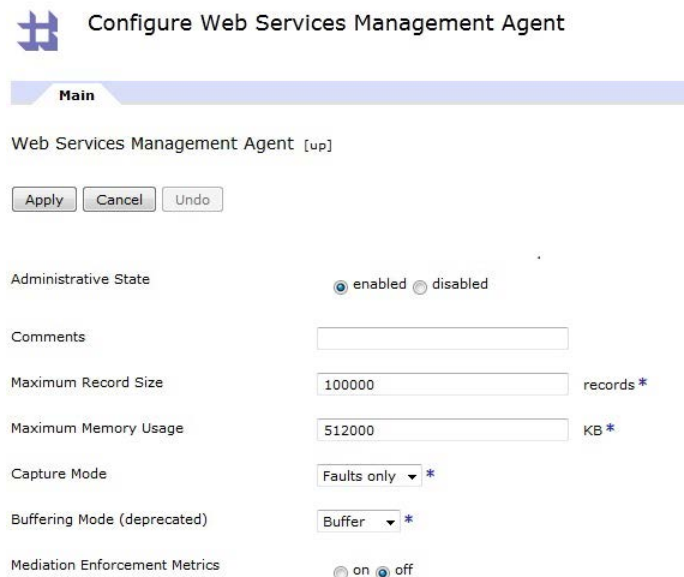
### Configuring the XML Management Interface

---

The XML Management Interface on the appliance must be enabled using the DataPower administration console.

To configure the XML Management interface, complete the following steps:

1. Start the DataPower administration console in a web browser (<https://hostname:9090/login.xml>).
2. Complete the following steps to enable the XML Management interface.
  - a. Log in to the administration console as the admin user for the default domain.



The screenshot shows the 'Configure Web Services Management Agent' page in the DataPower administration console. The page has a blue header with the title and a 'Main' tab. Below the header, there are three buttons: 'Apply', 'Cancel', and 'Undo'. The main content area contains several configuration options for the 'Web Services Management Agent'.

Configuration Option	Value	Unit/Note
Administrative State	<input checked="" type="radio"/> enabled <input type="radio"/> disabled	
Comments	<input type="text"/>	
Maximum Record Size	<input type="text" value="100000"/>	records *
Maximum Memory Usage	<input type="text" value="512000"/>	KB *
Capture Mode	<input type="text" value="Faults only"/>	*
Buffering Mode (deprecated)	<input type="text" value="Buffer"/>	*
Mediation Enforcement Metrics	<input type="radio"/> on <input checked="" type="radio"/> off	



- b. Navigate to **Objects > Management > XML Management Interface**.
  - c. Make note of the port number that is displayed. You must specify this port number later when you enable or disable data collection.
  - d. In the **Main** tab, find the **WS-Management Endpoint** option and select the **on** check box.
  - e. Click **Apply** to activate the changes and enable the WS-Management Endpoint.
3. Complete the following steps to configure the Web Services Agent for the default domain:
- a. Navigate to **Services > Miscellaneous > Web Services Agent**. For example:
  - b. Set **Administrative State** to enabled.
  - c. Set the set **Buffering Mode** option to `discard` or `buffer`. The default setting is `discard`.

When **Buffering Mode** is set to `buffer`, the Web Services Agent buffers transaction information for the current domain when no registered ITCAM for SOA data collectors are running. Buffering reduces the loss of transaction information, but consumes more memory. Transaction records are buffered until the configured size limits are reached. Buffering is a better choice when initially configuring data collection, when processing high volumes of data, or when there are multiple ITCAM for SOA subscribers.

When **Buffering Mode** is set to `discard`, transaction information from the current domain is discarded when no registered ITCAM for SOA data collectors are running. Complications can occur if a new ITCAM for SOA subscriber replaces a former subscriber. High volumes of transactions might cause the Complete Records Count to reach the configured Maximum Record Size limit and transaction information to be discarded. Setting **Buffering Mode** to `discard` is suited to an environment where there is a single ITCAM for SOA subscriber, where the DataPower appliance is handling a low volume of transaction data, and where the ITCAM for SOA subscriber is collecting a low volume of metrics. For information about troubleshooting scenarios where transaction metrics are being discarded, see the *IBM Tivoli Composite Application Manager Troubleshooting Guide*.

- 4. Adjust the values for Maximum Record Size and Maximum Memory Usage, if necessary.
- 5. If you want the data collector to record message content in addition to summary metrics, change **Capture Mode** from `faults` to `all-messages`.
- 6. Configure the Web Services Agent for *all other domains* that are monitored by the DataPower data collector. For each domain, switch to the domain and complete step 3a on page 6 to step 3e.

## Chapter 6. Enabling data collection

---

This section describes how to configure the DataPower environment for data collection.

### The DataPower configuration file

---

For the DataPower data collector, the Data Collector Configuration utility and the **KD4configDC** command manipulate the contents of a special DataPower configuration file by adding sections to the file when new DataPower monitoring is enabled, and removing sections from the file when monitoring is disabled.

ring is enabled, and removing sections from the file when monitoring is disabled. Each invocation of the Data Collector Configuration utility or the **KD4configDC** command adds, updates, or removes one section of the DataPower configuration file. Each section of the DataPower configuration file might be associated with its own data group, or it might be part of a larger data group to which other sections of the configuration file also belong.

The DataPower data collector uses this configuration file to identify the DataPower SOA appliances that are to be monitored and to specify all of the information that is needed to communicate with those appliances. Typical information that is stored for each connection includes host name and port, user ID and password, domains to monitor, and polling interval.

The configuration file is in the `ITCAM4SOA_Home/KD4/config` directory on Linux or UNIX systems and the `ITCAM4SOA_Home/KD4/config` directory on Windows systems and is called `KD4.dpdcConfig.properties`. This file is maintained separately from the existing `KD4.dc.properties` configuration file. This is a sample DataPower configuration file:

```
# Sample DataPower data collector configuration file DataPower.count=3
```

```
#
```

```
DataPower.host.1=dpbox1
```

```
DataPower.port.1=5550
```

```
DataPower.path.1=
```

```
DataPower.poll.1=60
```

```
DataPower.user.1=admin
```

```
DataPower.encpswd.1=#$%*&
```

```
DataPower.domainlist.1=default,testdom1
```

```
DataPower.displaygroup.1=dpbox1
```

```
DataPower.subExpire.1=15
```

```
DataPower.maxrecords.1=1000 #
```

```
DataPower.host.2=dpbox2
```

```
DataPower.port.2=5550
```

```
DataPower.path.2=
```

```
DataPower.poll.2=30
```

```
DataPower.user.2=user1
```

```
DataPower.encpswd.2=&*%$#
```

```
DataPower.domainlist.2=userdom1,userdom2,userdom3
```

```
DataPower.displaygroup.2=user_doms
```

```
DataPower.subExpire.2=15
```

```
DataPower.maxrecords.2=1000
```

```
#
```

```
DataPower.host.3=dpbox2
```

```
DataPower.port.3=5550
DataPower.path.3=/
DataPower.poll.3=30
DataPower.user.3=admin
DataPower.encpswd.3=%$#&
DataPower.displaygroup.3=all_doms
DataPower.subExpire.3=15
DataPower.maxrecords.3=1000
```

In the example, there are three sections in the configuration file. The properties in each of the three sections provide all of the information that is needed to establish and manage a single connection or session with each DataPower SOA appliance.

Change the information in this configuration file using either the Data Collector Configuration utility or the KD4configDC command. You can only modify the parameters that are set when you first run the Data Collector Configuration utility or when you first issued the KD4configDC command. To set additional parameters, you must manually add them to the configuration file.

Using various combinations of parameters in the Data Collector Configuration utility input pages or in the KD4configDC command, you can achieve different monitoring configurations to separate or aggregate data among domains and appliances. See “Considerations for enabling data collection for DataPower monitoring” on page 28 for more information.

Before you configure your DataPower environment for data collection, consult with your local systems management planners to understand which domains on which DataPower SOA appliances are to be monitored and how the data from these domains and appliances should be separated or aggregated for display in the Tivoli Enterprise Portal.

To set the DataPower.maxrecords property to an optimal value, it is useful to determine the number of transactions that are processed by each of the configured domains. The DataPower.maxrecords property must be set in line with the expected traffic levels of each configured domain. For more information about setting the transaction rate, see *Optimizing performance* (page 40).



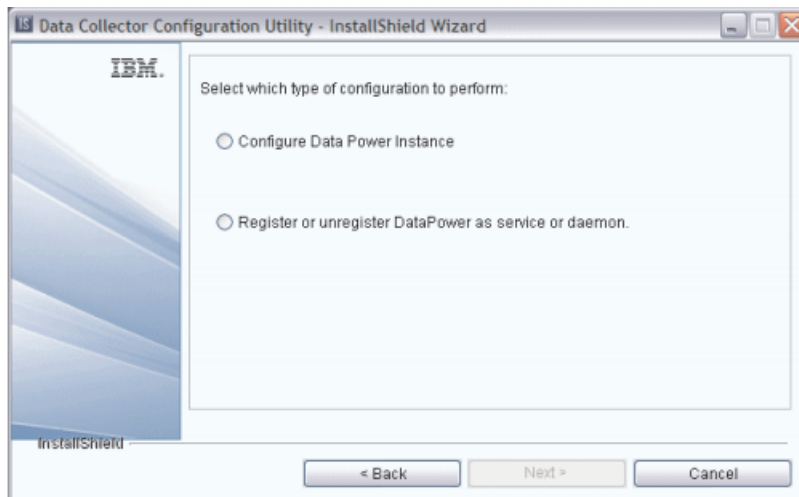
**Restriction:** In an upgrade scenario, to set the maximum number of records for an existing display group, you must add the DataPower.maxrecords parameter manually to the section in the KD4.dpdconfig.properties file that configures the display group.

## Enabling data collection using the Data Collector Configuration utility

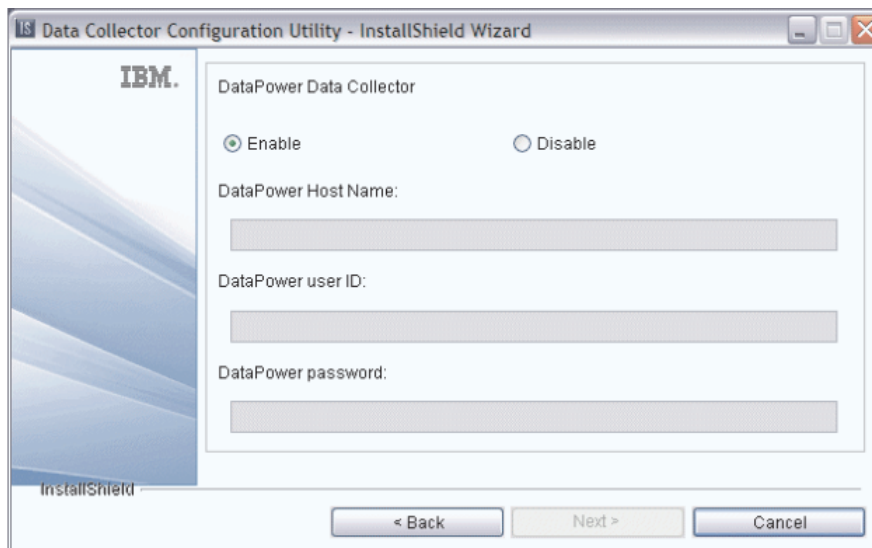
---


To enable data collection using the Data Collector Configuration utility, complete the following steps:

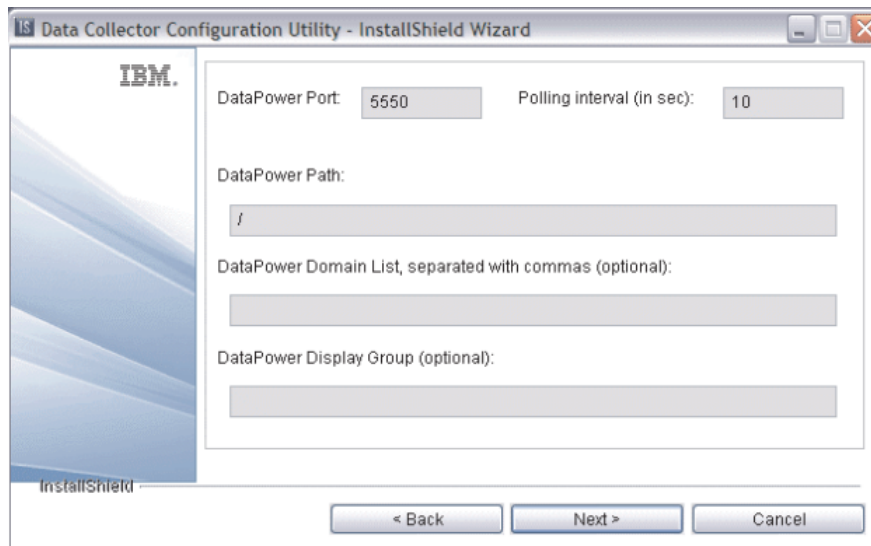
1. Run the Data Collector Configuration utility (see [Running the Data Collector Configuration utility \(page 17\)](#)):
  - a. Select the DataPower SOA Appliance runtime environment.
  - b. Select the **Configure > DataPower Instance** option.



- c. Select the option to enable data collection.
- d. Specify the DataPower Host Name.
- e. Specify the DataPower user ID.
- f. Specify the DataPower password.



- g. The default DataPower port number (5500) and the default polling interval (10 seconds) are provided. Accept these defaults or specify different values.
- h. Verify that the DataPower Path is set to /.
  -  **Restriction:** You cannot specify a path other than /. Changing its value has no effect.
- i. Specify the DataPower Domain List.
- j. Optionally specify the DataPower Display Group.



- k. Wait for the configuration utility to complete the operation.
- l. Exit the utility.

**Important:** When you deploy the DataPower data collector, you must start the data collector once you have enabled it to begin collecting data. For more information about starting the data collector, see [Starting and stopping the data collector \(page 17\)](#).

© For the remaining input parameters, refer to Table 2 on page 24 for a description of the information that is required, and see the additional information and examples of running the KD4configDC command to learn more about how to specify these parameters for your environment.

## Enabling data collection using the KD4configDC command

The syntax for running the KD4configDC command for the DataPower environment is similar to the syntax for other supported ITCAM for SOA data collector environments.

To run the **KD4configDC** command, first navigate to the following location, depending on your operating system:


Enter the KD4configDC command:

- For supported Windows operating systems: KD4configDC {-enable | -disable} -env 8
- For supported AIX, Solaris, HP-UX, and Linux operating systems: KD4configDC .sh {-enable | -disable} -env 8

## Specifying KD4configDC parameters

The env specific parameters defined for the DataPower invocation of the KD4configDC command are a series of key and value pairs that define the necessary properties for the affected section of the DataPower configuration file. These key and value pairs, which you can specify in any order on the command line, are shown in Table 2 on page 24.

**Table 1: DataPower key and value pairs for the KD4configDC command**

Parameter	Optional / Required	Default value	Description
-host <i>host name or IP address</i>	Required		Defines the DataPower SOA appliance host name or IP address. This host name is used to establish a socket connection and is used as part of the Web address pointing to the DataPower SOA appliance. This value can be any length string, with no blank characters. See <a href="#">Creating node names in Tivoli Enterprise Portal (page 17)</a> regarding possible truncation of this value in the node name.
-user <i>user ID</i>	Required		Defines the DataPower SOA appliance authentication user. This user must be a valid user for the DataPower SOA appliance defined by the -host parameter. See your DataPower documentation for information about creating and managing user IDs for DataPower SOA appliances. See <a href="#">Configuring a user account on the DataPower SOA appliance (page 8)</a> for more information.
-pswd <i>password</i>	Optional	User is prompted, if necessary	Defines the DataPower SOA appliance authentication password, entered in clear text (not encoded). This password must be valid for the user defined in the -user parameter, and must be valid for the DataPower SOA appliance defined by the -host parameter. This password is automatically converted to an encoded (masked) form and is stored in the DataPower configuration file. See your DataPower documentation for information about creating and managing passwords for DataPower SOA appliances.
-port <i>port number</i>	Optional	5550	Defines the DataPower SOA appliance port number. This port number is used to establish a socket connection and is used as part of the Web address pointing to the DataPower SOA appliance. This value must be an integer from 0 to 65535. If this parameter is not specified, the default value is used.
-path <i>path string</i>	Required	/	Defines the DataPower SOA appliance path. This path is used as part of the Web address pointing to the DataPower SOA appliance.   <b>Restriction:</b> You cannot specify a path other than /. Changing its value has no effect.
-poll <i>polling interval</i>	Optional	10 seconds	Defines the DataPower SOA appliance polling interval (in seconds). The data collector waits this amount of time between each poll of the DataPower SOA appliance. This must be an integer value, specified in seconds, between 1 and 300 (1 second to 5 minutes).
-maxrecords <i>maximum number of records</i>	Optional	15000	Defines the maximum number of records that the DataPower data collector can process from the DataPower SOA appliance per polling interval. This must be an integer value, between 1 and 30000.

Parameter	Optional / Required	Default value	Description
-subexpire <i>length of time the subscription is valid</i>	Optional	15	Defines the length of time, in minutes, that the subscription of the DataPower data collector to the DataPower appliance remains valid. At the end of the subscription period, the DataPower data collector renews its subscription to the DataPower appliance. This must be an integer value, specified in minutes, between 3 and 30.
-domainlist <i>domainA, domainB, ...domainZ</i>	Optional	No domainlist property is generated	Defines the DataPower SOA appliance domain list. This is a comma-separated list of domains to be monitored on the associated DataPower SOA appliance. Any domains in this list that are not authorized to the user defined by the <code>-user</code> parameter are not monitored. Each domain can be any string, with no blank characters. If you specify more than one domain name, separated by commas, the entire domain list must be enclosed in double quotation marks (for example, <code>-domainlist "domain1, domain2, domain3"</code> ). See <a href="#">Considerations for enabling data collection for DataPower monitoring (page 17)</a> for more information about using this domain list.
-displaygroup <i>display group</i>	Optional	No displaygroup property is generated	Defines the DataPower SOA appliance display name. The name can be any string, with no blank characters, up to 64 characters long. See <a href="#">Creating node names in Tivoli Enterprise Portal (page 17)</a> regarding possible truncation of this value in the node name. See <a href="#">Considerations for enabling data collection for DataPower monitoring (page 17)</a> for more information about the use of this property.



**Important:** When you deploy the DataPower data collector, you must start the data collector once you have enabled it to begin collecting data. For more information about starting the data collector, see [Starting and stopping the data collector \(page 17\)](#).

## Chapter 7. Disabling data collection

---

This section describes the procedures for disabling data collection in the DataPower environment.

To unconfigure the Data Power® data collector, you must stop the data collector before disabling it. For more information about stopping the data collector, see [Starting and stopping the data collector \(page 17\)](#).



**Important:** You do not have to stop the data collector first if you are making configuration changes.

### Upgrading the data collector

---

If you are upgrading the data collector for the DataPower environment, *do not* use the `-disable` option of the `KD$configDC` script or the Data Collector Configuration utility described in this section.

Instead, you should complete the following steps:

1. Stop the DataPower data collector using the `stopDC` command (see [Starting and stopping the data collector \(page 17\)](#) for more information).
2. Deregister the service or daemon, if applicable. See [Running the DataPower data collector as a Windows service or UNIX daemon \(page 17\)](#) for the procedures to stop a registered DataPower data collector and to deregister the service to remove it from the list of Windows services, if applicable.

See [Upgrading to ITCAM for SOA version 7.2](#) for more information about upgrading your monitoring environment from a previous version.

### Disabling the data collector using the Data Collector Configuration utility

---

To disable data collection with the Data Collector Configuration utility, complete the following steps:

1. Run the Data Collector Configuration utility (see [Running the Data Collector Configuration utility \(page 17\)](#)):
  - a. Select the DataPower SOA Appliance runtime environment.
  - b. Select the Configure DataPower Instance option.
  - c. Select the option to disable data collection.  
For the remaining input parameters, refer to Table 2 on page 24 for a description of the information that is required, and see the additional information and examples of running the `KD4configDC` command to learn more about how to specify these parameters for your environment.
  - d. Specify the DataPower Host Name.
  - e. Specify the DataPower user ID.
  - f. Specify the DataPower password.
  - g. The default DataPower port number (5500) and the default polling interval (10 seconds) is provided. Accept these defaults or type over them to specify different values.
  - h. Specify the DataPower Domain List.
  - i. Optionally specify the DataPower Display Group.
  - j. Wait for the configuration utility to complete the operation.
  - k. . Exit the utility.



## **Chapter 8. Additional topics**

---

The following topics within this chapter contain empty pages that are referenced in the document, that we were not asked to transfer into DITA for the assignment.

As requested, I have created empty topics for the references to ensure the links work in the document.

### **Starting and stopping the data collector**

---

### **Optimizing performance**

---

### **Creating node names in Tivoli Enterprise Portal**

---

### **Required software**

---

### **Integrating with ITCAM for transactions**

---

### **Running the data collector configuration utility**

---

### **Considerations for enabling data collection for DataPower monitoring**

---

### **Running the DataPower data collector as a Windows service or UNIX daemon**

---