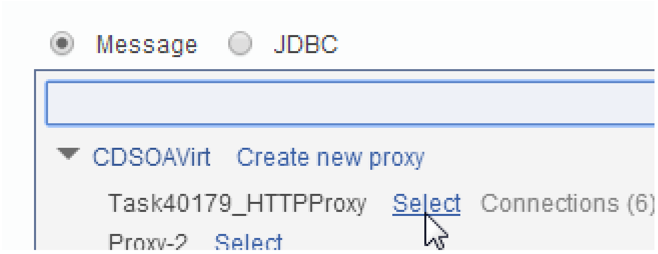
Configuring Message Proxies

When configuring a component instance with a message proxy, you can either select an existing message proxy or create a new one. Once a proxy is enabled, you can start or stop recording via CTP.

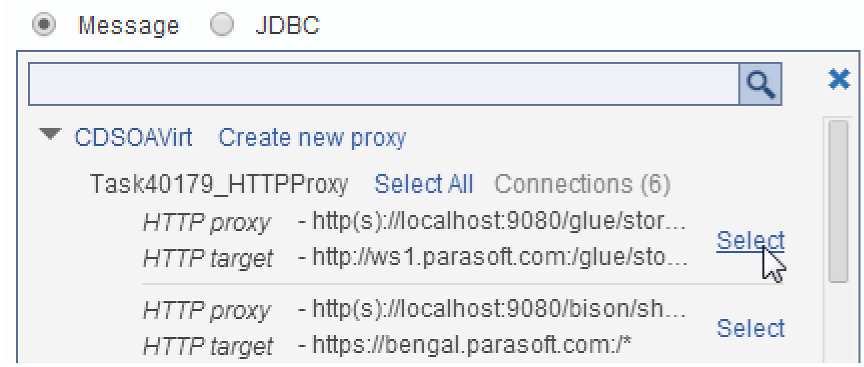
Selecting an Existing Proxy

To configure a component instance with an existing message proxy:

1. In the Components wizard area—or the Proxy area of the Instance editor, set **Proxy Type** to **Message**, then click **Select a message proxy**.
2. Specify which proxy connections to add:
   - If you want to select all connections for an available proxy, click the **Select** link.



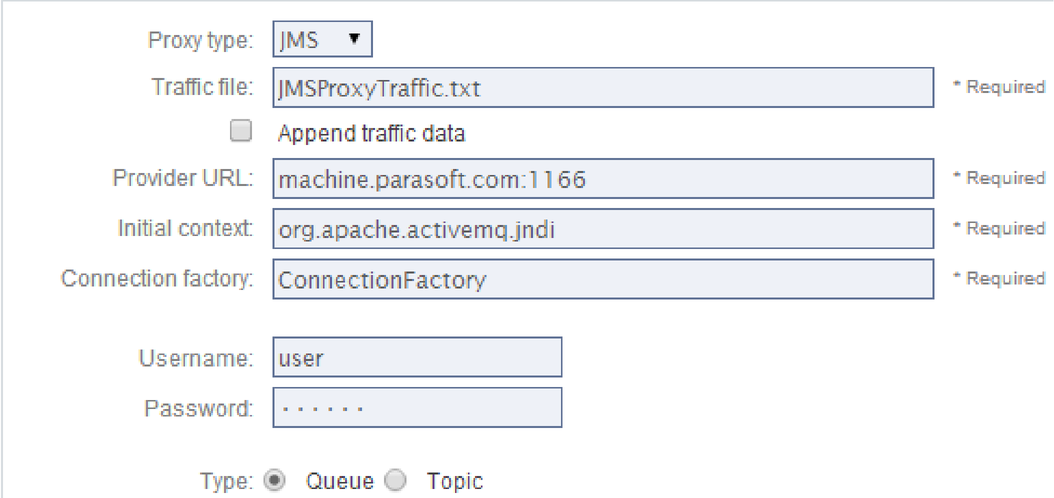
   - If you want to select a specific connection for an available proxy (e.g., you have 3 HTTP connections, 1 MQ connection, and 1 JMS connection configured—but you are using only the MQ connection right now), hover over the proxy, click the **Connections** link that appears, then click the **Select** link for the connection you want to add. You could also click **Select All** to select all shown connections. Each available connection's listener/proxy path and forward/target path will be shown.



HTTP proxy - http(s)://localhost:9080/glue/stor...
HTTP target - http://ws1.parasoft.com:/glue/sto...

HTTP proxy - http(s)://localhost:9080/bison/sh...
HTTP target - https://bengal.parasoft.com:/*

3. If you want to adjust proxy settings (taken from the proxy's current state), click the **Edit** icon, then make the desired modifications; options are described in Proxy Configuration Details.



Proxy type: JMS ▼

Traffic file: JMSProxyTraffic.txt * Required

□ Append traffic data

Provider URL: machine.parasoft.com:1166 * Required

Initial context: org.apache.activemq.jndi * Required

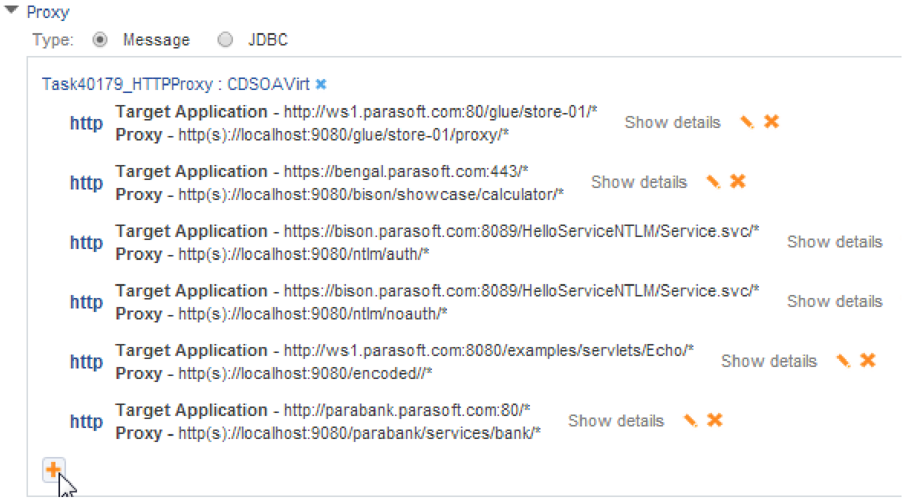
Connection factory: ConnectionFactory * Required

Username: user

Password: ······

Type: ● Queue ○ Topic

4. If you want to add a message proxy connection, click the + icon, then specify the connection settings as described in Proxy Configuration Details.



▼ Proxy

Type: ● Message ○ JDBC

Task40179_HTTPProxy : CDSOAVirt ✖

http **Target Application** - http://ws1.parasoft.com:80/glue/store-01/* **Proxy** - http(s)://localhost:9080/glue/store-01/proxy/* Show details

http **Target Application** - https://bengal.parasoft.com:443/* **Proxy** - http(s)://localhost:9080/bison/showcase/calculator/* Show details

http **Target Application** - https://bison.parasoft.com:8089/HelloServiceNTLM/Service.svc/* **Proxy** - http(s)://localhost:9080/ntlm/auth/* Show details

http **Target Application** - https://bison.parasoft.com:8089/HelloServiceNTLM/Service.svc/* **Proxy** - http(s)://localhost:9080/ntlm/noauth/* Show details

http **Target Application** - http://ws1.parasoft.com:8080/examples/servlets/Echo/* **Proxy** - http(s)://localhost:9080/encoded//* Show details

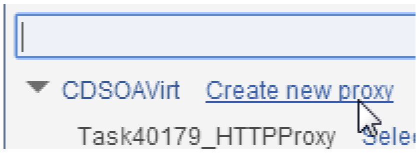
http **Target Application** - http://parabank.parasoft.com:80/* **Proxy** - http(s)://localhost:9080/parabank/services/bank/* Show details

+

Creating a New Proxy

To create and add a new proxy when configuring a component instance:

1. In the Components wizard area—or the Proxy area of the Instance editor, set **Proxy Type** to **Message**, then click **Select a message proxy**.
2. In the selection box that opens, click the **Create new proxy** link to the right of the Virtualize server on which you want the new proxy deployed.

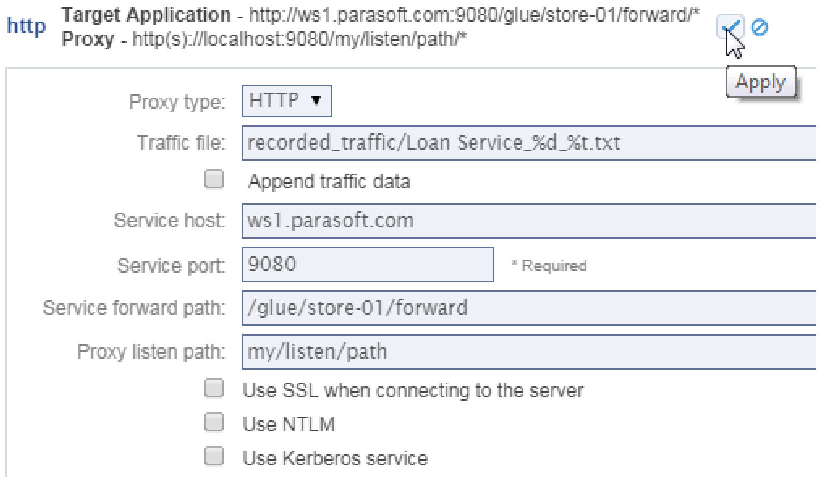


▼ CDSOAVirt Create new proxy

Task40179_HTTPProxy Selec

3. Specify proxy settings. Note that the **Target Application** connection setting must match the real or virtual endpoint specified for the current instance. For details, see Proxy Configuration Details.

4. Click the **Apply** icon.



http **Target Application** - http://ws1.parasoft.com:9080/glue/store-01/forward/*
Proxy - http(s)://localhost:9080/my/listen/path/*

Proxy type: HTTP ▾

Traffic file: recorded_traffic/Loan Service_%d_%t.txt

□ Append traffic data

Service host: ws1.parasoft.com

Service port: 9080 * Required

Service forward path: /glue/store-01/forward

Proxy listen path: my/listen/path

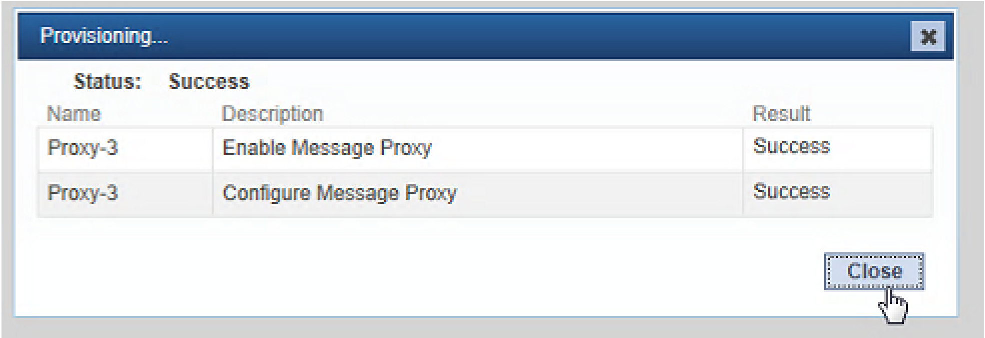
□ Use SSL when connecting to the server

□ Use NTLM

□ Use Kerberos service

Once the component is saved, the proxy will be added to the designated Virtualize server (and available in CTP). The proxy's name will be assigned by the Virtualize server (for example, Proxy-2). To see the new proxy in the Virtualize UI, refresh your Virtualize server view in the Virtualize UI.

The new proxy will be disabled until you provision an environment with this component instance. At that point, it will be enabled and configured. Any traffic files created from this proxy will be saved in Virtualize's VirtualAssets project by default.



Provisioning...

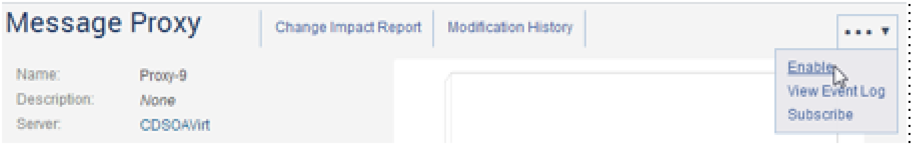
Status: Success

Name	Description	Result
Proxy-3	Enable Message Proxy	Success
Proxy-3	Configure Message Proxy	Success

Enabling Proxies

Proxies can be enabled by:

- Provisioning an environment with a component instance which uses that proxy.
- Selecting the **Enable** action from the proxy's page-level action menu.



Message Proxy

Name: Proxy-9
Description: None
Server: CDSOAVirt

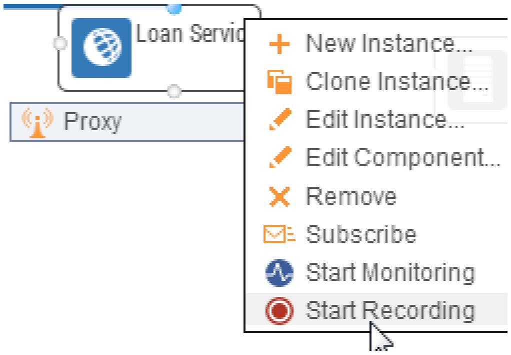
- Enabling the proxy in the Virtualize UI.
- Calling the appropriate operation from the Virtualize API.

Starting and Stopping Proxy Recording

Proxies must be enabled before CTP can start recording. Proxies can be enabled in CTP (e.g., by provisioning an instance with a proxy or enabling a proxy from its details page) or in Virtualize (e.g., from the Virtualize Server view). Proxy recording can be started and stopped from the Virtualize UI, Virtualize API, or CTP.

To start recording from CTP:

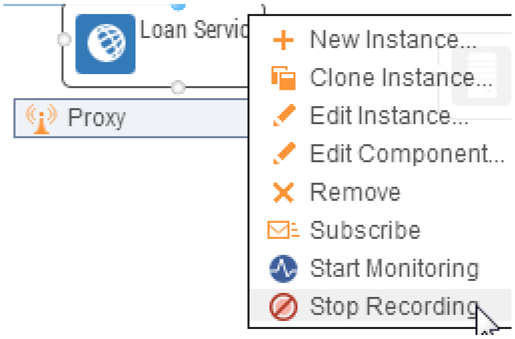
- In Edit mode, hover over the component set to use the enabled proxy, then select **Start Recording** from the drop-down menu.



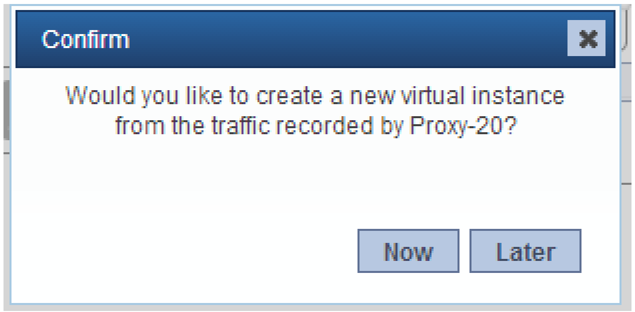
A box in the lower right corner will confirm that recording has started.

When you want to stop recording:

- In Edit mode, choose **Stop Recording** from the component's drop-down menu.



After recording stops, you'll see a dialog asking you whether you'd like to create a virtual asset for this recorded traffic now or later.



Confirm

Would you like to create a new virtual instance from the traffic recorded by Proxy-20?

If you choose **Now**, CTP will automatically preconfigure a new component instance with a new virtual asset for this traffic. You will just need to confirm the settings, (optionally) rename the instance, and click **Finish**, then the new virtual asset will be created and deployed.

Proxy Settings Details

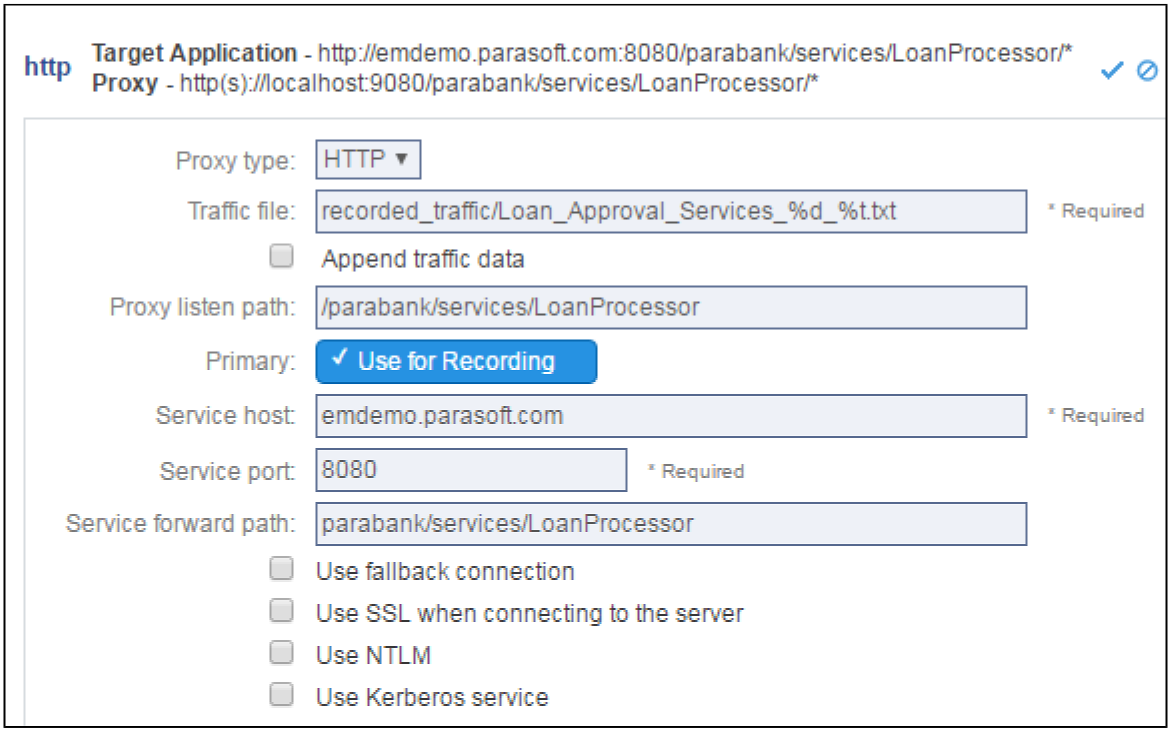
A "put" queue is always where the AUT/client is putting/sending request messages. A "get" queue is where the client/AUT is getting response messages from. Virtualize will capture request messages sent to the *client Put queue* and forward them to the *server Put queue f*or processing. The *server Get queue* is the queue that the server will place a response message on (after processing the request message). Virtualize will capture these messages and forward them to the *client Get queue*.

HTTP Options

Option	Description

Traffic file	Specify where you want to save the traffic data that will be captured when the proxy is set to record mode. You can later use this traffic file to generate virtual assets that represent the live traffic captured in record mode. By default, traffic will be recorded in a file named %n_%d_%t.txt (<proxy_name>_<current_date>_<current_time>.txt). It will be stored within the recorded_traffic folder (this will be created if it does not exist). You can modify the file name, but not the folder. The folder is always located within the VirtualAssets project. When specifying the file name, you can use variables such as %d (current date) %t (current time), %n (proxy name), and %u (unique time-based id). Wildcards can be used together and mixed in with the name. For example, you could use %nProxyTraffic%d or %u_%d%nTraffic. Do not configure multiple proxy connections to write to the same traffic file at the same time. This could corrupt the traffic file. **Append traffic data** adds new traffic data to an existing traffic file (the one specified in the Traffic file field). If the specified file does not already exist, a new file will be created
Proxy listen path	Enter the path where the proxy should listen for incoming connections. No two message proxies can have HTTP connections with the same proxy path or with a path that matches an existing virtual asset's HTTP path. In the simplest case, you can set P**roxy** listen **path** to the path of your service and leave **Service forward path** empty. With this configuration, the proxy will automatically forward all messages it receives on that path to the same path at the Service host and Service port. If you need the proxy to listen on a different path than the path of your service, set **Service forward path** to the actual path where you want the received messages to be sent. The proxy will forward the path and any query parts to the target service. If the **Proxy listen path** and the **Service forward path** are different, then any segments in the request after the **Proxy listen path** will be appended to the forwarded request. The **Proxy listen path** is essentially being replaced with the **Service forward path** so that the entire path (as received by the proxy) gets sent to the service.
Proxy URL	Displays the URL that should be given to the application under test (AUT).
Service host	Enter the host name of the machine where the service resides. This is the machine to which the proxy will send messages. If you want the proxy to forward to a virtual asset on the local Virtualize server without consuming an HTTP connection, enter localhost or 127.0.0.1 rather than the actual host name.
Service port	Enter the port where the service is listening. This is the port to which the proxy will send messages.
Service forward path	(Optional) Enter the path to which the proxy should forward the messages that it receives. If blank, this defaults to the value in the **Proxy listen path** field. If the HTTP proxy is sending messages to localhost, you must enter a **Service forward path** because the proxy doesn't allow forwarding to itself. If the **Service forward path** sends a redirect, the proxy will follow the redirect and then respond. It will not pass the redirect back to the client.
Additional options	• **Use fallback connection:** If you want traffic to be redirected to a fallback connection (e.g., a secondary proxy endpoint) when the primary connection fails or the responder/virtual asset is not available, enable this option. See the section below for details. • **Use SSL when connecting to the server:** If the service you are virtualizing uses SSL, enable this option and complete the fields that display.

	• **Use NTLM:** If the service you are virtualizing uses SSL, enable this option and complete the fields that display. • **Use Kerberos service:** If your service requires Kerberos authentication, enable this option and specify the service principal to authenticate the request.



http **Target Application** - http://emdemo.parasoft.com:8080/parabank/services/LoanProcessor/*
Proxy - http(s)://localhost:9080/parabank/services/LoanProcessor/*

Proxy type: HTTP ▾

Traffic file: recorded_traffic/Loan_Approval_Services_%d_%t.txt * Required

□ Append traffic data

Proxy listen path: /parabank/services/LoanProcessor

Primary: ✓ Use for Recording

Service host: emdemo.parasoft.com * Required

Service port: 8080 * Required

Service forward path: parabank/services/LoanProcessor

□ Use fallback connection

□ Use SSL when connecting to the server

□ Use NTLM

□ Use Kerberos service

Pointing to virtual assets or actual endpoints

A proxy can use a virtual asset on a Virtualize server as its target service. To do this:

1. Set the service host and port to that of the Virtualize server where the virtual asset is deployed. If you want the proxy to forward to a virtual asset on the local Virtualize server without consuming an HTTP connection, enter localhost or 127.0.0.1 rather than the actual host name.
2. Set the proxy connection’s **Service forward path** to the virtual asset’s path.

JMS Options

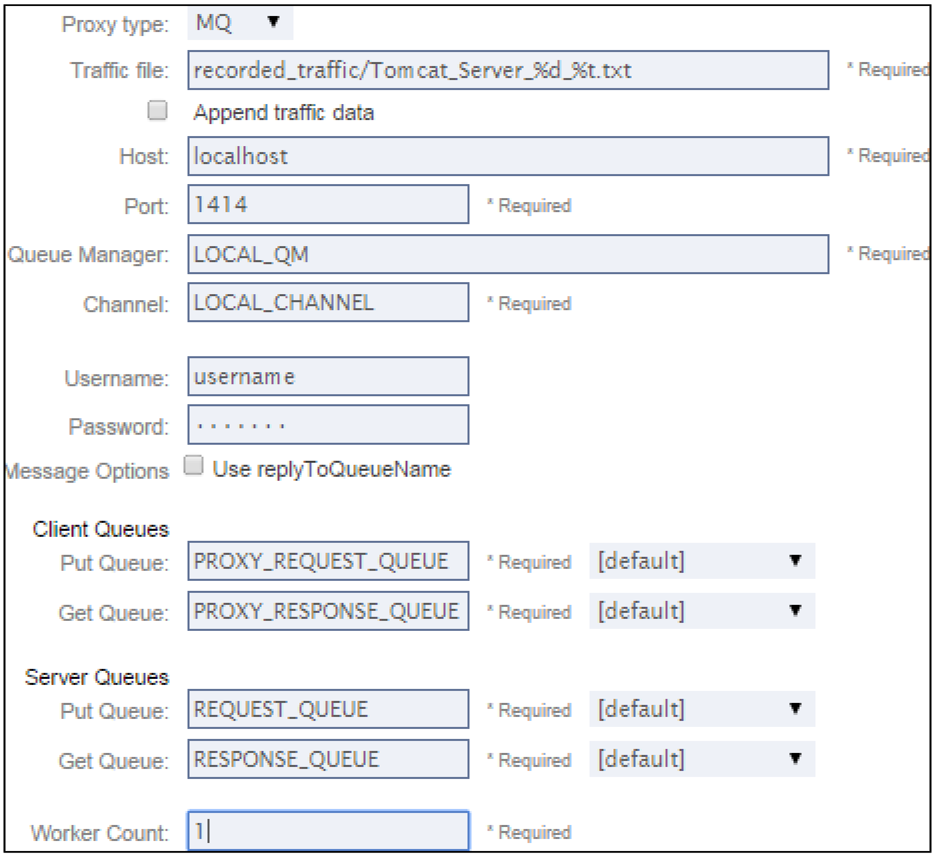
Option	Description
Traffic file	Specify where you want to save the traffic data that will be captured when the proxy is set to record mode. You can later use this traffic file to generate virtual assets that represent the live traffic captured in record mode. By default, traffic will be recorded in a file named %n_%d_%t.txt (<proxy_name>_<current_date>_<current_time>.txt). It will be stored within the recorded_traffic folder (this will be created if it does not exist). You can modify the file name, but not the folder. The folder is always located within the VirtualAssets project. When specifying the file name, you can use variables such as %d (current date) %t (current time), %n (proxy name), and %u (unique time-based id). Wildcards can be used together and mixed in with the name. For example, you could use %nProxyTraffic%d or %u_%d%nTraffic.

	Append traffic data adds new traffic data to an existing traffic file (the one specified in the Traffic file field). If the specified file does not already exist, a new file will be created
Provider URL	Specify the location of the JMS Administered Objects.
Initial context	Specify the Java class that contains all the JMS properties mappings.
Connection factory	Specify the key used to look up the MOM-specific factory from the initial context. This can be either a Queue Connection Factory or a Topic Connection Factory.
Username/password	Enter the username and password for authentication.
Queue/Topic	For Queues (Point-to-Point): Virtualize will capture messages sent to the client Destination queue and forward them to the server Reply to queue for processing. The server Destination queue is the queue that the server will place a response message on (after processing the request message). Virtualize will capture these messages and forward them to the client Reply to queue. For Topics (Publish-and-Subscribe): Virtualize monitors incoming requests on the client Subscribe topic and outgoing responses on the server Publish topic.
Use JMS ReplyTo	Specifies whether to use the message's JMSReplyToQueueName header to determine where the proxy sends the response. If it is enabled, values from the incoming request will be used to determine where to send the response. If it is not enabled, the response will be sent to the queue specified in the UI; the values in the JMS message header will be ignored.
Worker count	Worker count impacts the number of listener worker threads that get created.Increasing the worker count can help performance under concurrency.
Additional initial context JNDI properties	Specifies any additional JNDI properties you want applied to this deployment.

MQ Options

Option	Description
Traffic file	Specify where you want to save the traffic data that will be captured when the proxy is set to record mode. You can later use this traffic file to generate virtual assets that represent the live traffic captured in record mode. By default, traffic will be recorded in a file named %n_%d_%t.txt (<proxy_name>_<current_date>_<current_time>.txt). It will be stored within the recorded_traffic folder (this will be created if it does not exist). You can modify the file name, but not the folder. The folder is always located within the VirtualAssets project. When specifying the file name, you can use variables such as %d (current date) %t (current time), %n (proxy name), and %u (unique time-based id). Wildcards can be used together and mixed in with the name. For example, you could use %nProxyTraffic%d or %u_%d%nTraffic. **Append traffic data** adds new traffic data to an existing traffic file (the one specified in the Traffic file field). If the specified file does not already exist, a new file will be created
Host	Specify the name of the host running MQ.
Port	Specify the port where MQ is running.
Queue manager	Specify the queue manager.
Channel	Specify the name of the server-defined channel.

Username/password	Enter the username and password for authentication.
Use replyToQueueName	This option specifies whether to use the message's replyToQueueName header to determine where the proxy sends the response. It impacts responses to MQ messages of type MQMT_REQUEST.
Client and server queues	Specify the client and server queues. A "put" queue is always where the AUT/client is putting/sending request messages. A "get" queue is where the client/AUT is getting response messages from.
Worker count	Worker count impacts the number of listener worker threads that get created. Increasing the worker count can help performance under concurrency.



Proxy type: MQ ▼

Traffic file: recorded_traffic/Tomcat_Server_%d_%t.txt * Required

□ Append traffic data

Host: localhost * Required

Port: 1414 * Required

Queue Manager: LOCAL_QM * Required

Channel: LOCAL_CHANNEL * Required

Username: username

Password: ·······

Message Options □ Use replyToQueueName

Client Queues

Put Queue: PROXY_REQUEST_QUEUE * Required [default] ▼

Get Queue: PROXY_RESPONSE_QUEUE * Required [default] ▼

Server Queues

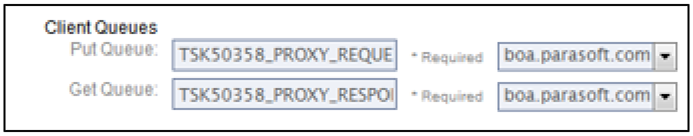
Put Queue: REQUEST_QUEUE * Required [default] ▼

Get Queue: RESPONSE_QUEUE * Required [default] ▼

Worker Count: 1 * Required

MQ Queue Managers

If you want to configure queues deployed on different MQ servers within a single proxy connection (e.g., you want a specific proxy connection to use two queues that are deployed on two different MQ servers), you can define them globally in Virtualize and reference them when configuring proxies in CTP.



Client Queues

Put Queue: TSK50358_PROXY_REQUE * Required boa.parasoft.com ▼

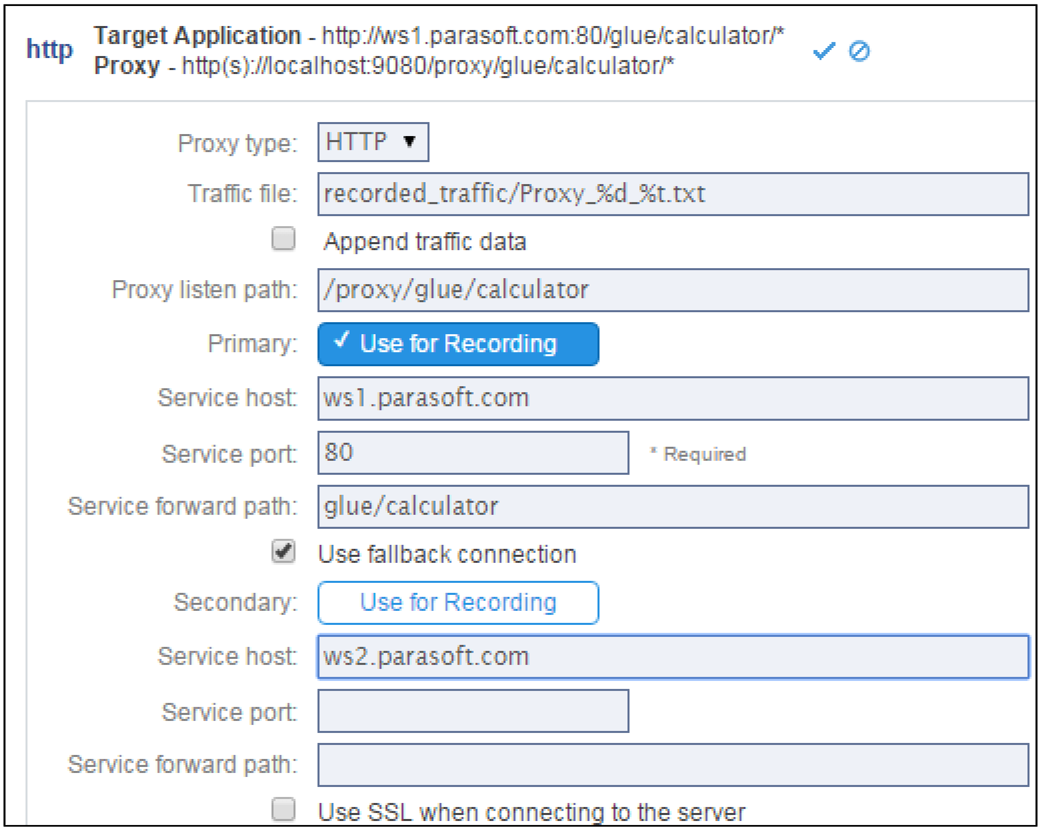
Get Queue: TSK50358_PROXY_RESPOI * Required boa.parasoft.com ▼

Specifying a Fallback Connection / Secondary Endpoint (HTTP/S Proxies Only)

If you want traffic to be redirected to a fallback connection (e.g., a secondary proxy endpoint) when the primary connection fails or the responder /virtual asset is not available, enable the **Use fallback connection** option, then provide connection details for the alternate endpoint. The connection will be considered "failed" if the response status code is 400 level or higher.

For instance, you might want to specify a secondary endpoint if you want a virtual asset to be used whenever the live endpoint is unavailable. Or, if a virtual asset does not handle a given use case, you could use a secondary endpoint to have that traffic redirected to the live endpoint. You could then optionally record that live traffic for creating a new virtual asset to cover that use case.

For both the primary and secondary connection, you can use the buttons to quickly toggle recording on or off. At least one of the connections must be enabled in order for recording to occur.



http **Target Application** - http://ws1.parasoft.com:80/glue/calculator/* ✓ ⊘
Proxy - http(s)://localhost:9080/proxy/glue/calculator/*

Proxy type: HTTP ▼
Traffic file: recorded_traffic/Proxy_%d_%t.txt
☐ Append traffic data
Proxy listen path: /proxy/glue/calculator
Primary: ✓ Use for Recording
Service host: ws1.parasoft.com
Service port: 80 * Required
Service forward path: glue/calculator
☑ Use fallback connection
Secondary: Use for Recording
Service host: ws2.parasoft.com
Service port:
Service forward path:
☐ Use SSL when connecting to the server

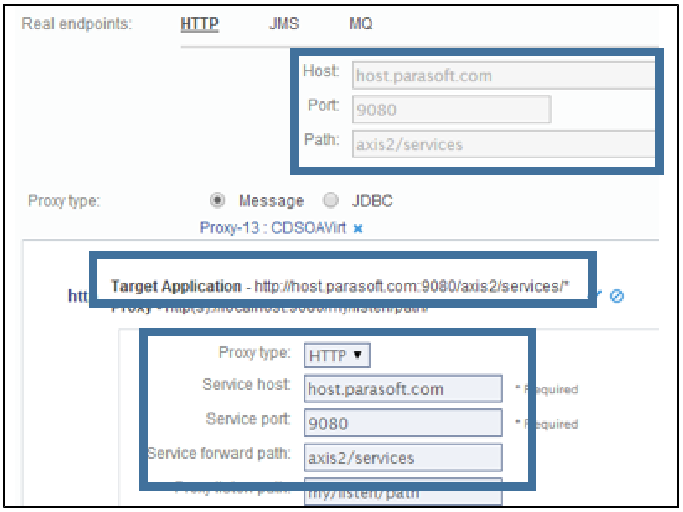
- **Using both connections for recording:** Records traffic for both the primary and secondary connections. Error messages from the primary will not be recorded; instead, the messages will be sent to the secondary and the responses will be recorded. Errors reported by the secondary will be recorded.
- **Using only the primary connection for recording:** Records traffic for the primary connection. Does not record errors.
- **Using only the secondary connection for recording:** Records traffic for the secondary connection, including errors.

Proxy Configuration Notes

Target Application Connection Settings Must Match Endpoint Settings

The Target Application connection setting must match the real or virtual endpoint specified for the current instance. The connection setting is derived from the various proxy fields. It is shown in the **Target Application** area.

For example, if you have an HTTP proxy, the **Service host**, **Service port**, and **Service forward paths** for the proxy must match the **Host**, **Port**, and **Path** for the real or virtual endpoint.



Real endpoints: HTTP JMS MQ

Host: host.parasoft.com

Port: 9080

Path: axis2/services

Proxy type: ● Message ○ JDBC

Proxy-13 : CDSOAVirt

Target Application - http://host.parasoft.com:9080/axis2/services/*

Proxy type: HTTP ▾

Service host: host.parasoft.com * Required

Service port: 9080 * Required

Service forward path: axis2/services

my/listen/path

Automated Updating of Endpoint and Proxy Settings

Proxy> Endpoint

If an endpoint is not already defined when you create a proxy, proxy settings will be automatically copied to the endpoints area when the proxy settings are applied.
If the proxy setting values you enter do not match the corresponding endpoint values, the endpoint values will automatically be updated when you apply your proxy settings.

Endpoint> Proxy

If a proxy is already defined and you edit endpoint settings, the corresponding proxy values will automatically be updated.

Instances with Virtual Assets as well as Proxies

If the component instance is configured with a virtual asset, only the following proxy fields will be editable:

- **For HTTP:** Listen path
- **For JMS with queues:** Client queues, Use JMSReplyTo, Worker Count, JNDI properties
- **For JMS with topics:** Use JMSReplyTo, Worker Count, JNDI properties, Use JMSReplyTo
- **For MQ:** Client get and put queues, Worker Count, Use replyToQueueName

For additional proxy configuration details and tips, see the Virtualize User's Guide.