

# Configuring Message Proxies

- [Configuring a Component Instance with an Existing Proxy](#)
- [Creating a New Proxy](#)
- [Enabling Proxies](#)
- [Starting and Stopping Proxy Recording](#)
- [Proxy Settings Details](#)
- [Proxy Configuration Notes](#)

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.

## Configuring a Component Instance with an Existing Proxy

1. Edit the environment diagram and choose **New Instance** from the component drop-down menu. The menu becomes visible on hover. See [Adding Component Instances](#) for details.
2. Specify a name and click the **Select a message proxy link**.

New Instance for Component 'Client'

**Components**    Health Checks    Variables

Name: docs-message-proxy \* Required

Description:

Provisioning action: Select a provisioning action

Virtual asset file: Select a virtual asset

Real endpoints: **HTTP**    JMS    MQ

Host:

Port:

Path:

Enable HTTP authentication

Message Proxy     JDBC Controller

[Select a message proxy](#)

3. If you want to select all connections for an available proxy, click **Select**.

Message Proxy     JDBC Controller

demo [Create new proxy](#)

- admin [Select](#) [Connections \(1\)](#)
- admin-2 [Select](#)
- Client-Proxy [Select](#)
- Cloud-Proxy [Select](#)
- Loan Service-Proxy [Select](#)
- LoanProcessor-Proxy [Select](#)
- LoanProcessor-Proxy-4 [Select](#)
- Proxy-Proxy [Select](#)

hanyuan [Create new proxy](#)

howland [Create new proxy](#)

- 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.

4. 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](#).

HTTP **JMS** MQ

Provider URL:

Username:

Password:

Initial context:

Message Selector Expression:

Point-to-Point  
 Publish-and-Subscribe

Connection factory:

Destination queue:

Reply to queue:

Additional initial context JNDI properties

Property	Value	
<input type="text" value="p3"/>	<input type="text" value="v3"/>	
<input type="text" value="p1"/>	<input type="text" value="v1"/>	

[+](#)

5. If you want to add a message proxy connection, click the **+** icon, then specify the connection settings as described in [Proxy Configuration Details](#).

Message Proxy  JDBC Controller  
 admin : emdemo ✕

**http** Target Application - http://localhost:9080/admin/\*  
 Proxy - http://localhost:9080/proxy/admin/\* Show details ✎ ✕

[+](#)

## Creating a New Proxy

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

1. Edit the environment diagram and choose **New Instance** from the component drop-down menu. The menu becomes visible on hover. See [Adding Component Instances](#) for details.
2. Click the **Create new proxy** link to the right of the Virtualize server on which you want the new proxy deployed.

Message Proxy  JDBC Controller  
[Select a message proxy](#)

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 Settings Details](#).

4. Click the **Apply** icon.

Target Application - Proxy

Proxy type: HTTP

Traffic file: recorded\_traffic/Docs\_New Type\_%d\_%t.txt \* Required

Append traffic data

Use HTTP listener

Port: 9081  Secure

Proxy listen path: my/listen/path

Primary:  Use for Recording

Service host: ws1.parasoft.com \* Required

Service port: 9080 \* Required

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

Use fallback connection

Use SSL when connecting to the server

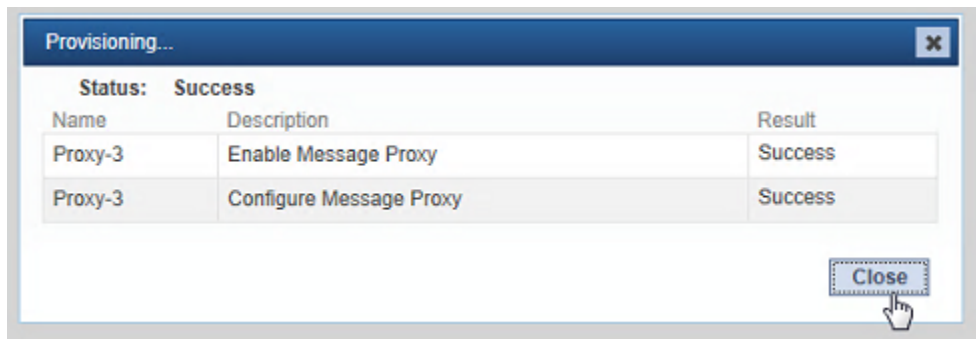
Use NTLM

Use Kerberos service

Cancel Finish

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.

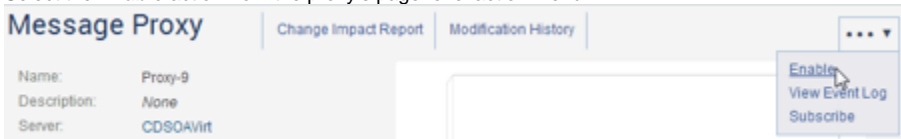
The new proxy will be disabled until you provision an environment with this component instance. At that point, it will be enabled and configured. Any traffic files created from this proxy will be saved in Virtualize's VirtualAssets project by default.



## Enabling Proxies

There are several ways to enable proxies:

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



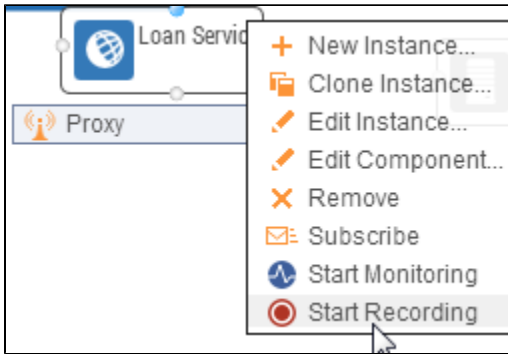
- Enable the proxy in the Virtualize UI.
- Call the appropriate operation from the Virtualize API.

## 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:

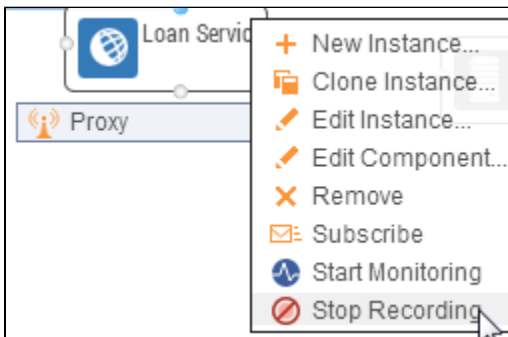
- In Edit mode, hover over the component set to use the enabled proxy, then select **Start Recording** from the drop-down menu.



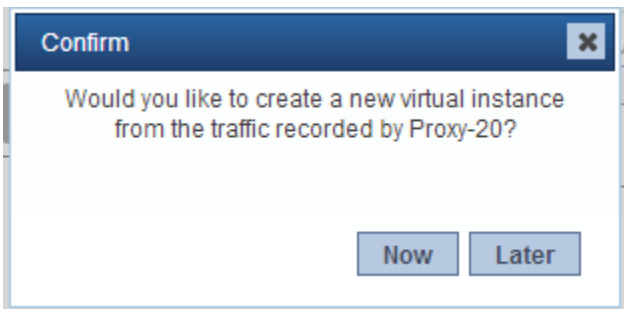
A box in the lower right corner will confirm that recording has started.

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.



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 puts/sends request messages. A "get" queue is where the client/AUT gets response messages. Virtualize will capture request messages sent to the *client Put queue* and forward them to the *server Put queue* for 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

Choose **HTTP** from the Proxy type drop-down menu to configure message proxies that connect over HTTP.

Option	Description
--------	-------------

<b>Traffic file</b>	<p>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.</p> <p>By default, traffic will be recorded in a file named %n_%d_%t.txt (&lt;proxy_name&gt;_&lt;current_date&gt;_&lt;current_time&gt;.txt) and will be stored within the recorded_traffic folder (this will be created if it does not exist). The traffic file must be inside the VirtualAssets project when provisioning an instance that contains the message proxy. If set a location outside of the VirtualAssets project, the provision request (PUT request) will fail. CTP, however, can read a traffic file (GET request) that is outside of the VirtualAssets project when the proxy was configured with Virtualize.</p> <p>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.</p> <p>Do not configure multiple proxy connections to write to the same traffic file at the same time. This could corrupt the traffic file.</p>
<b>Append traffic data</b>	<p>Enable this option to add new traffic data to an existing traffic file (the one specified in the <b>Traffic file</b> field). If the specified file does not already exist, a new file will be created</p>
<b>Use HTTP listener</b>	<p>Enable this option to specify a port specific to your proxy.</p> <p>If the client sends traffic over SSL, enable the <b>Secure</b> option and specify your verification options:</p> <ul style="list-style-type: none"> <li>• Enable <b>Use Keystore</b> and specify the server-side authentication settings.</li> <li>• Enable <b>Perform client authentication</b> and specify the trust store verification settings.</li> </ul> <div data-bbox="245 751 1479 856" style="border: 1px solid #ccc; padding: 10px; margin: 10px 0;"> <p> <b>Version Compatibility</b></p> <p>Virtualize 9.10.4 or newer is required to use HTTP listeners.</p> </div> <p>You can configure one listener per proxy. If you want to use multiple HTTP listeners, you must create multiple components and configure them separately. For additional information about HTTP listeners, see the <a href="#">Virtualize Desktop documentation</a>.</p>
<b>Proxy listen path</b>	<p>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.</p> <p>In the simplest case, you can set the <b>Proxy listen path</b> to your service's path and leave the <b>Service forward path</b> setting 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.</p> <p>If you need the proxy to listen on a different path than the path of your service, set <b>Service forward path</b> 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.</p> <p>If the <b>Proxy listen path</b> and the <b>Service forward path</b> are different, then any segments in the request after the <b>Proxy listen path</b> will be appended to the forwarded request. The <b>Proxy listen path</b> is essentially being replaced with the <b>Service forward path</b> so that the entire path (as received by the proxy) gets sent to the service.</p>
<b>Proxy URL</b>	<p>Displays the URL that should be given to the application under test (AUT).</p>
<b>Service host</b>	<p>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.</p>
<b>Service port</b>	<p>Enter the port where the service is listening. This is the port to which the proxy will send messages.</p>
<b>Service forward path</b>	<p>(Optional) Enter the path to which the proxy should forward the messages that it receives. If blank, this defaults to the value in the <b>Proxy listen path</b> field. If the HTTP proxy is sending messages to localhost, you must enter a <b>Service forward path</b> because the proxy doesn't allow forwarding to itself. If the <b>Service forward path</b> sends a redirect, the proxy will follow the redirect and then respond. It will not pass the redirect back to the client.</p>
<b>Additional options</b>	<ul style="list-style-type: none"> <li>• <b>Use fallback connection:</b> 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 <a href="#">section below</a> for details.</li> <li>• <b>Use SSL when connecting to the server:</b> If the service you are virtualizing uses SSL, enable this option and complete the fields that display.</li> <li>• <b>Use NTLM:</b> If the service you are virtualizing uses SSL, enable this option and complete the fields that display.</li> <li>• <b>Use Kerberos service:</b> If your service requires Kerberos authentication, enable this option and specify the service principal to authenticate the request.</li> </ul>

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

**i** 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
<b>Traffic file</b>	<p>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.</p> <p>By default, traffic will be recorded in a file named %n_%d_%t.txt (&lt;proxy_name&gt;_&lt;current_date&gt;_&lt;current_time&gt;.txt) and will be stored within the recorded_traffic folder (this will be created if it does not exist). The traffic file must be inside the VirtualAssets project when provisioning an instance that contains the message proxy. If set a location outside of the VirtualAssets project, the provision request (PUT request) will fail. CTP, however, can read a traffic file (GET request) that is outside of the VirtualAssets project when the proxy was configured with Virtualize.</p> <p>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.</p> <p><b>Append traffic data</b> 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</p>
<b>Provider URL</b>	Specify the location of the JMS Administered Objects.
<b>Initial context</b>	Specify the Java class that contains all the JMS properties mappings.
<b>Connect ion factory</b>	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.
	Enter the username and password for authentication.

<b>Username /password</b>	
<b>Queue /Topic</b>	<p>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.</p> <p>For Topics (Publish-and-Subscribe): Virtualize monitors incoming requests on the client Subscribe topic and outgoing responses on the server Publish topic.</p>
<b>Use JMS ReplyTo</b>	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.
<b>Worker count</b>	Worker count impacts the number of listener worker threads that get created. Increasing the worker count can help performance under concurrency.
<b>Additional initial context JNDI properties</b>	Specifies any additional JNDI properties you want applied to this deployment.

## MQ Options

Option	Description
<b>Traffic file</b>	<p>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.</p> <p>By default, traffic will be recorded in a file named %n_%d_%t.txt (&lt;proxy_name&gt;_&lt;current_date&gt;_&lt;current_time&gt;.txt) and will be stored within the recorded_traffic folder (this will be created if it does not exist). The traffic file must be inside the VirtualAssets project when provisioning an instance that contains the message proxy. If set a location outside of the VirtualAssets project, the provision request (PUT request) will fail. CTP, however, can read a traffic file (GET request) that is outside of the VirtualAssets project when the proxy was configured with Virtualize.</p> <p>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.</p> <p><b>Append traffic data</b> 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</p>
<b>Host</b>	Specify the name of the host running MQ.
<b>Port</b>	Specify the port where MQ is running.
<b>Queue manager</b>	Specify the queue manager.
<b>Channel</b>	Specify the name of the server-defined channel.
<b>Username /password</b>	Enter the username and password for authentication.
<b>Use replyTo QueueName</b>	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.
<b>Client and server queues</b>	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.
<b>Worker count</b>	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 x

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

Proxy - http(s)://localhost:9080/proxy/glue/calculator/\*

Proxy type: HTTP

Service host: host.parasoft.com \* Required

Service port: 9080 \* Required

Service forward path: axis2/services

## 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.