The Mainframe Software Partner
For The Next 50 Years

iStrobe
Configuration Guide

Release 17.02

Please direct questions about iStrobe
or comments on this document to:

iStrobe Customer Support

https://go.compuware.com

Doc. CWISDX1723
January 4, 2017

Contents

Introduction

This guide provides instructions to complete the configuration of iStrobe after it has been installed via Compuware Enterprise Services (see the *Compuware Web Products Installation and Configuration Guide* for the installation of iStrobe and other Compuware products that use that service).

iStrobe is an application performance analysis product designed to interface with the Strobe MVS Application Performance Measurement System and runs in the Compuware Enterprise Services web application server.

After installing iStrobe, you will be able to view the sample Performance Profile data packaged with it.

Intended Audience

This installation guide is intended for the administrator or individual installing iStrobe. You should be familiar with administering the operating system and your network security policies. If you are unfamiliar with any of the prerequisite software, contact your administrator for help.

How This Guide is Organized

This guide contains the following chapters and appendixes:

Chapter 1, “iStrobe System Overview”

Chapter 2, “iStrobe Configuration”

Appendix A, “iStrobe APIs”

Appendix B, “iStrobe Plug-in for Topaz Workbench”

iStrobe Publications

To learn more about using iStrobe:

- See the iStrobe online help within the product.
- Visit FrontLine, Compuware’s support website at **https://go.compuware.com** and select iStrobe, for the latest technical information on iStrobe.

iStrobe 3rd Party Licensing Documentation

To view iStrobe 3rd party licensing documentation, refer to the legal subdirectory that is included as part of the iStrobe installation.

Compuware Customer Support

Compuware provides a variety of support resources to make it easy for you to find the information you need.

Compuware FrontLine Customer Support Website

You can access online information for Compuware products via our FrontLine customer support website at **https://go.compuware.com**.

Compuware FrontLine provides access to critical information about your Compuware products. You can review frequently asked questions, read or download documentation, access product fixes, or e-mail your questions or comments. The first time you access Compuware FrontLine, you are required to register and obtain a password. Registration is free.

Contacting Customer Support

Phone

- USA and Canada: 1-800-538-7822 or 1-313-227-5444.
- All other countries: Contact your local Compuware office. Contact information is available at **https://go.compuware.com**.

Web

You can report issues via the Quick Link **Create & View Support Cases** on the Compuware FrontLine home page.

Note: Please report all high-priority issues by telephone.

Mail

Compuware Customer Support
Compuware Corporation
One Campus Martius
Detroit, MI 48226-5099

Corporate Website

To access Compuware's site on the Web, go to **https://www.compuware.com**.

The Compuware site provides a variety of product and support information.

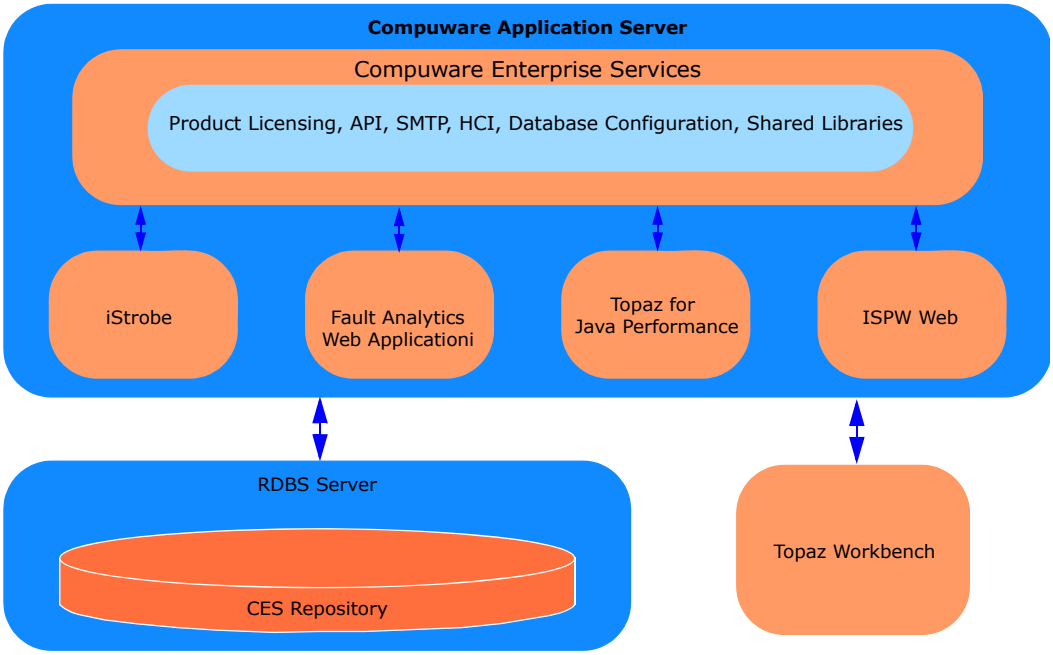
Chapter 1.
iStrobe System Overview

The diagram below is an overview of the components and data flow in iStrobe.

iStrobe is required to be installed in the same operating system environment as that in which CES was installed so that iStrobe's files are contained within the CES installation directory.

Refer to the operating systems-specific installation chapters for setup and security considerations.

Figure 1-1. iStrobe Components and Data Flow



Software and Hardware Requirements

For complete software and hardware requirements, refer to the details described in the *iStrobe Release Notes* for this version.

Individuals to Participate in the Installation

This section identifies individuals who should participate in the installation and the information needed to complete the installation.

Installation Environment

The installation environment requires an administrator familiar with either a Windows, z/OS Unix, or zLinux environment, as is appropriate for your site. The user performing the installation needs to have the appropriate authorizations in the selected environment.

Security Environment

The security features in iStrobe can utilize LDAP security servers for user authentication. To implement LDAP, the iStrobe server post-installation configuration requires a security administrator with knowledge of LDAP security settings.

Chapter 2.
iStrobe Configuration

By default, the iStrobe installation, via Compuware Web Products, sets up much of the application configuration. Compuware recommends reviewing all the configuration parameters after initially installing the application. Refer to the iStrobe online help for detailed configuration instructions.

After installing iStrobe, Compuware recommends configuring the following:

- Host Connections
- Security
- SMF Manager Settings (within General Configuration)
- Profile Email Settings (within General Configuration)

You may also optionally configure the following:

- Auto Delete
- Users,Roles, and Groups
- SMF Data Management
- Profile History
- General Configuration
  - Profiles
  - Usage Data
  - BMC Mainview Explorer

Starting iStrobe

1. Open the iStrobe application by pointing your web browser to:

   `<host address>:<application server port number>/istrobe`

   - *host address* is the name of the server where you just installed iStrobe.
   - *application server port number* is the port on which the application server is listening.
2. Start iStrobe in your browser and click the **Administration** button. The **Administration** page appears.
3. Login to iStrobe by providing any user name. From the iStrobe landing page, click **Administration** and provide the default password **isadministration**.

Default Password

The default password for configuring iStrobe settings is `isadministration`. Enter the administration password and click **OK**.

Host Connections Configuration

Host Connections are used to define configuration connections to the Host Communications Interface (HCI) component to support measurement requests from the iStrobe Web Service. The Compuware HCI can be configured to support multiple Strobe instances within a network.

1. Start iStrobe in your browser, click the **Administration** button. The Administration page appears.
2. Click **Host Connections**. The **Host Connections** page appears.

   This page allows you to enter specifications for multiple HCI instances. Refer to the Strobe/HCI Configuration documentation for more information on details to support multiple Strobe instances. If you wish to use this web service, contact Compuware Technical Support for full documentation.

Security Configuration

The security features in iStrobe are optional and can utilize your existing LDAP security servers, X.509 certificates from a smart card, or Kerberos for user authentication. iStrobe does not store passwords, but does store user IDs. By requiring a user ID and either a password or PIN to access iStrobe, you are able to provide role-based content and give users access to specific functionality.

By default, iStrobe security is *disabled* upon first installing iStrobe and all content is available to all users.

As an administrator, you may configure and enable iStrobe security after installing iStrobe. The first time you click the button to the administration section, you are prompted to provide the administration password. The default password is "isadministration". Having been provided the password, you are able to act as the administrator and enable security. You also have the ability to change the administrator password. Do this by clicking the **Security** button within the **Administration** section.

Note: Although you are not required to secure content, you should consult with the network security group at your site to determine whether or not to enable security for iStrobe. You always have the ability to disable security that has been enabled.

With security configured, users must present credentials for authentication and access to iStrobe. When security is enabled with an LDAP authentication server, users are prompted for both a user ID and password. When security is enabled with an X.509 certificate from a smart card, users are prompted for a PIN only.

Enable security using LDAP

To configure and enable LDAP security, the security administrator must provide the following:

- iStrobe administrator(s) ID. *Do not* include the domain name in this field.
- Binding URL for binding the URL to the LDAP server
- Distinguished Name (DN) of a service account used to search LDAP for the service account
- Password of an account that can be used to bind to the LDAP server
- Search base and filter to use to locate the user's ID

When logging on, users are prompted for their user ID and password.

1. Start iStrobe in your browser and click the **Administration** button. The **Administration** page appears.
2. Click **Security**. The **Security** page appears.
3. Select the LDAP security mode:
4. Enter the required information in each of the fields:

   - LDAP server URL
     The location of the server running LDAP (Lightweight Directory Access

Protocol).
`Ex. ldap://ldap.example.com`

- LDAP server port number
  The port used for LDAP on the server
- Bind with
  The process where the LDAP server authenticates the client. This can be done with either a search filter or a DN. If binding with User DN, another dialog box will be displayed for Login ID and Password.
- Distinguished name (DN)
  A DN is a sequence of relative distinguished names (RDN) which are connected with commas. Each RDN is an attribute value pair (i.e., attribute1=value1,attribute2=value2). Note that spaces are not to be included after commas. If binding with DN, enter CN={0} and on the next dialog, whatever value supplied to Login ID will be used in place of {0}.
  `Ex. CN={0},OU=User Accounts,OU=Detroit Corp,DC=example,DC=corp`
- Password for DN
  Required only when binding with search filter. If binding with DN, another dialog box will be displayed for this information.
- Search base
  Required only when binding with search filter. This defines the base level in the directory where the search will begin at. This is defined with the DN of the search base object.
  `Ex. OU=Sales,DC=example,DC=com`
- Search filter
  Required only when binding with search filter. This defines how to filter the search, such as including or excluding specific values.
  `Ex. (cn={0}) - This will search for an entry with the cn (common name) equal to the User ID entered. It is required for the search filter to have the parentheses such as listed in our example.`
- iStrobe administrator(s)
  Required so that the iStrobe administrator account can be set in the database. Otherwise, you may be locked out of the system once the security mode is set.

5. Click **LDAP server connection test**. If an LDAP server connection is available, you will be able to apply this security configuration.
6. Click **Apply**.

You *must* restart your web application for the security settings to become effective. When logging on, users will be prompted for their user ID and password.

Enable security using X.509 (Smart Card)

With security configured for X.509 (Smart Card), users must first have their smart card plugged into the reader. They must also have a valid X.509 certificate. And they must log on using the `https://` protocol as the first element in the URL.

To configure and enable X.509 (Smart Card) security, the security administrator must provide the following:

- iStrobe administrator(s) ID
- X.509 mask. This is needed to extract the user ID from the smart card certificate.

When logging on, users are prompted for their smart card PIN. Those users without both the smart card and PIN for that card are denied access to iStrobe.

1. Start iStrobe in your browser and click the **Administration** button. The **Administration** page appears.
2. Click **Security**. The **Security** page appears.
3. Select the X.509 (Smart Card) security mode:
4. Enter the required information in each of the fields:
    - X.509 mask
    - iStrobe administrator(s)
5. Click **Apply**.

You *must* restart your web application for the security settings to become effective. When logging on, users will be prompted for their smart card PIN.

Enable security using X.509 with LDAP

With security configured for X.509 with LDAP, users can log on with a smart card and PIN using the `https://` protocol or with LDAP using the `http://` protocol.

To configure and enable X.509 with LDAP security, the security administrator must provide the following:

- LDAP server URL
- LDAP server port number
- Distinguished name (DN)
- Password for DN
- Search base
- Search filter
- iStrobe Administrator
- X.509 mask. This is needed to extract the user ID from the smart card certificate.

1. Start iStrobe in your browser and click the **Administration** button. The **Administration** page appears.
2. Click **Security**. The **Security** page appears.
3. Select the X.509 with LDAP security mode:
4. Enter the required information in each of the fields:
    - LDAP server URL
      The location of the server running LDAP (Lightweight Directory Access Protocol).
      `Ex. ldap://ldap.example.com`
    - LDAP server port number
      The port used for LDAP on the server
    - Bind with
      The process where the LDAP server authenticates the client. This can be done with either a search filter or a DN. If binding with User DN, another dialog box will be displayed for Login ID and Password.
    - Distinguished name (DN)
      A DN is a sequence of relative distinguished names (RDN) which are connected with commas. Each RDN is an attribute value pair (i.e., attribute1=value1,attribute2=value2). Note that spaces are not to be included after commas. If binding with DN, enter CN={0} and on the next dialog, whatever value supplied to Login ID will be used in place of {0}.
      `Ex. CN={0},OU=User Accounts,OU=Detroit Corp,DC=example,DC=corp`
    - Password for DN
      Required only when binding with search filter. If binding with DN, another dialog box will be displayed for this information.

- Search base
  Required only when binding with search filter. This defines the base level in the directory where the search will begin at. This is defined with the DN of the search base object.
  `Ex. OU=Sales,DC=example,DC=com`
- Search filter
  Required only when binding with search filter. This defines how to filter the search, such as including or excluding specific values.
  `Ex. (cn={0}) - This will search for an entry with the cn (common name) equal to the User ID entered. It is required for the search filter to have the parentheses such as listed in our example.`
- X.509 mask
  Extracts the user ID from the smart card certificate.
- iStrobe administrator(s)
  Required so that the iStrobe administrator account can be set in the database. Otherwise, you may be locked out of the system once the security mode is set.

5. Click **LDAP server connection test**. If an LDAP server connection is available, you will be able to apply this security configuration.
6. Click **Apply**.

You *must* restart your web application for the security settings to become effective. When logging on, users will be prompted for their user ID and password for LDAP or their smart card PIN.

Enable security using Kerberos

With security configured for Kerberos, users are automatically signed on using their user ID.

To configure and enable Kerberos, the security administrator must provide the following:

- Service principal
- Keytab location
- iStrobe administrator(s).

1. Start iStrobe in your browser and click the **Administration** button. The **Administration** page appears.
2. Click **Security**. The **Security** page appears.
3. Select the Kerberos security mode:
4. Enter the required information in each of the fields:
   - Service principal
   - Keytab location
     Set this as a URL.
     `Ex. file:///etc/s100086.keytab`
   - iStrobe administrator(s)
5. Click **Kerberos login test**. If you are able to log in, you will be able to apply this security configuration.
6. Click **Apply**.

You *must* restart your web application for the security settings to become effective. When logging on, users are not prompted.

Important:
Only administrators can add or remove users and manage access to specific functionality. This function appears in the list of functions on the administration tab in the Application Controls panel. See "Profile Email Configuration" on page 15.

Disable security

1. Start iStrobe in your browser and click the **Administration** button. The **Administration** page appears.
2. Click **Security**. The **Security** page appears.
3. Select the **None** radio button. You can optionally disable the User Login and Administration Password requirements when logging into Administration by clearing the check boxes for those features.
4. Click **Apply**.

You must restart your web application for the security settings to become effective. When logging on, users are no longer prompted for their user ID and password, and all content and profiles are available to all users.

SMF Manager Settings Configuration

SMF Manager Settings enables SMF data collection. For this functionality to work, you must do the following:

- Configure associated fields in the Strobe Parameter dataset, and set the SMF Port number to match that specified in iStrobe.
  - **GM_MONITOR**: Specifies whether to enable Global Monitoring. Must = YES for SMF processing.
  - **GM_SMFDATA**: Specifies that SMF Data is to be collected and sent to iStrobe. Must = YES for SMF processing.
  - **GM_SMFHOST** or **GM_SMFIP**: GM_SMFHOST indicates the iStrobe SMF server name. GM_SMFIP indicates the iStrobe SMF server IP address. Specify either GM_SMFHOST or GM_SMFIP. If both are specified, GM_SMFHOST is used.
  - **GM_SMFPORT**: Specifies the iStrobe SMF server port number. Must equal the SMF port number applied in iStrobe.
  - **GM_TCPNAME**: Specifies the TCP/IP job name of the IP Stack on the LPAR that Global Monitoring SMF is to use.
  - **MNASPROCNAME**: Specifies the Global Monitoring Address Space (MNAS) startup procedure name. This job comes up with Strobe and must be executing.

1. Start iStrobe in your browser and click the **Administration** button. The **Administration** page appears.
2. Click **General Configuration**. The **General Configuration** page appears.
3. In the **SMF Manager Settings** section, enable SMF data collection in iStrobe by placing a check mark in the **Enable SMF data collection** box. Enter an SMF port number, or use the default port number as provided. Click **Apply** to save and apply these settings.

Profile Email Configuration

The Profile Email Settings option allows you to customize the email notifications received when either a measurement completes and a profile is created or when sending profile links by email. These settings are populated by default but can be customized.

Further details for customizing email notifications are provided in the online help for iStrobe.

Appendix A.
iStrobe APIs

iStrobe accepts an HTTP request to initiate a Strobe measurement of an active z/OS process. You can use this feature with a performance monitor to start a Strobe measurement when you notice performance problems on the mainframe and would like a deep-dive analysis.

Among the APIs:

- Measurement API
- SQLAF On Demand API
- Alternative Measurement API

iStrobe Configuration

To configure iStrobe you need to specify Host Name or IP address, Port number, and Strobe signature for each System you want to use with the APIs. The z/OS systems programmer who set up Strobe and the HCI will have this information. Go to the **Administration section** and select **Host Connections**. You may configure as many HCIs as needed to connect to your Strobe Release 5.2 and above installations. The connection for an individual measurement is specified in the Web Service request. Refer to the iStrobe online help **Manage HCIs** page for more details about the individual fields.

Measurement API

In the Measurement API, measurement requests are sent to the iStrobe Web Server as a Web Service request via HTTP or HTTPS. You should consider using an HTTPS connection, because the z/OS ID and password are included in the request. The z/OS ID only needs permission to start a Strobe measurement. It does not need access to TSO.

Requesting WSDL URL

The Web Services Description Language (WSDL) of this Web Service can be retrieved using this URL:

Figure A-1. URL to Retrieve WSDL

```
HTTP://<server>:<port>/iStrobe/ws/Measurement/measurement.wsdl
```

Web Service Request to iStrobe Server

The SOAP body expected by the iStrobe Web Service is described below. The requester will receive the return value formatted as a SOAP response. See below for the available request types.

Figure A-2. URL Format of the Web Service Request to the iStrobe Server

```
HTTP://<server>:<port>/iStrobe/ws/Measurement
```

When the message for an “addActive” request is sent to the iStrobe Web Service, a response will be returned. If the request is successfully processed, the response will include the URL for the iStrobe measurement report.

Figure A-3. Example Web Service Request SOAP Body Format

```
<!-- Copyright (c) 2010 Compuware Corporation.  All rights reserved. -->
<AddActiveRequest xmlns="http://istrobe.compuware.com/ws/Measurement" >
    <reqType>addActive</reqType> <!-- addQueue for Add Queued request -->
    <logonid>mainframe-userid</logonid>
    <password>mainframe-password</password><!-- sample java code will ask this value at runtime
     -->
    <jobname>YOURJOBO</jobname>
    <system>yourSystem</system>
    <!-- Optional -->
    <tags>list of tags</tags>
    <profileName>profile name to be created</profileName>
    <emailto>email-id to notify</emailto><!-- iStrobe should be configured to use email
    notification -->
    <duration>minimum measurement time</duration>
    <samples>number of samples</samples>
    <limit>number of smaple dataset to be created</limit>
    <finalAction>quit|stop|continue</finalAction>
    <hlq>MY.GROUP</hlq>
    <tranid>transaction id mask</tranid>
</AddActiveRequest>
```

Descriptions of Elements

reqType

addActive. Adds a request for measurement of an active job.

logonid

Required. z/OS logon ID.

password

Required. z/OS password. An SSL connection should be used to prevent exposing the password to the network.

jobname

Required. Jobname to be measured.

system

Required. Host Connection name defined by the iStrobe HostConnections configuration screen.

tags

Optional. Tags to be assigned to profile.

profileName

Optional. Name of the profile. The default is the jobname.

emailto

Optional. SMTP e-mail address to notify when the measurement is complete and the profile is ready to view.

duration

Optional. Estimated minimum measurement time in minutes. See the *Strobe User Guide* for details.

samples

Optional. The target number of samples to take during the measurement session. See the *Strobe User Guide* for details.

limit

Optional. Suspends sampling when the target number of samples is reached. See the *Strobe User Guide* for details.

finalAction

Optional. Controls the measurement session when the final dataset has been completed. Value can be one of the following: {QUIT | STOP | CONTINUE}. See the *Strobe User Guide* for details.

hlq

Optional. High Level Qualifier. DSNAME High level qualifier - Temporary dataset prefix.

tranid

Optional. May occur up to 5 times. Used for transaction profiling, the tranids are transaction ID masks used to specify the transactions to be measured.

Figure A-4. Example of Returns: SOAP Body Format

```
<?xml version="1.0" encoding="UTF-8"?>
<ns2:AddActiveResponse xmlns:ns2="http://istrobe.compuware.com/ws/Measurement">
    <ns2:reqType>addQueue</ns2:reqType>   <!-- addActive | addQueue -->
    <ns2:returnCode>0</ns2:returnCode>
    <!-- below is the iStrobe reporter url when the returnCode is less than 5 -->
    <ns2:reportUrl>http://iStrobe.server:8080/iStrobe43/iStrobe.html?js=on&amp;auto=on&
    amp;report=MSD&amp;profile=D%3A%5Ceclipse%5C... Sample11</ns2:reportUrl>
    <ns2:messageList>
        <ns2:message>STR6300I Input = ADD SBHCI,STEP=*ALL,GOMIN=0002,SAMPLES=009999,
        NONOTIFY,LIMIT=(01,QUIT),ISPFFLAG=0000,RJCLFILE=(_YES_)</ns2:message>
        <ns2:message>STR6261I 0581 JOBNAME1 QUEUED STEP=*ALL CREATED=(09:29:53
        06/23/2011) GOMIN=2 SAMPLES=9999 LIMIT=(1,QUIT)</ns2:message>
        <ns2:message>STR6261I EXPIRATION=(06/30/2011) NONOTIFY</ns2:message>
        <ns2:message>STR6130I ADD operation completed</ns2:message>
    </ns2:messageList>
    <ns2:statusList>
        <ns2:status number="581" state="QUEUED"/>  <!-- QUEUED | RUNNUNG -->
    </ns2:statusList>
</ns2:AddActiveResponse>
```

If there is an error in the addActive request, the return code will be non-zero with an appropriate message.

connectTest Web Service Request to iStrobe Server - Detail

This request is used to test the z/OS connection information to confirm that it is correct and available.

Figure A-5. URL Format of connectTest Web Service Request

```
HTTP://<server>:<port>/iStrobe/ws/Measurement
```

See Figure A-6 for the available request types.

Figure A-6. Web Service Request SOAP Body Format

```
<ConnectTestRequest xmlns="http://istrobe.compuware.com/ws/Measurement"/>
```

Figure A-7. Returns (Response): Soap Body Format

```
<?xml version="1.0" encoding="UTF-8"?>
<ConnectTestResponse>
      <returnCode>nnnn</returnCode>
      <message>message_string</message>
</ConnectTestResponse>
```

If there is an error in the connectTest request, the return code will be non-zero with an appropriate message. If the request is successful, the return code will be 0, and the message will include the available system list.

Using SSL with the Web Service

You may secure communications between the web server and the web service client using Secure Sockets Layer (SSL/HTTPS). The protocol is controlled by the web server (Compuware Enterprise Services). No special coding is needed in the iStrobe web service.

Settings for the web server configuration for SSL and the client should be documented by the web server provider. Here is an example of how to set up the SSL configuration for the CES server and the web service client using Java Secure Socket Extension (JSSE).

Compuware Enterprise Services Server Configuration for SSL

To configure the Compuware Enterprise Services server for HTTPS, use the instructions at the following link:

```
https://wiki.eclipse.org/Jetty/Howto/Configure_SSL#Setting_the_Port_for_https
```

The file to modify to add the SSL connector is:

```
<ces install dir>/data/jetty/etc/jetty_selector.xml
```

To use Smart Card support for authentication, use the following parameter in jetty_selector.xml:

```
-wantClientAuth=true
```

Web Service Java Client Using SSL Connection

To access iStrobe web service via SSL, use the following JVM parameter:

```
-Djavax.net.ssl.trustStore=client.keystore
```

Or, you can set the following parameter in your web service client Java program:

```
System.setProperty("javax.net.ssl.trustStore", "<proper-path>/client.keystore");
```

The file **client.keystore** is the same file generated in the previous section. The URL for the web service will be similar to the following:

```
https://istrobeHost:8443/iStrobe
```

SQLAF On Demand API

The SQLAF On Demand API executes the Strobe for DB2 SQL Analysis Feature on the supplied SQL statement. The output will be a browser window with the analysis. There is no parsing of the statement to determine if it is syntactically correct.

Issue a post request:

```
http://<server>:<port>/istrobe/jsp/public/sqlaf.jsp?lpar=X&sqlText=Y&ssid=Z
```

lpar:

This is the LPAR where Strobe is installed. Required to find an appropriate HCI connection to use.

sqlText:

This is the SQL text. Because of the length of the text, it is recommended that the URL be submitted using a POST operation.

ssid:

This is the DB2 subsystem ID (like DB09, not the location, like DB09CW09).

Alternative Measurement API

The Alternative Measurement API allows the user to initiate a measurement from iStrobe. Unlike the Measurement API, the Alternate Measurement API allows the user to determine if the measurement parameters are correct in the iStrobe user interface before it is submitted.

Issue a post request:

```
http://<server>:<port>/istrobe/jsp/measurement/preMeasurementCheck.jsp?
jobname=<jobname>&system=<system>&profilename=<profilename>
```

jobname:

The name of the job to be measured.

system:

The LPAR where Strobe is installed.

profilename:

The name of the profile to view in iStrobe. It's assumed that the parameter values will be URL encoded as part of the request.

Appendix B.
iStrobe Plug-in for Topaz Workbench

The iStrobe plug-in to Topaz Workbench allows iStrobe to be launched from within the Topaz Workbench browswer. The plug-in can also be installed into a supported version of Eclipse or RDz instance. To install the iStrobe plug-in into Topaz Workbench, refer to the *Topaz Workbench Installation Guide* for installation instructions.