

Using IxLoad on Linux

Release 9.20

User Guide

Notices

Copyright Notice

© Keysight Technologies 2016–2021

No part of this document may be reproduced in any form or by any means (including electronic storage and retrieval or translation into a foreign language) without prior agreement and written consent from Keysight Technologies, Inc. as governed by United States and international copyright laws.

Warranty

The material contained in this document is provided “as is,” and is subject to being changed, without notice, in future editions. Further, to the maximum extent permitted by applicable law, Keysight disclaims all warranties, either express or implied, with regard to this manual and any information contained herein, including but not limited to the implied warranties of merchantability and fitness for a particular purpose. Keysight shall not be liable for errors or for incidental or consequential damages in connection with the furnishing, use, or performance of this document or of any information contained herein. Should Keysight and the user have a separate written agreement with warranty terms covering the material in this document that conflict with these terms, the warranty terms in the separate agreement shall control.

Technology Licenses

The hardware and/or software described in this document are furnished under a license and may be used or copied only in accordance with the terms of such license.

U.S. Government Rights

The Software is “commercial computer software,” as defined by Federal Acquisition Regulation (“FAR”) 2.101. Pursuant to FAR 12.212 and 27.405-3 and Department of Defense FAR Supplement (“DFARS”) 227.7202, the U.S. government acquires commercial computer software

under the same terms by which the software is customarily provided to the public. Accordingly, Keysight provides the Software to U.S. government customers under its standard commercial license, which is embodied in its End User License Agreement (EULA), a copy of which can be found at

<http://www.keysight.com/find/sweula>.

The license set forth in the EULA represents the exclusive authority by which the U.S. government may use, modify, distribute, or disclose the Software. The EULA and the license set forth therein, does not require or permit, among other things, that Keysight: (1) Furnish technical information related to commercial computer software or commercial computer software documentation that is not customarily provided to the public; or (2) Relinquish to, or otherwise provide, the government rights in excess of these rights customarily provided to the public to use, modify, reproduce, release, perform, display, or disclose commercial computer software or commercial computer software documentation. No additional government requirements beyond those set forth in the EULA shall apply, except to the extent that those terms, rights, or licenses are explicitly required from all providers of commercial computer software pursuant to the FAR and the DFARS and are set forth specifically in writing elsewhere in the EULA. Keysight shall be under no obligation to update, revise or otherwise modify the Software. With respect to any technical data as defined by FAR 2.101, pursuant to FAR 12.211 and 27.404.2 and DFARS 227.7102, the U.S. government acquires no greater than Limited Rights as defined in FAR 27.401 or DFAR 227.7103-5 (c), as applicable in any technical data. 52.227-14 (June 1987) or DFAR 252.227-7015 (b)(2) (November 1995), as applicable in any technical data.

Contacting Us

Keysight headquarters

1400 Fountaingrove Parkway
Santa Rosa, CA 95403-1738
www.ixiacom.com/contact/info

Support

Global Support	+1 818 595 2599	support@ixiacom.com
<i>Regional and local support contacts:</i>		
APAC Support	+91 80 4939 6410	support@ixiacom.com
Australia	+61-742434942	support@ixiacom.com
EMEA Support	+40 21 301 5699	support-emea@ixiacom.com
Greater China Region	+400 898 0598	support-china@ixiacom.com
Hong Kong	+852-30084465	support@ixiacom.com
India Office	+91 80 4939 6410	support-india@ixiacom.com
Japan Head Office	+81 3 5326 1980	support-japan@ixiacom.com
Korea Office	+82 2 3461 0095	support-korea@ixiacom.com
Singapore Office	+65-6215-7700	support@ixiacom.com
Taiwan (local toll-free number)	00801856991	support@ixiacom.com

CONTENTS

Contacting Us	3
Introduction	1
Part 1: Create the Test	3
Part 2: Deploy the image	4
Part 3: Connect to the VM and Upload the Test	5
Part 4: Run the Test	7
Using the Web UI	8
Authentication	9
Web UI Authentication	10
Web UI and IxLoadGateway	11
Ixia User Management	13
Authentication and the API Browser	16
Workflow	17
Connecting to the Web UI	18
Creating a new session	18
Ports	20
Timeline and Objectives	22
Running a test	23
Logs	24
Statistics	25
Reporter	28
Settings	31
File operations	32

My Account	32
Administration	33
Updates	34
Authentication	34
Maintenance	36
Server Certificate	37
Managing the Test Configuration and Files	39
Saving the test configuration	40
Loading a different test configuration	41
Downloading the test configuration	43
API Browser	43

Introduction

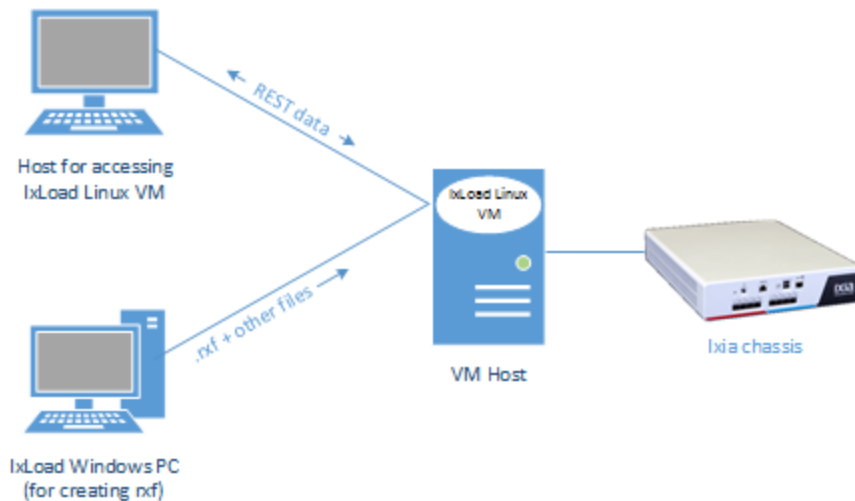
IxLoad can be used on Linux through the IxLoad REST API. Most, but not all, of the features supported from the REST API on Windows are also supported on Linux. See [IxLoad Features not supported from REST on Linux below](#) for details.

To use IxLoad on Linux, Ixia supplies VM images in two formats:

- OVA
- QCOW2

Both images have the following software pre-installed:

- IxLoad middleware (infrastructure software only, no UI support)
- IxLoad REST gateway service



Workflow

The workflow for using IxLoad on Linux is:

1. Create a test in the IxLoad GUI, and save the .rxf file.
2. Deploy the OVA or QCOW2 image and start the VM.
3. Connect to the IxLoad REST gateway service on the VM.
4. Upload the rxf and supporting files to the VM.
5. Use the REST API to issue commands to start and run the test.

This section describes this workflow.

IxLoad Features not supported from REST on Linux

- AppLibrary protocols
- Resource Manager

Introduction

- Profiles (e.g. Real files)
- Creating or editing voice scenarios
- Creating or editing Diameter scenarios (except for importing/exporting XML files, which is supported)

Part 1: Create the Test

1. On a Windows PC with the IxLoad client installed, create the test that you want to run.
2. Save the test repository (.rxf or .crf) file, along with any supporting files (sample audio files, traffic capture files, etc.) that the test requires in a location that can be accessed from the VM.

Part 2: Deploy the image

Note: Beginning with the 9.20 release, the IxLoad Linux image contains an Ubuntu 20.04 server installation, which creates a VM that has a command line interface only. Prior to 9.20, the IxLoad Linux image deployed an Ubuntu 14.04 desktop OS that included a GUI.

Deploy the OVA or QCOW 2 image:

OVA

1. Use the hypervisor of your choice to deploy the OVA, and start the VM.
2. Use the hypervisor's console to find the IP address of the VM.

QCOW2

The QCOW2 image is embedded in a shell (.sh) script. This image is pre-configured with 4 vCPUs and 8 GB RAM. The name of the script identifies the image's IxLoad release. For example, for the 8.50 EA release, the script name is `IxLoad-8.50.0.465.sh`.

Prerequisites

- To import the QCOW2 image, the IxLoad .sh file must be executable. Use the following command to change the permissions:
`chmod +777 IxLoad-{version}.sh`
- The following tools must be installed on the Linux system where you are extracting the QCOW2 image from the .sh file:
 - `virt-install`
 - `libvirt`

Deploying the image

Based on the platform type you are using, use one of the following procedures to deploy the image:

KVM	OpenStack
<p>To import the QCOW2 image on KVM: Execute the <code>IxLoad-<version>.sh</code> script. After you accept the EULA terms, the script will extract and deploy the QCOW2 image.</p>	<p>To import the QCOW2 image on OpenStack:</p> <ol style="list-style-type: none">1. In any Linux environment, use the following command to accept the EULA terms and then extract the QCOW2 image: <code>run "IxLoad-{version}.sh -z"</code>2. Copy and import the QCOW2 image into the OpenStack environment.3. OpenStack ignores the pre-configured CPU and RAM values. Therefore, you should manually specify at least 4 vCPUs and 8 GB RAM.

Part 3: Connect to the VM and Upload the Test

- Using a browser extension or application (such as PuTTY), establish an SCP connection to the VM. When you connect to the VM, the default path is automatically set to a shared folder intended for transferring test files to and from the VM.
- Upload the .rxf file and any supporting files to the VM. The maximum size of a file you can upload is 1GB.

There are two ways to upload files:

- Through a script
- Through a remote file browser

Script method

To upload files from a script, the IxLoad REST API includes the `uploadFile` operation. You must create a script that includes `uploadFile`. You can use any scripting language that has libraries capable of HTTP file upload requests (such as `httplib` on Python). You cannot use a GUI REST client to upload files.

IxLoad includes a sample Python REST script, `IxLoadUtils.py`, that demonstrates the use of `uploadFile`. `IxLoadUtils.py` and other sample REST scripts are stored on the IxLoad client installation path, in a subfolder named `RestScripts`.

To upload a file, the script executes a POST request on the following URL:

```
http://127.0.0.1:8080/api/v0/resources
```

The `uploadFile` operation in the script takes three parameters:

<code>filename</code>	represents the path of the local file to be uploaded to remote location
<code>uploadPath</code>	<p>represents the path relative to the shared folder (<code>/mnt/ixload-share</code>) on the Linux VM.</p> <p>For example, if the upload path is:</p> <pre>uploads/SimpleRun.rxf</pre> <p>the file will be uploaded to:</p> <pre>/mnt/ixload-share/uploads/SimpleRun.rxf</pre>
<code>overwrite</code>	determines whether or not an existing file on the remote location with the same name as the uploaded file is overwritten. The default value is <code>true</code> .

The image below shows an example of a script that uses the uploadFile operation.

```
import os
import requests

url = 'http://127.0.0.1:8080/api/v0/resources/'
headers = {'Content-Type': 'multipart/form-data'}

def uploadFile(fileName, uploadPath, overwrite=True):
    params = {'overwrite': overwrite, 'uploadPath': uploadPath}

    print 'Uploading...'
    try:
        with open(fileName, 'rb') as f:
            resp = requests.post(url, data=f, params=params, headers=headers)
    except requests.exceptions.ConnectionError as e:
        print (
            'Upload file failed. Received connection error. One common cause for this error is the size of the file to be uploaded.'
            'The web server sets a limit of 1GB for the uploaded file size. Received the following error: %s' % str(e)
        )
    except IOError as e:
        print 'Upload file failed. Received IO error: %s' % str(e)
    except Exception:
        print 'Upload file failed. Received the following error: %s' % str(e)
    else:
        print 'Upload file finished.'
        print 'Response status code %s' % resp.status_code
        print 'Response text %s' % resp.text

fileNamePath = 'SimpleRun.rxf'
relativeUploadPath = 'uploads/' + os.path.split(fileNamePath)[1]
overwrite = True

uploadFile(fileNamePath, relativeUploadPath, overwrite)
```

For full information on uploadFile and the other IxLoad REST commands, see the *IxLoad REST API Guide* (available from the Ixia website: <https://support.ixiacom.com/user-guide>).

Remote file browser method

You can upload files using a remote file browser. To use this method, connect to /mnt/ixload-share and pass the following credentials:

Username:	ixload
Password:	ixia123

Part 4: Run the Test

1. Start the REST client you want to use for the test.
2. Issue the REST commands to start and run the test. For information on the REST commands, see the *IxLoad REST API Guide* (available from the Ixia website: <https://support.ixiacom.com/user-guide>).

When used on Windows, REST API calls that operate on files (such as the .rxf file) require the full path to the file. The same is true on Linux -- you must use the full path to the file. The file path on the VM always begins with /mnt/ixload-share. Uploading programatically (i.e., from a script) or from a remote file browser must be done from this location.

For example, the `loadTest` operation loads the rxf file.

On Windows, the path might be:

```
{"fullPath": "C:\\path\\to\\files\\myTest.rxf"}
```

On Linux, the path might be:

```
{"fullPath": "/mnt/ixload-share/myTest.rxf"}
```

If the .rxf file includes references to any other files, make sure these files are also uploaded in the shared location on the VM. If the files referenced from the .rxf have absolute paths, you must modify them (for example, by doing a PATCH request) to point to their new location on /mnt/ixload-share.

Using the Web UI

The IxLoad Linux OVA and qcow2 images include the IxLoad Web UI, an IxLoad GUI that you access from a web browser.

The Web UI uses the IxLoad REST API for all of its functions, meaning that all IxLoad Web UI sessions are IxLoad REST sessions.

The Windows version of IxLoad does not include the Web UI.

Supported features

You can perform the following functions in the IxLoad Web UI:

- Launch and connect to an IxLoad Web session
- Load (and upload) configuration files in the IxLoad Web session
- Add new chassis to the configuration
- Remap ports
- Modify L47 activity objectives and timeline options
- Enable Analyzer on ports
- Launch the IxLoad API Browser (which allows you to view and change the IxLoad traffic configuration)
- View IxLoad logs in real time
- Run a test
- View real time statistics
- Download port capture files locally
- Download a report

The scenario editor is not available in the Web UI, so there is no visual representation of the NetTraffics and L2-3 and L4-7 activities. Instead, you can use the API Browser in the Web UI to view and change these parameters.

Authentication

In the IxLoad Web UI, authentication depends on the interaction between three separate components:

- The authentication controls in the Web UI
- IxLoadGateway
- Ixia User Management

The following sections describe how each of these components affects authentication in the Web UI.

Web UI Authentication

The IxLoad Web UI can use either of two authentication modes:

- Local
- Ixia User Management

The controls configuring authentication in the Web UI are on the [Authentication](#) page.

Local authentication

Under Local authentication, only one username can be used: the pre-configured `admin` user. Every session that is open in the Web UI is open under the `admin` user's credentials. Every user that connects to the IxLoad Linux VM's IP address can see all the currently open sessions because they are all logged on as the `admin` user.

Local authentication is the default mode, and is automatically selected when a new IxLoad Linux VM is deployed.

Ixia User Management authentication

Under Ixia User Management authentication, users must log into the IxLoad Web UI using their Ixia User Management usernames and passwords. Each user can only see the IxLoad Web UI sessions they have opened.

Under Ixia User Management authentication, the default `admin` username cannot be used to create IxLoad Web UI sessions. It can only be used to log on, enable or disable authentication, and manage sessions (including ending other users' sessions).

Web UI and IxLoadGateway

The IxLoadGateway service controls REST sessions' access to the IxLoad application. The IxLoad Web UI works with the IxLoadGateway service and Ixia User Management to manage authentication.

If you change the authentication mode in the IxWeb UI, that change is also automatically made to IxLoadGateway.

IxLoadGateway can run in either of two modes:

- No authentication
- Authentication through Ixia User Management

No authentication

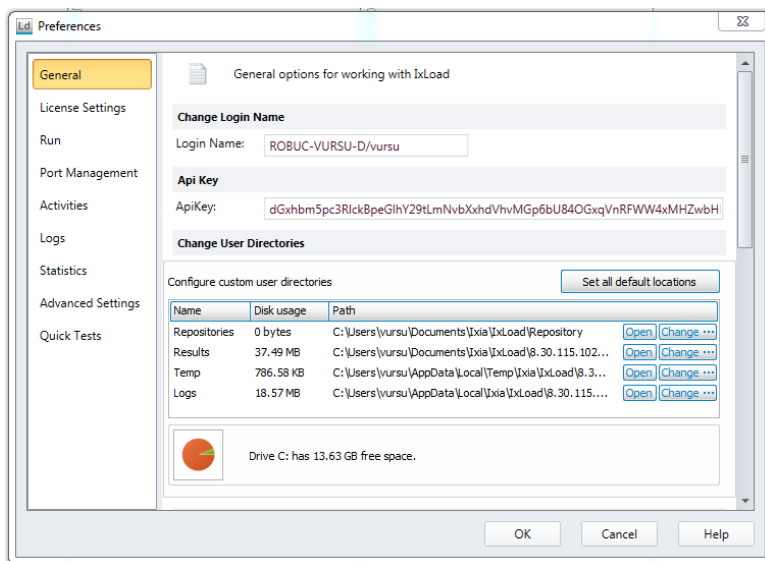
In No authentication mode:

- Any user can make REST requests to create a new IxLoad REST API session.
- Any user can view, modify, or delete any REST API session.

Authentication through Ixia User Management

With authentication enabled in Ixia User Management, you must provide an API Key when making REST API calls.

You can retrieve the API Key from the Ixia User Management server or from the IxLoad UI, after logging in the UI.



The API Key must be provided in the `x-api-key` header of the REST API request, as in the following image:

Using the Web UI

POST	https://localhost:8443/api/v0/sessions			
Authorization	Headers (2)	Body	Pre-request Script	Tests
Key	Value			
<input checked="" type="checkbox"/> Content-Type	application/json			
<input checked="" type="checkbox"/> x-api-key	dnRyYwIzdGFwb3Blc2N1QGI4aWFjb20uY29tfHR6T3R3WE0wdU9aT21QUndvNEkwdk2U3QwOD0=			

After creating a REST API session in authenticated mode, only the user that created it (that is, only requests that provide the correct api key) can browse that session data model.

All requests to the URLs `/sessions` and `/sessions/X` are allowed with or without an `api-key`. URLs starting with `/sessions/X/ixload` require an `api-key`.

Enabling authentication in IxLoadGateway

On Windows, IxLoadGateway authentication is enabled from the IxLoad installer. Run (or rerun) the installer and select the option for authentication through IxLoadGateway.

On Linux, authentication is enabled or disabled by running the following commands:

Enable authentication	<code>bash /opt/ixia/ixloadgateway/configRestAuth.sh --um-address x.x.x.x</code>
Disable authentication	<code>bash /opt/ixia/ixloadgateway/configRestAuth.sh --disable-auth</code>

Ixia User Management

Ixia User Management provides authentication to a number of Ixia applications.

To use User Management authentication in the IxLoad Web UI, the Web UI host must have access to a User Management server.

In User Management, users belong to groups, and groups have permissions. The group permissions determine what the users in the group can or cannot do.

- To log into the Web UI, a user must belong to a group that has either Read-only or Full Access permission in User Management.
- To be an administrator in the Web UI, a user must belong to the User Management group in the Web UI as the Admin group (see [Authentication on page 34](#)).

If you want to use User Management to manage access to the Web UI, you must:

1. Have access to an existing User Management server, or deploy a new one.
2. Configure the Web UI to use the User Management server for authentication.

This section describes how to deploy and configure a User Management server for use with the Web UI.

To configure Web UI authentication, see [Authentication on page 34](#)

Deploying Ixia User Management and logging in

Deploying Ixia User Management and logging in

The UM server is supplied as an OVA VM image, and is available from the Ixia software download page. The version required for IxLoad Web UI integration is 1.0.0.55 or later.

To deploy Ixia User Management and log in:

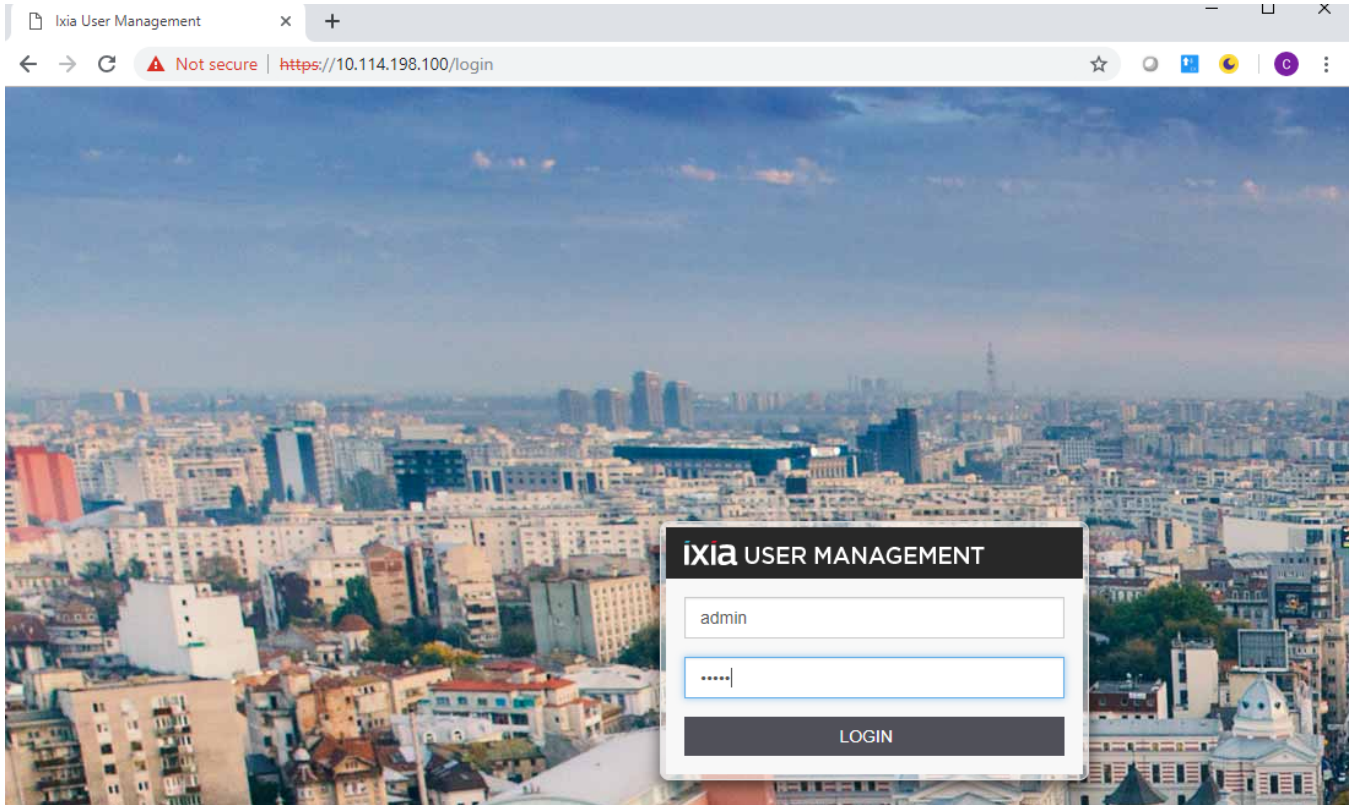
1. Deploy the User Management OVA.
2. Start the VM.
3. Open the console window, and login with the following credentials:

Username:	ixia
Password:	bJXINge7eF82

4. Use `ifconfig` to retrieve the IP address of the User Management server.
5. Open a web browser, and login to the UM server with the following credentials:

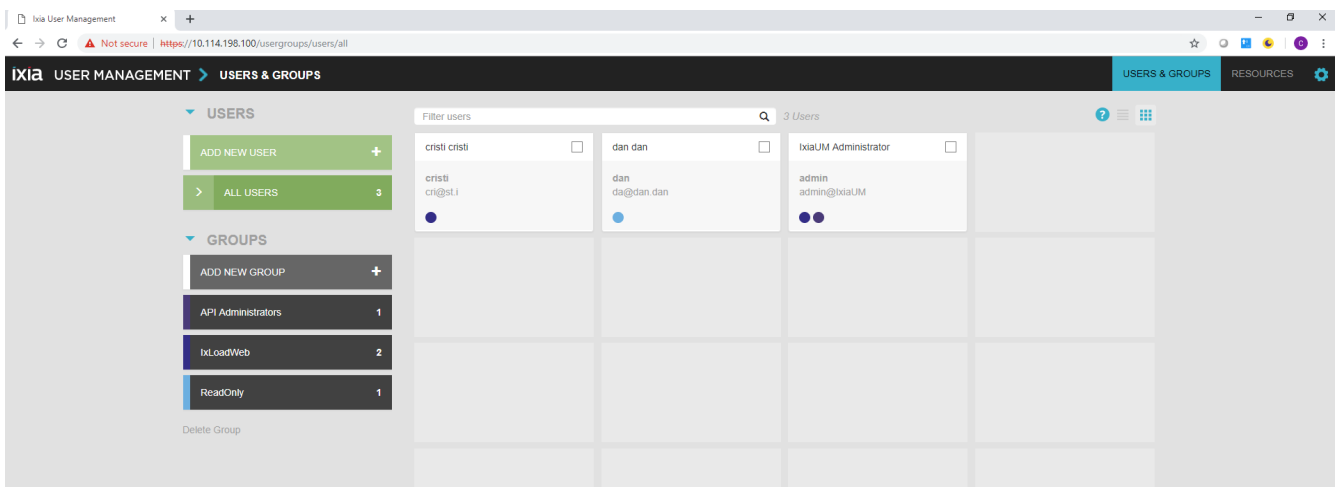
Username:	admin
Password:	admin

Using the Web UI



Configuring User Management for IxLoad Web UI authentication

After you log in to the Ixia UM server, the Users & Groups page displays.



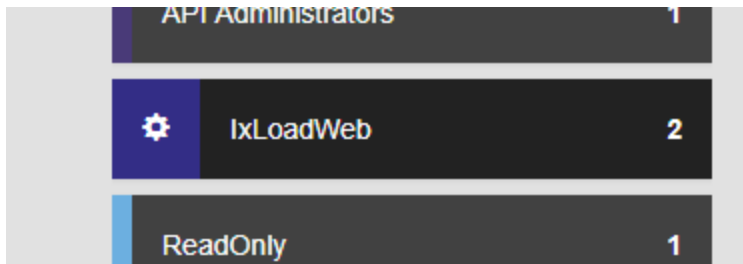
In the center of page, the users configured on the UM server are listed.

On the left side under Groups, the groups configured on the UM server are listed.

Every group has one or more users in it, and a set of permissions assigned to it, which apply to the users in the group.

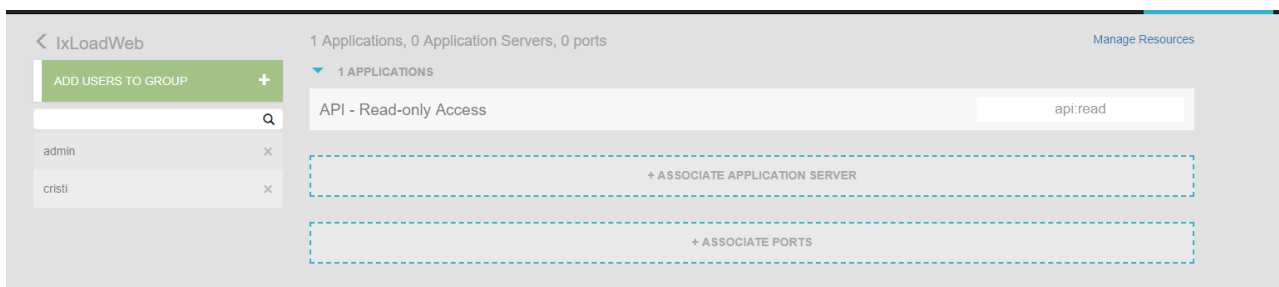
To configure User Management for IxLoad Web UI authentication:

1. Select the group that you want to use for authentication in the IxLoad Web UI.
If the group does not exist, create it.
2. Select the Settings icon to the left of the group name.



The group's permissions display.

3. Ensure that the group has the `API-Read` permission, which allows the group's users to log in to the IxLoad Web UI.

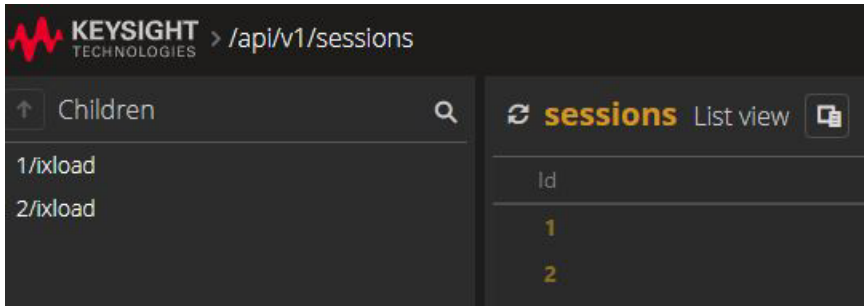


4. If necessary, add users to the group.
If the user that you want to allow to access the IxLoad Web UI does not exist, create it.
5. When you are finished, log out of Ixia User Management.

Authentication and the API Browser

You can use the API Browser to view the current REST API (and Web UI) sessions that are open on the IxLoad Linux VM.

- If the Web UI uses Local authentication, the API Browser can display any open session that is open on the VM.
- If the Web UI uses Ixia User Management authentication, all the sessions open on the VM appear in the left side of the API Browser, but you can only view the sessions open under your username.



Workflow


The workflow for running a test in the Web UI is:

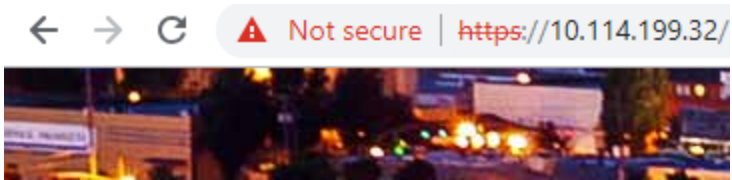
1. Start the IxLoad VM, and connect to the Web UI.
2. Select a test configuration, then create a test session for it.
3. Select the ports for the test.
4. Start the test, and view the statistics.

Connecting to the Web UI

To connect to the Web UI:

1. Start the IxLoad VM.
2. In a web browser's URL field, enter the IxLoad VM's IP address.

 **Note:** The Web UI listens on the default HTTPS port (443).



When you connect to the Web UI, IxLoad displays the Sign In window.



3. Enter the following credentials:

Username	admin
Password	admin

then click Sign In.

If this is the first time you have logged into the Web UI, it prompts you to change the password.

The default authentication mode is Local authentication. To change the authentication mode, select the Administration option on the main dashboard. For more information about authentication, see [Authentication on page 9](#).

Creating a new session

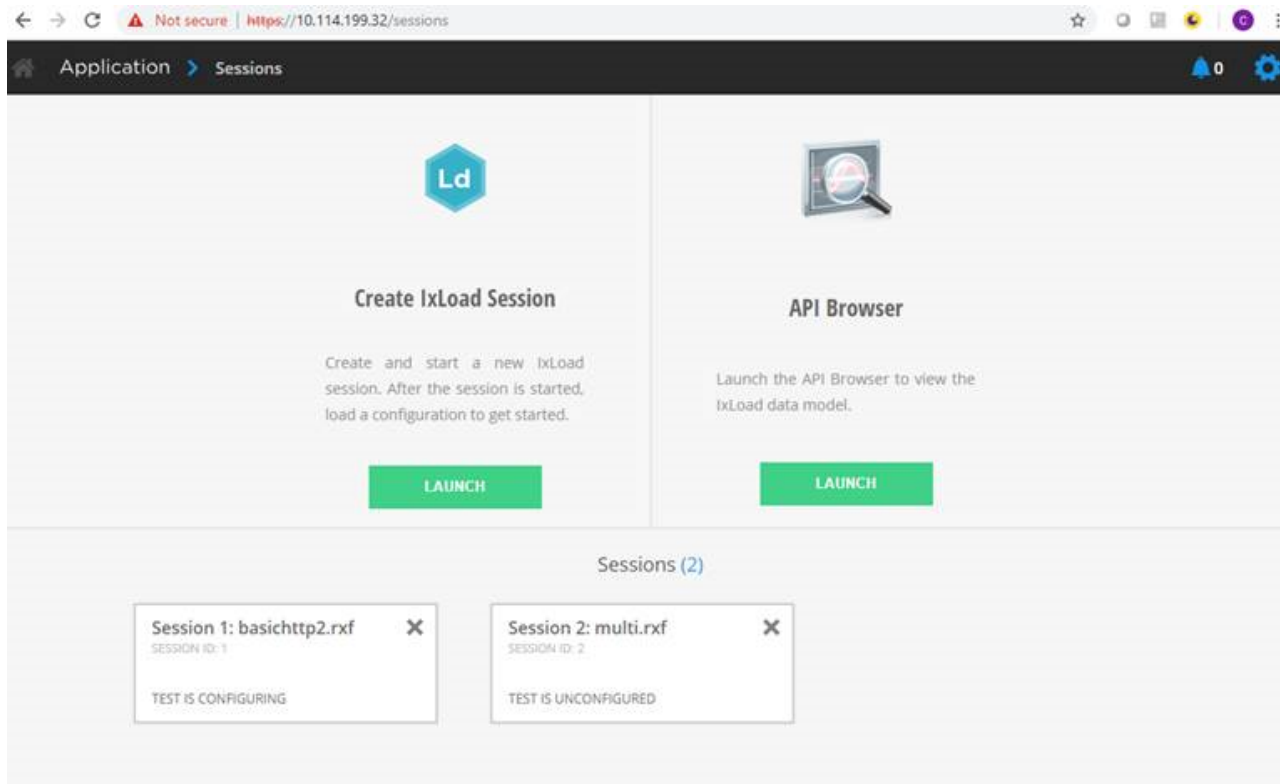
After you login, the Sessions window displays.

The Sessions window displays the sessions that are currently in progress, and allows you start a new session.

For sessions in progress, a card displays their status, and the name of the configuration file they are using. You can click on a session's card and display its configuration page, which allows you to view the currently loaded .configuration file or select a new one.

To create a new session:

1. Click Launch.



2. Specify the .test configuration file to use.

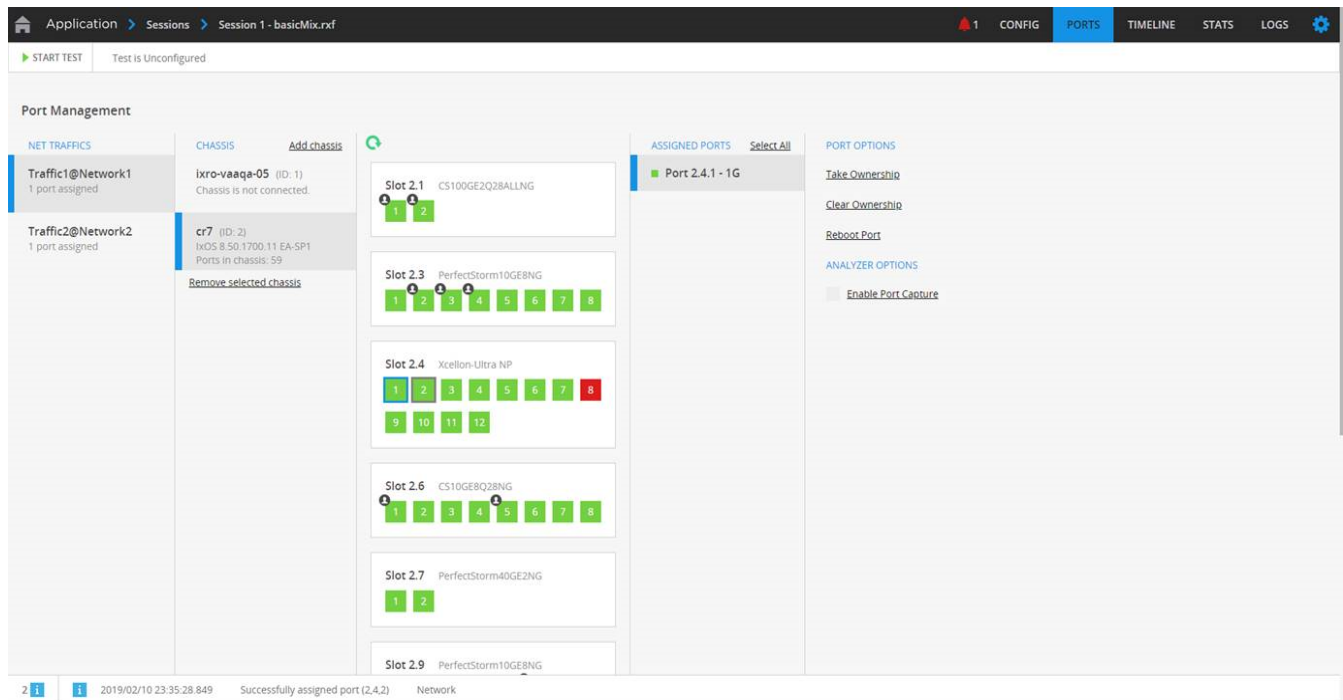
Choose one:

To...	Do this:
Load a recently used file (a file that is already on the Linux VM).	Choose a file from the list, then select OK.
Upload an .rxf or .crf file from the local machine to the Linux VM.	<ol style="list-style-type: none"> Select Browse. Choose an .rxf or .crf file, then select OK. <p>IxLoad uploads the file from the local machine to the Linux VM.</p> <p>If you selected a .crf file, IxLoad uploads it to the VM, and then extracts it in .rxf format.</p>
Manually enter the path to a file on the VM.	<ol style="list-style-type: none"> Select Server path.

To...	Do this:
	b. In the field, enter the absolute path of a configuration file (.rxf or .crf) that already exists on the Linux VM. c. Select OK.

Ports

The Ports option in the navigation bar displays the Port Management page, which allows you to view and manage the test ports.



NetTraffics

The NetTraffics column lists the NetTraffics currently being used in the test, and the number of ports assigned to each NetTraffic.

Chassis

The Chassis column contains a list of chassis, along with their name, ID, number of ports, and the IxOS version.

Adding a Chassis:	To add a chassis, click Add Chassis.
Removing a Chassis:	To remove a chassis, select the chassis, then click Remove Selected Chassis.

Cards and Ports

The Cards and Ports column displays all the cards contained in the selected chassis. For each card, Web UI displays its card ID, the card type and all the ports.

Ports display as either green or red:

Green	Port is link up
Red	Port is link down

If a port is owned by a user, an icon displays in the upper left corner. To view the owner's name, hover over the port:



To refresh the chassis display, click the Refresh icon at the top-left of the column.

Assigned Ports

The Assigned Ports column displays the ports assigned to the selected NetTraffic.

The Port Options column contains the commands you use to manage the ports on the chassis:

Take Ownership	Select the ports you want to take ownership of, then click Take Ownership.
Clear Ownership	Select the ports you want to release ownership of, then click Clear Ownership.
Reboot Port	Select the ports you want to reboot, then click Reboot Ports.

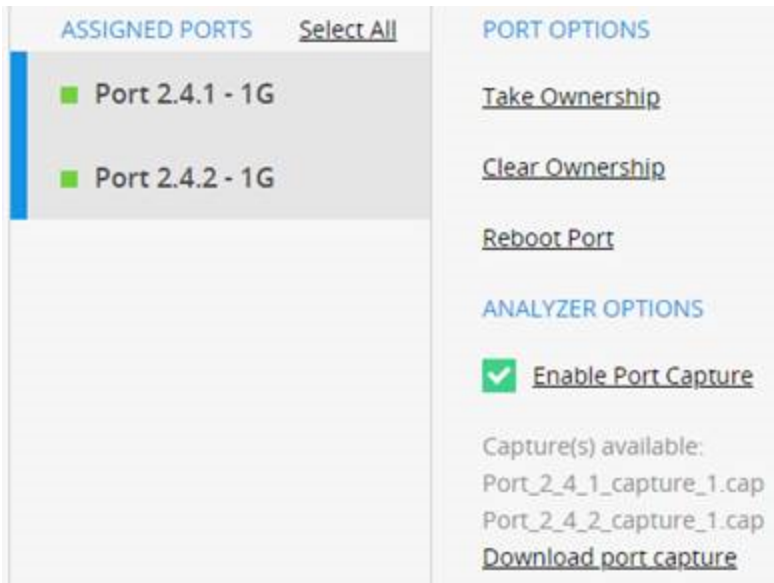
Analyzer Options

The Analyzer Options control the capture of traffic on the ports.

If you select Enable Port Capture, traffic to and from all the selected the ports is captured during the test and saved on the VM.

Using the Web UI

After the test has been run and the captures have been saved, a button displays below the Enable Port Capture checkbox that enables you to download the port capture files from the VM.



The screenshot shows a web interface with two main sections: "ASSIGNED PORTS" and "PORT OPTIONS".

- ASSIGNED PORTS:** Contains two entries: "Port 2.4.1 - 1G" and "Port 2.4.2 - 1G", each with a green square icon.
- PORT OPTIONS:** Contains three links: "Take Ownership", "Clear Ownership", and "Reboot Port".
- ANALYZER OPTIONS:** Contains a checked checkbox labeled "Enable Port Capture".

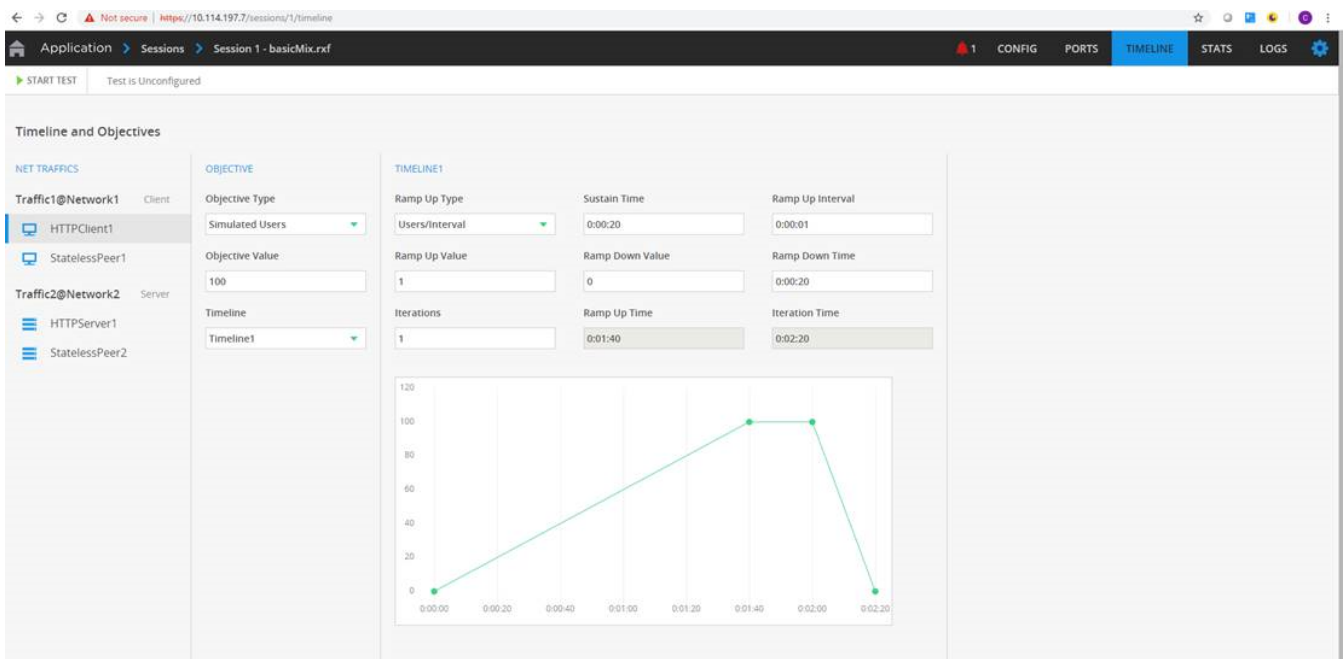
Below the "ANALYZER OPTIONS" section, there is a list of capture files:

- Capture(s) available:
- Port_2_4_1_capture_1.cap
- Port_2_4_2_capture_1.cap

A link "Download port capture" is located at the bottom of this list.

Timeline and Objectives

The Timeline and Objectives option in the navigation bar enables you to set the test objective and configure the test timing.



The screenshot shows the "Timeline and Objectives" configuration page in a web browser. The browser address bar shows "https://10.114.197.7/sessions/1/timeline". The navigation bar includes "Application", "Sessions", "Session 1 - basicMix.rxf", "CONFIG", "PORTS", "TIMELINE", "STATS", and "LOGS".

The main content area is titled "Timeline and Objectives" and is divided into three sections:

- NET TRAFFICS:** Lists "Traffic1@Network1" (Client) and "Traffic2@Network2" (Server). Under "Traffic1@Network1", there are "HTTPClient1" and "StatelessPeer1". Under "Traffic2@Network2", there are "HTTPServer1" and "StatelessPeer2".
- OBJECTIVE:** Contains a dropdown for "Objective Type" (set to "Simulated Users"), an input for "Objective Value" (set to "100"), and a dropdown for "Timeline" (set to "Timeline1").
- TIMELINE1:** Contains several configuration fields:
 - Ramp Up Type: "Users/Interval"
 - Sustain Time: "0:00:20"
 - Ramp Up Interval: "0:00:01"
 - Ramp Up Value: "1"
 - Ramp Down Value: "0"
 - Ramp Down Time: "0:00:20"
 - Iterations: "1"
 - Ramp Up Time: "0:01:40"
 - Iteration Time: "0:02:20"

At the bottom of the "TIMELINE1" section, there is a line graph showing the test timing. The x-axis represents time from 0:00:00 to 0:02:20. The y-axis represents the number of users, ranging from 0 to 120. The graph shows a ramp-up phase from 0:00:00 to 0:01:40, where the number of users increases from 0 to 100. It then shows a sustain phase from 0:01:40 to 0:02:00, where the number of users remains constant at 100. Finally, it shows a ramp-down phase from 0:02:00 to 0:02:20, where the number of users decreases from 100 to 0.

NetTraffics

The NetTraffics column displays the NetTraffics currently being used in the test and the L4-7 activities in each NetTraffic.


Objective

The Objective column contains the Objective Type, Objective Value and Timeline associated with the activity selected in the NetTraffics column. To change objective type, select a new objective from the list.

Timeline

The Timeline column displays the parameters that define the timeline of the selected activity. The chart displays how the objective value will be applied based on the timeline options.

To change the timeline, select a new timeline from the list, or select New Timeline to create a new timeline.

 **Note:** In the WebUI, you can only select or edit basic timelines. If you need to select or edit an advanced timeline, you can use the REST API.

Running a test

You use the Start and Stop buttons at the top of the page to control a test:

To run a test, click Start Test.

To stop a test, click Stop Test.

The status bar next to the Start/Stop buttons display the test's current status, and when the test starts, its progress. Test status can be :

Unconfigured	Test is not running.
Configuring	Test configuration is being loaded onto ports.
Starting Run	Test starting to send traffic.
Cleaning	Test is removing configuration from the ports.

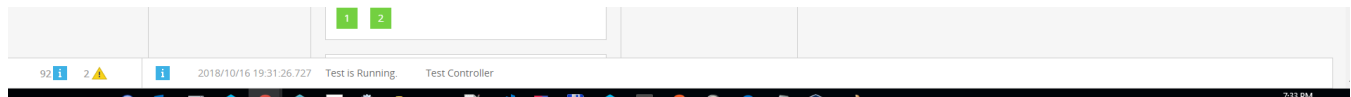


When the test enters the Running stage, a progress bar and the elapsed time displays.



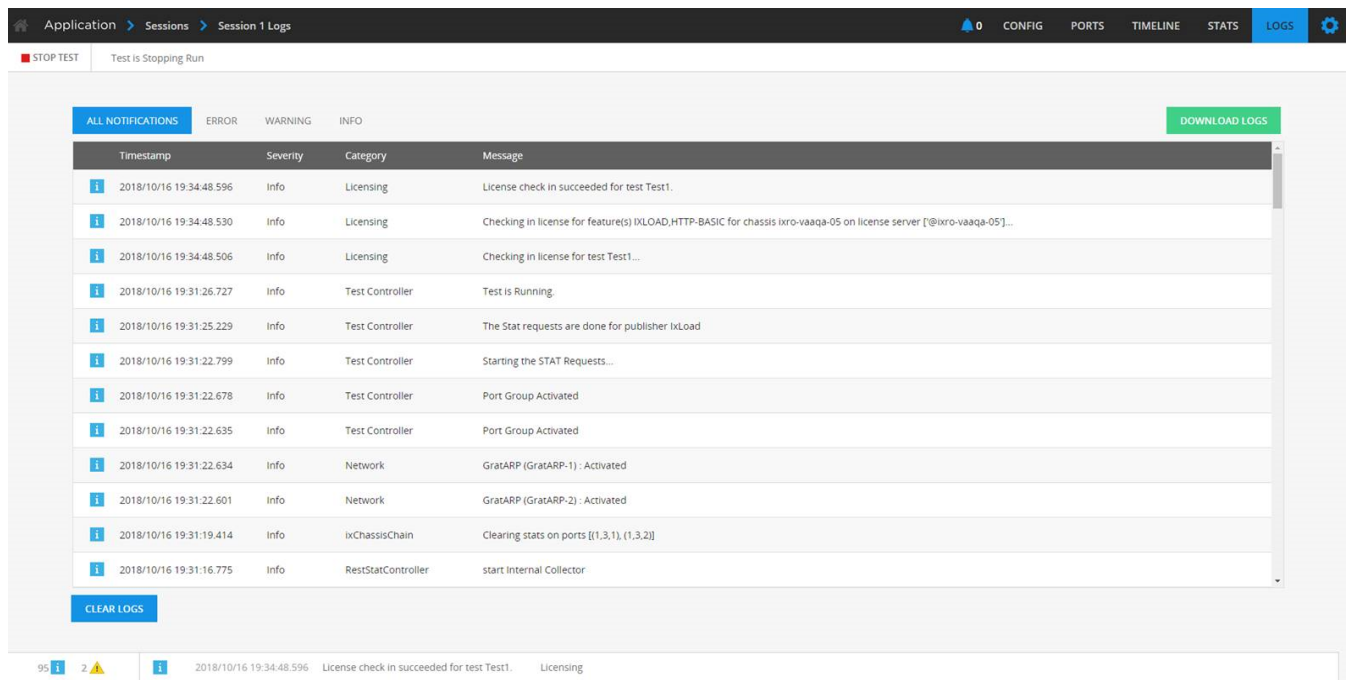
Logs

The log area at the bottom of the Web UI pages displays a running count of the number of Info/Warning/Error messages, and the text of the most recent message.



If you click on the log area, the Logs page displays.

The Logs page contains a table that contains all of the logged event messages.



You can sort the messages by column, and filter them by message type:

Sorting log messages

To sort the messages, click on the column headings.

Timestamp	Date and time event occurred
Severity	Seriousness of event: (Info/Warning/Error)
Category	Component that message applies to
Message	Text of message

Filtering log messages

To filter the messages, click the Severity of the messages that you want to filter for.

Downloading log files

To download the log to the local system, click Download Logs. Log files are in .csv format.

Clearing the log

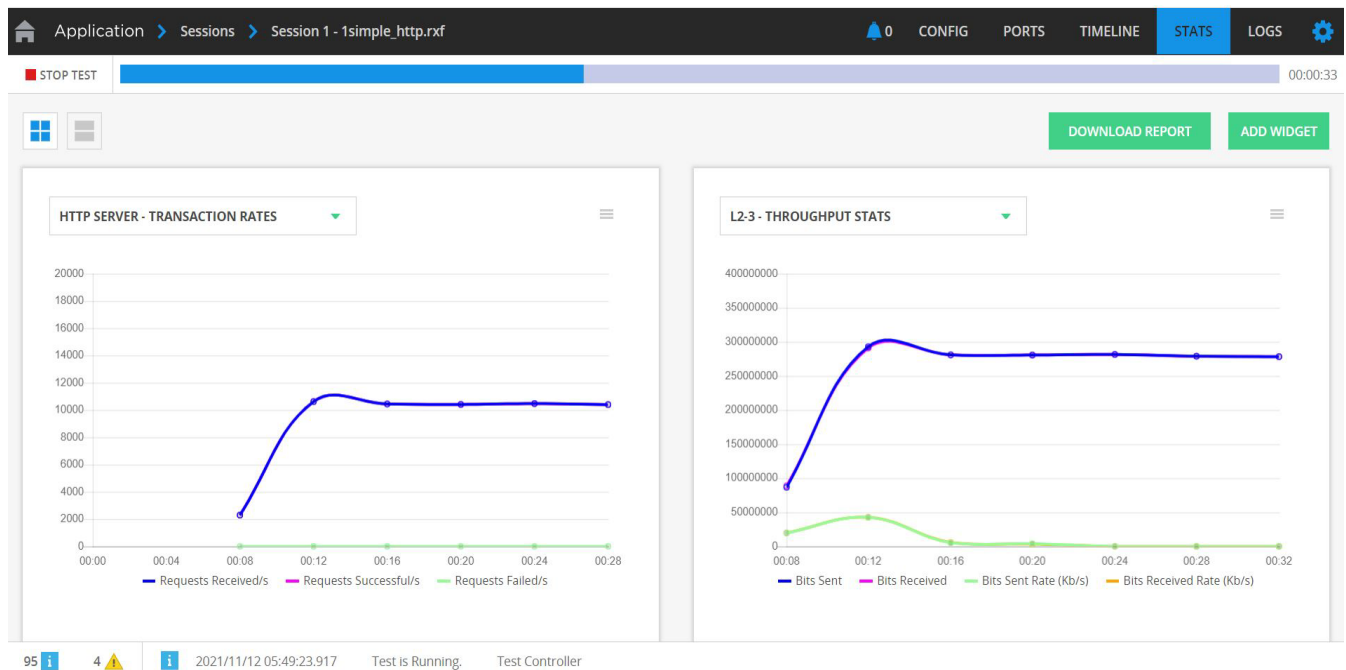
To remove all the entries from the log, click Clear Logs.

Statistics

The Statistics page contains two charts that are populated with statistics in real time as a test runs.

The chart on the left displays per-protocol statistics.

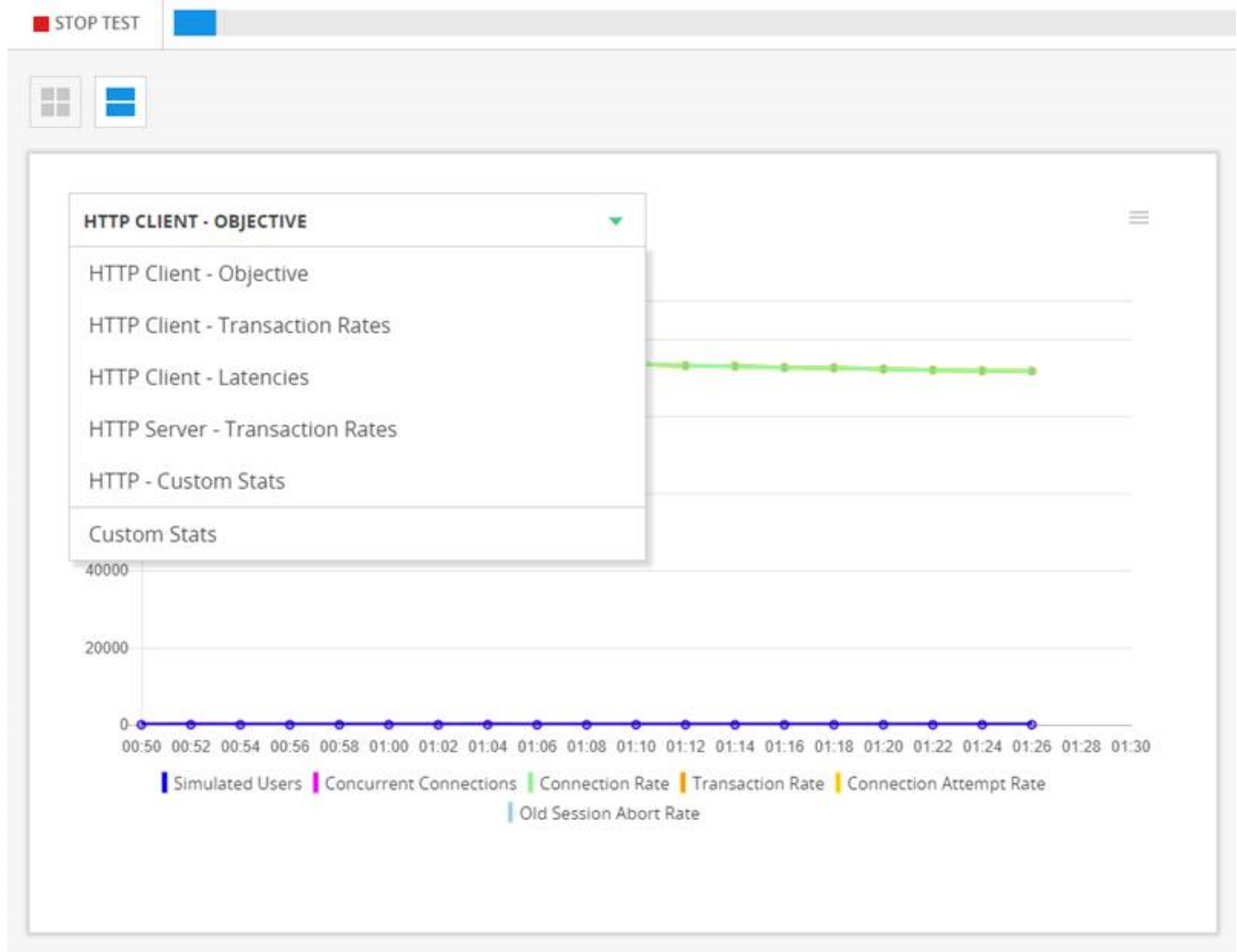
The chart on the right displays IxServer statistics.



To display a different view of statistics:

1. Click the drop-down button.
2. Select a new view from the list.

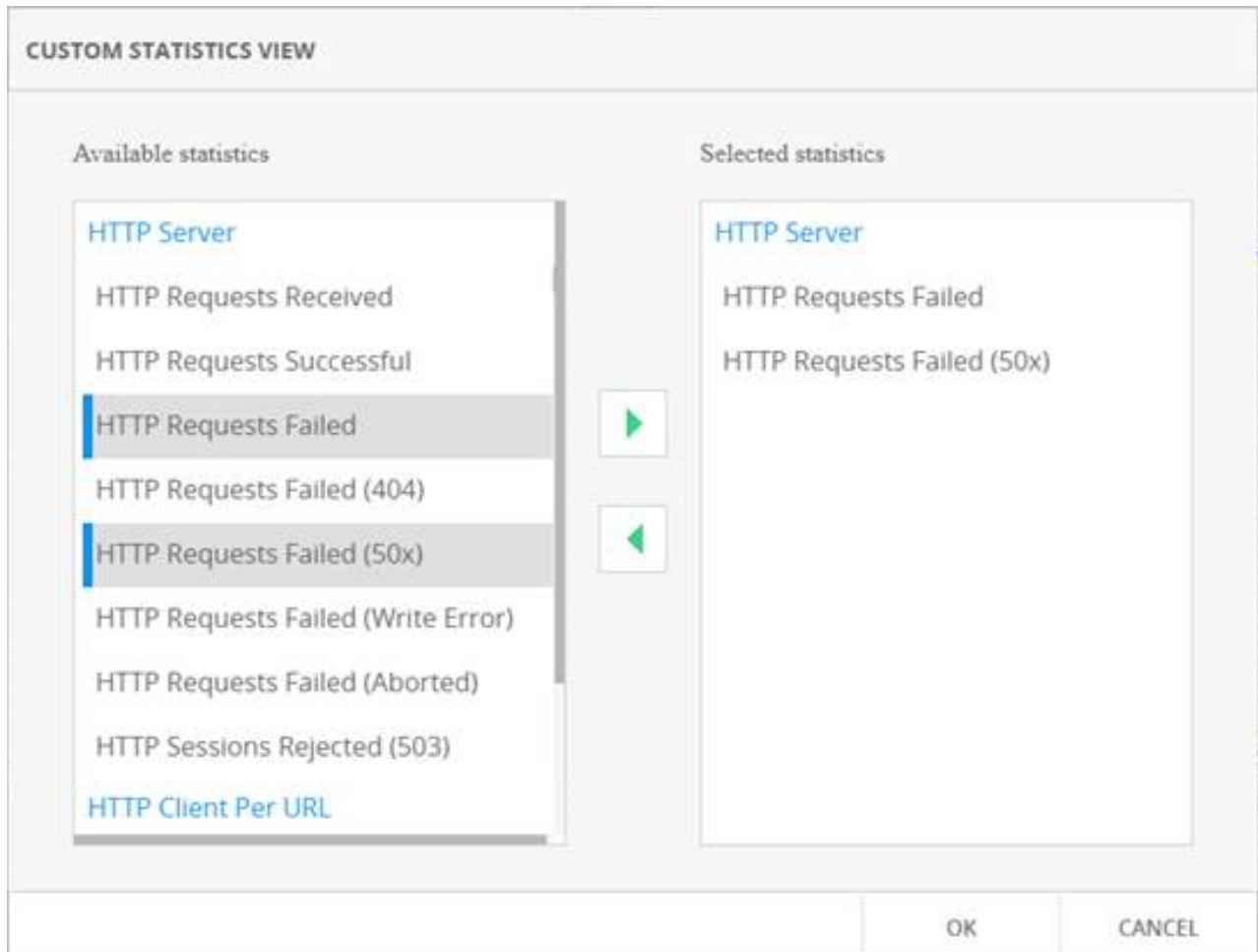
You can select from a set of predefined views, or you can select a custom view.



Custom views

To display a custom view:

1. Select Custom Stats from the drop down.

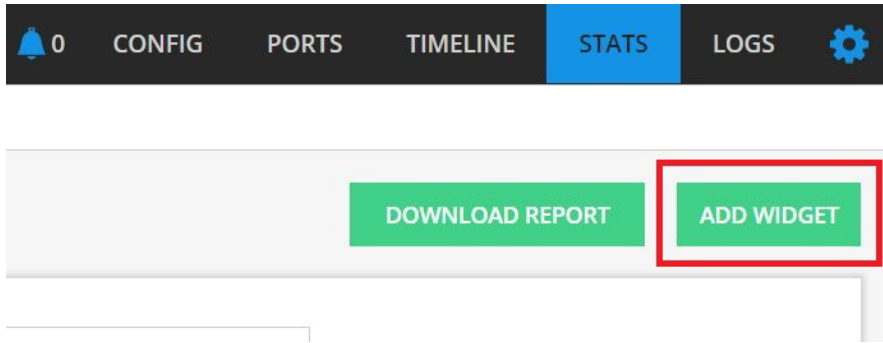


The Custom Statistics View window displays.

2. Select a statistic in the Available Statistics list, then click the > button to move it into the Selected Statistics list.
To remove a statistic from a custom view, select it in the Selected Statistics list, then click the < button to move it back to the Available Statistics list.

Adding Widgets

You can add widgets to the Statistics view that enable you to analyze the statistics from a test.



To add a widget:

1. On the Statistics view, select Add Widget.
2. Choose the widget you want to add, then click OK.

Reporter

The REST API includes an API that can generate a PDF report after a test run. Report generation does not require installing any additional software.

You can generate reports for the following protocols:

- HTTP
- FTP
- IPSec
- DNS
- Voice

To generate reports, you must set the following preferences to `True` before you run a test:

- `enableL23RestStatViews`
- `enableRestStatViewsCsvLogging`
- `saveDataModelSnapshot`

You can set these from the preferences URL:

`https://127.0.0.1:8443/api/v0/sessions/{sessionId}/ixload/preferences`

or from Application Settings in the WebUI :

APPLICATION SETTINGS

File upload location:

Allow IP Overlapping

Allow Route Conflicts

Logger Size:

Overload Protection:

Customize IxLoad VE license count:

CSV Throughput Units:

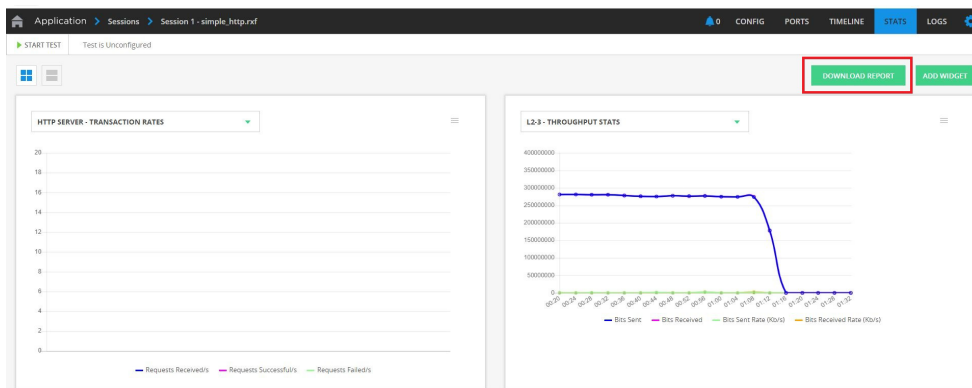
Enable L23 Rest Stat Views

Enable Rest Stat Views CSV Logging

Save Data Model Snapshot

You can only generate a report immediately after a test has run in the IxLoad REST session.

In the WebUI, the option to download a report is on the Stats tab and is only enabled after the test stops and enters the Unconfigured state. When you click Download, the system generates the report, places it in the results folder on the Linux machine, and then downloads it to the downloads folder of your browser. If you refresh the page after the test stops, the Download option is not available.

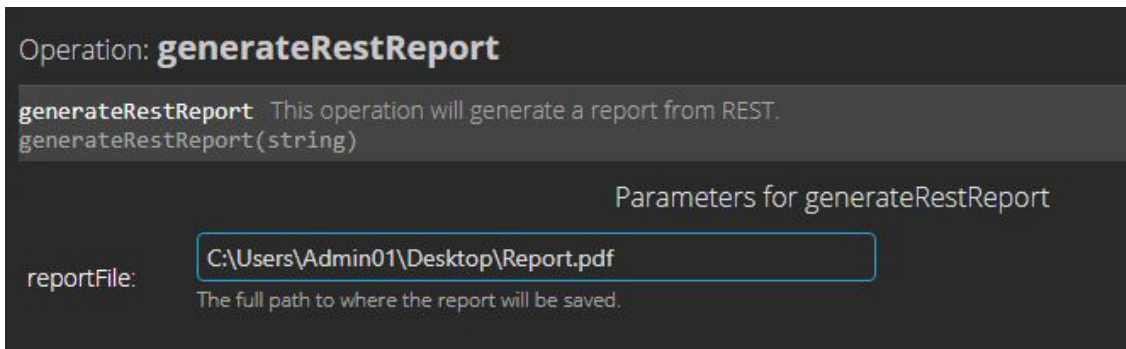
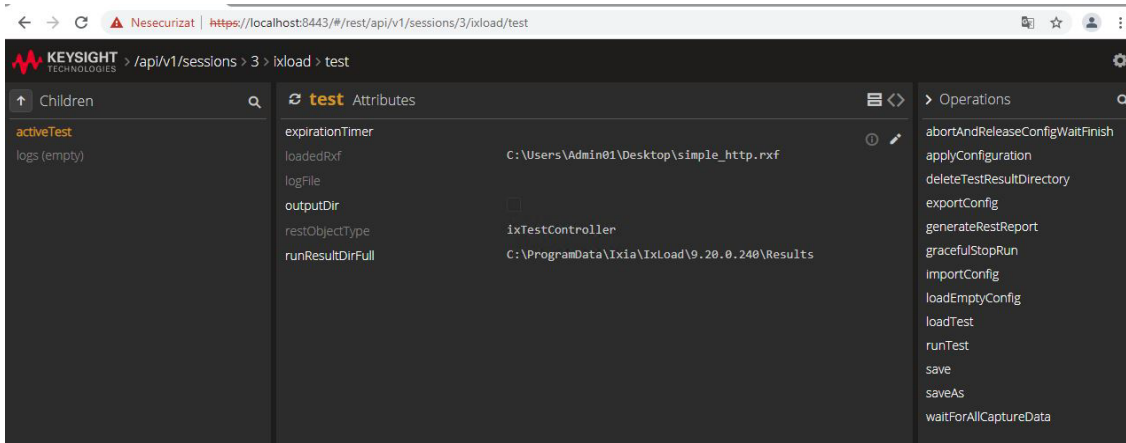


A report can be generated only after a test has run in the IxLoad REST session.

From the API Browser, a `generateRestReport` operation needs the full path of the `reportFile` parameter, including the PDF file name. In an IxLoad Linux deployment, reports must be generated under the regular shared folder location: `/mnt/ixload-share`.

Using the Web UI

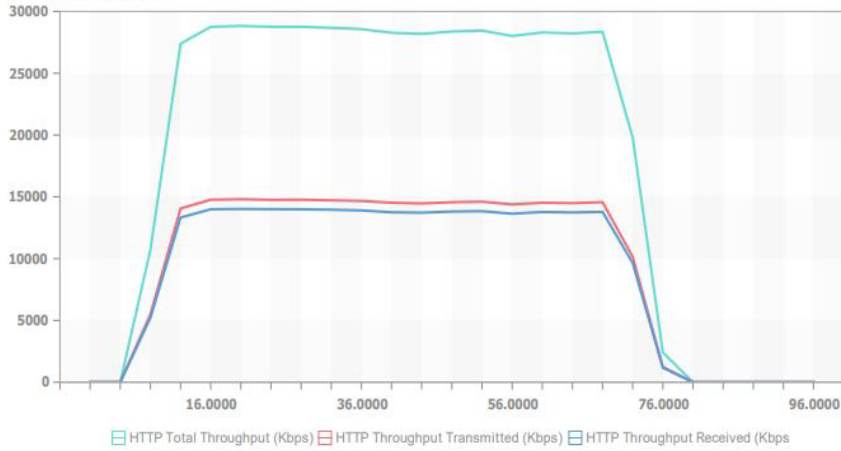
The images below show the API Browser with the full path of the `reportFile` parameter being passed to the `generateRestReport` operation.



The following figure shows an example of a report:

Report

HTTP Throughput



	HTTP Total Throughput (Kbps)	HTTP Throughput Transmitted (Kbps)	HTTP Throughput Received (Kbps)
Minimum	0	0	0
Maximum	28,824	14,804	14,019
Average	18,351.40	9,421.32	8,929.64

Settings

The settings menu contains commands that enable you to configure aspects of the IxLoad Web UI, to upload and download files, to display the help, and to logout.

File operations

You can upload files from the host where you are using the WebUI to the Linux VM, or download files from the VM to the host.

Uploading files

To upload a file:

1. Select Config | File operations | Upload File.
The Upload File window displays.
2. Select Browse, then select the file to upload.
3. In the Server path for the file field, you can specify a path for the file.
If you do not specify a path, the file is saved to the default upload path: `/mnt/ixload-share/`
To specify a different path, specify the path relative to `/mnt/ixload-share/`.
For example, if you specify:
`config/test/`
the file is saved to:
`/mnt/ixload-share/config/test/`

Downloading files

To download a file:

1. Select Config | File operations | Download File.
The Download File window displays.
2. In the Server path for the file field, specify the file and optionally, the path for the file (you can use the REST API to find the path and filename if you do not know them).
If you do not specify a path, IxLoad expects the file to be on the default upload path: `/mnt/ixload-share/`
If the file is on a different path, specify the path relative to `/mnt/ixload-share/`.
For example, if the file and path is:
`/mnt/ixload-share/config/test/sp_2activities.rxf`
specify the file and path as:
`config/test/sp_2activities.rxf`

My Account

The My Account page displays information about the account you used to login to IxWeb UI.

Select Settings | My Account.

The account information displays:

Username	Username currently logged in.
----------	-------------------------------

Email	Email address associated with username.
Name	Descriptive name for username.
API Key	Select Show to display the API Key. If you are using Local authentication the API Key is not necessary, and is displayed for information only. If you are using Ixia User Management authentication, you must include the displayed API Key with REST requests. Under Ixia User Management authentication, each username has a unique API Key.
Role	Privileges allowed to the username.
User Management	Redirects to the configured User Management server, so that you can configure the User Management settings on the server.
User Preferences	Displays the controls for setting personal preferences for using the IxLoad Web UI.

Administration

If you logged into the IxLoad Web UI with an account that has admin rights, the Sessions page includes Administration option.

The screenshot shows a web browser window with the URL <https://10.114.197.180/sessions>. The page title is "Application > Sessions". There are three main cards on the page:

- Create IxLoad Session**: Includes an "Ld" icon and a "LAUNCH" button. Description: "Create and start a new IxLoad session."
- API Browser**: Includes a monitor icon and a "LAUNCH" button. Description: "Launch the API Browser to view the IxLoad data model. An IxLoad session must be active in order to connect the API Browser to it."
- Administration**: Includes a wrench and screwdriver icon and a "LAUNCH" button. Description: "Launch the Administration page, from where Ixia User Management can be enabled."

At the bottom of the cards, it says "Sessions (0)".

Which users have admin rights depends on the Authentication mode that is in use on the IxLoad Web UI:

Authentication mode	Users with admin privileges
Local (default)	admin user (the only user)
Ixia User Management	Any user belonging to the user group on the Ixia User Management server that manages Admin access to the IxLoad Web UI.

The options available on the Administration page are:

- Updates displays the system information and the option to update the Web UI software.
- Authentication manages the settings for access to the Web UI.
- Maintenance enables you to restart the Web UI and the manage the current Web UI sessions.
- Server certificate page enables you upload a custom SSL Certificate for the IxLoad Web UI.

Updates

Updates displays the system information and enables you to update the Web UI software.

SYSTEM SETTINGS

UPDATES

AUTHENTICATION

MAINTENANCE

SERVER CERTIFICATE

System Information

Application Version	1.0.0.88
Disk Usage	15.33% of 96.1GiB used

UPDATE SYSTEM

Installed Applications

IXLOAD WEB	Version: 1.0.0.36
------------	-------------------

UPDATE PACKAGES

Updating the IxLoad Web UI

To update the IxLoad Web UI, select Update System.

The Web UI checks for a new update package, and if one is available, downloads and installs it. After installing the new package, it prompts you to confirm restarting the Web UI VM.

Authentication

Authentication manages the authentication mode that the IxLoad Web UI uses.

The IxLoad Web UI can use either of two authentication modes:

Local (default)	Under Local authentication, only one username can be used: the pre-configured
-----------------	---

	`admin` user.
Ixia User Management	Under Ixia User Management authentication, users must log into the IxLoad Web UI using their Ixia User Management usernames and passwords.

For more information on authentication, see [Authentication on page 9](#)

SYSTEM SETTINGS

UPDATES

AUTHENTICATION

MAINTENANCE

SERVER CERTIFICATE

Authentication Settings

Local
 Ixia User Management

Server address

TEST CONNECTION

Admin group name:

APPLY

Authentication settings

Note: If you change the authentication mode and then apply the new setting, the IxLoad Web UI terminates all current REST API and Web UI sessions and then restarts the Web UI. The new mode is active when the Web UI restarts.

To change the authentication settings:

1. Select Administration | Authentication.
2. Select the authentication type:

1.	Local (default)	Authentication by logging in with the admin username and password.
	Ixia User Management	Authentication by logging in with Ixia User Management usernames and passwords.

3. If you selected Ixia User Management authentication, configure the related parameters:

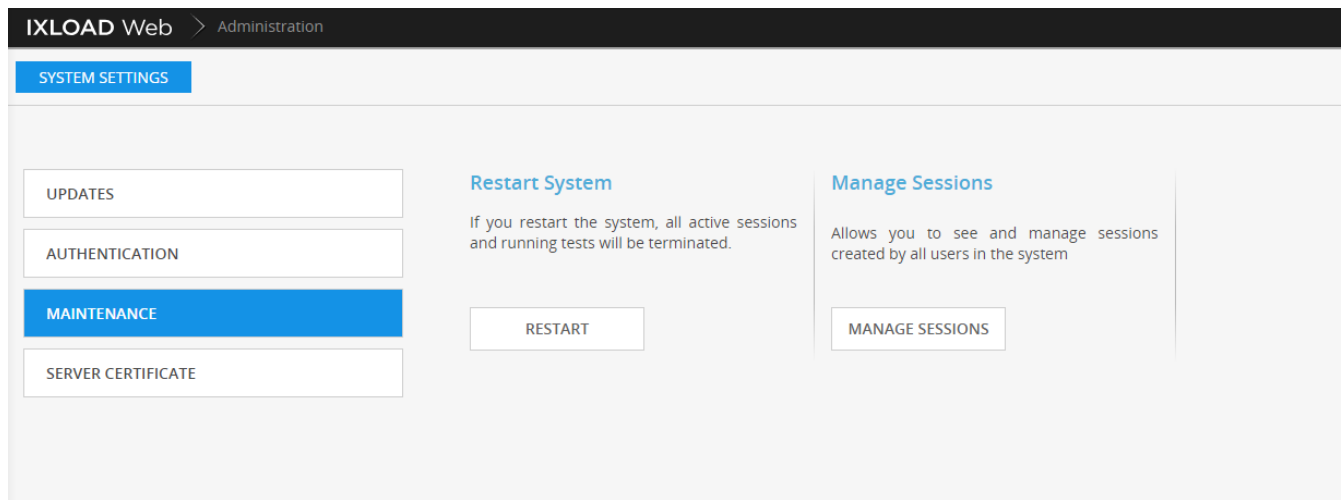
Server	IP address of the Ixia User Management server.
--------	--

address	
Admin group name	Name of the user group on the User Management server that will have admin rights to this IxLoad WebUI.

4. Select Test Connection to contact the server and obtain the server's security certificate.
The first time you try to connect to a new User Management server using Test Connection, the IxLoad Web UI prompts you to add the server's certificate to the chain of trust.
Select Yes to add the certificate.
5. Select Apply.
IxLoad Web UI terminates all current REST API and Web UI sessions and then restarts the Web UI.
The new mode is active when the Web UI restarts.

Maintenance

Maintenance enables you to restart the Web UI and the manage the current Web UI sessions.



Restarting the IxWeb UI

If you restart IxWeb UI, all the existing sessions and running tests are terminated and then the system is rebooted.

To restart, IxWeb UI, click Restart.

Managing IxWeb UI sessions

You can view all the current sessions and delete sessions.

1. To manage the IxWeb UI sessions, click Manage Sessions.
IxWeb UI displays the list of current sessions.

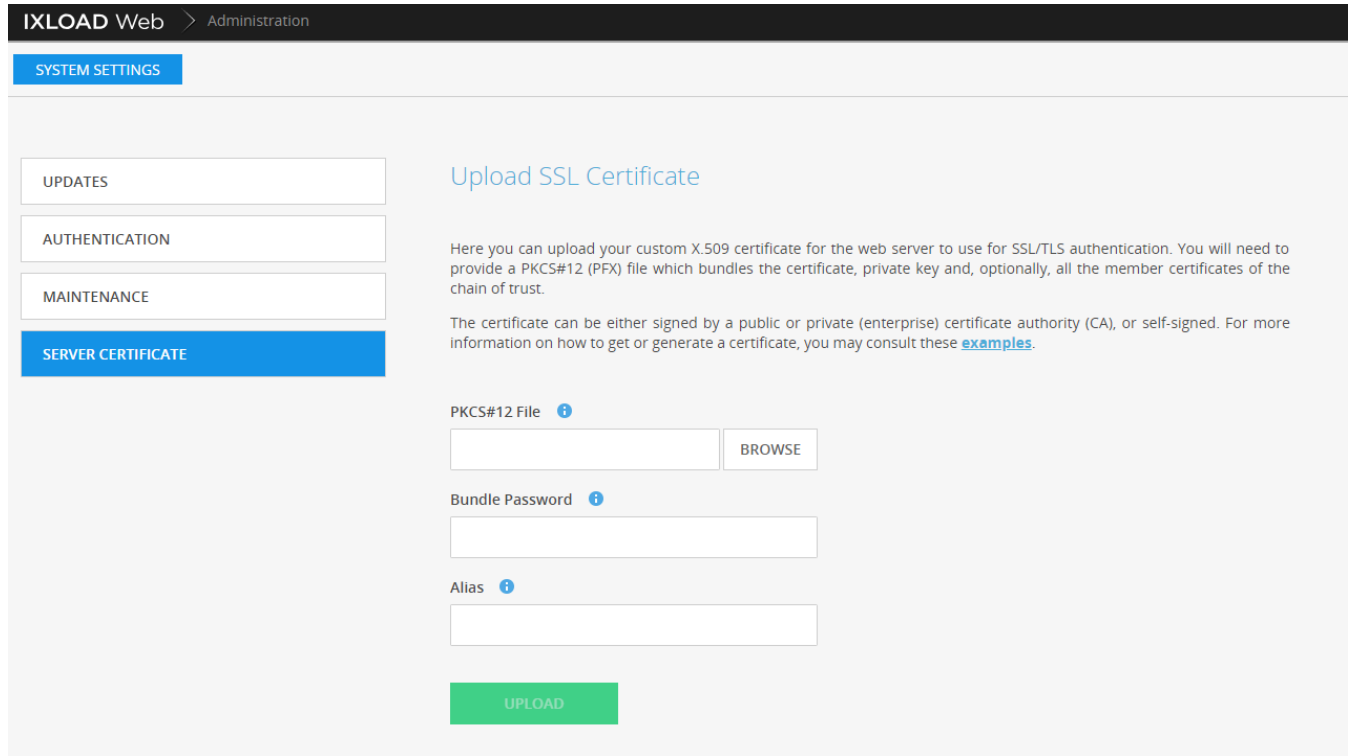
Manage Sessions

	NAME	OWNER	STATE	SUBSTATE	DATE CREATED
<input type="checkbox"/>	Session 1: basicHttp-W...	dan	Active	Test is unc...	3/22/2019, 6:35:58 PM (UTC+02:00)
<input type="checkbox"/>	Session 2: basicHttp-W...	cristi	Active	Test is unc...	3/22/2019, 6:36:20 PM (UTC+02:00)

2. To delete a session, select it, then click Delete.
3. Select Close to return to the Maintenance page.

Server Certificate

The Server Certificate page enables you upload a custom SSL Certificate for the IxLoad Web UI.



To upload a server certificate:

1. In the PKCS #12 File field, select Browse, then select the certificate file.
2. In the Bundle Password field, enter the password for the certificate file.
3. In the Alias field, enter the alias for the certificate keystore.
4. Click Upload.

To begin using the new certificate, you must restart IxWeb UI.

Managing the Test Configuration and Files

This section describes how to:

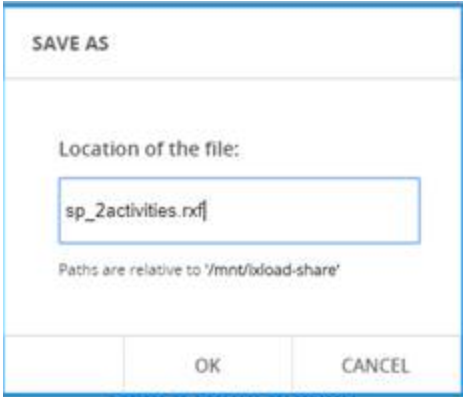

- Save the the test configuration, or load a different test configuration
- Upload and download the test configuration and test files

Saving the test configuration

You can save the current test configuration (in .rxf format) either with the same name or with a different name.

Saving the test

To save the test configuration, choose one:

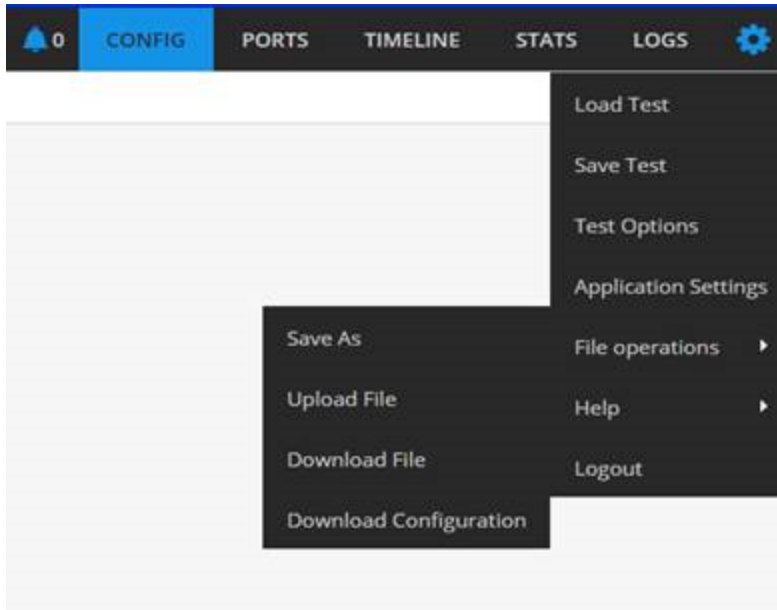
Same name	Different name
<p>To save the test with the same name, select Config File operations Save Test.</p>	<p>To save the test with a different name:</p> <ol style="list-style-type: none">1. Select Config File operations Save As. The Save As window displays. 2. Specify a name and path for the file. If you do not specify a path, the file is saved to the default upload path: <code>/mnt/ixload-share/</code> To specify a different path, specify the path relative to <code>/mnt/ixload-share/</code>. For example, if you specify: <code>config/test/sp_2activities.rxf</code> the file is saved to: <code>/mnt/ixload-share/config/test/sp_2activities.rxf</code> <hr/> <p> Note: To retrieve the upload path, you can use the REST API to perform a GET request on <code>http://localhost:8080/api/v1/resources</code>.</p>

Loading a different test configuration

If you have an existing test session, you can change the test configuration loaded in it. .

To load a different configuration:

1. Display the session's configuration page.
2. Click Load Test.



The Load Config window displays.



3. Specify the .test configuration file to use.

Choose one:

To...	Do this:
Load a recently used file (a file that is already on the Linux VM).	Choose a file from the list, then select OK.
Upload an .rxf or .crf file from the local machine to the Linux VM.	<ol style="list-style-type: none">a. Select Browse.b. Choose an .rxf or .crf file, then select OK. IxLoad uploads the file from the local machine to the Linux VM. If you selected a .crf file, IxLoad uploads it to the VM, and then extracts it in .rxf format.
Manually enter the path to a file on the VM.	<ol style="list-style-type: none">a. Select Server path.b. In the field, enter the absolute path of a configuration file (.rxf or .crf) that already exists on the Linux VM.c. Select OK.

 **Note:** You can also load a configuration from the Settings menu.

Downloading the test configuration

You can download the current test configuration from the Linux VM to the host where you are using the WebUI.

To download the test configuration:

1. Select Config | File operations | Download Configuration.
2. If you have changed the configuration after it was loaded, IxLoad prompts you to save the file.

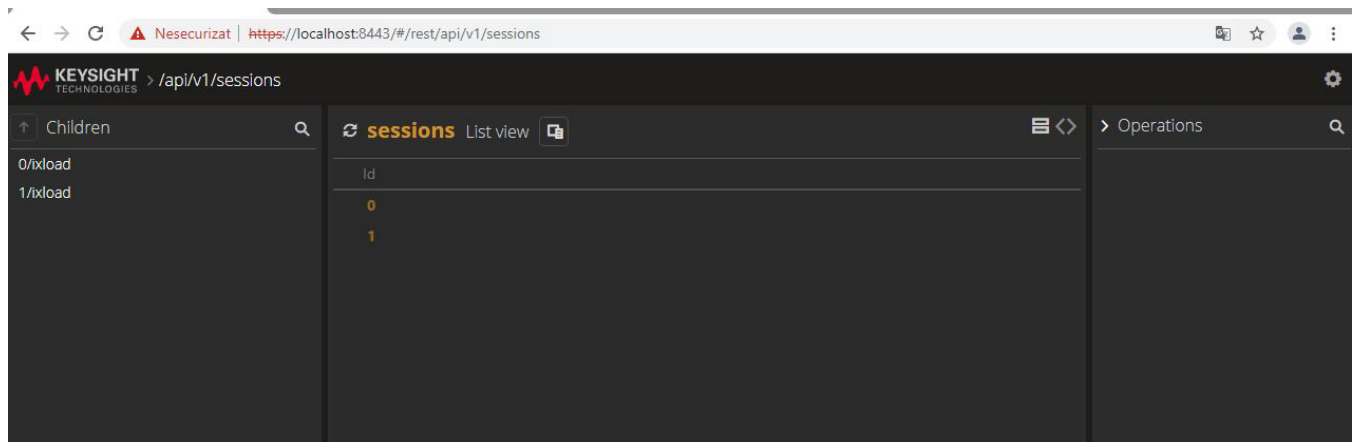
Choose one:

- If you want to save the current configuration before downloading it, select Yes.
- If you want to download the original configuration, select No.

IxLoad downloads the file.

API Browser

The API Browser enables you to view and modify the contents of an open IxLoad REST API session. You can access it on the root URL of the IxLoadGateway service: <https://localhost:8443/> or <http://localhost:8080/>.





© Keysight Technologies, 2016–2021

Keysight Technologies, Inc.
1400 Fountaingrove Parkway
Santa Rosa, CA 95403-1738

www.keysight.com