



# BreakingPoint Release Notes

Release 9.20, December 2021

Release Notes Version 1.0



## **Notices**

### Copyright Notice

© Keysight Technologies 2006 - 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> or <https://support.ixiacom.com/support-services/warranty-license-agreements>. 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 DFARS 227.7103-5 (c), as applicable in any technical data. 52.227-14 (June 1987) or DFARS 252.227-7015 (b)(2) (November 1995), as applicable in any technical data.

**Keysight headquarters**

26601 West Agoura Road  
Calabasas, California 91302  
+1 877 367 4942 – Toll-free North America  
+1 818 871 1800 – Outside North America  
+1.818.871.1805 – Fax  
[www.ixiacom.com/contact/info](http://www.ixiacom.com/contact/info)

Global Support	+1 818 595 2599	<a href="mailto:support@ixiacom.com">support@ixiacom.com</a>
<i>Regional and local support contacts:</i>		
APAC Support	+91 80 4939 6410	<a href="mailto:support@ixiacom.com">support@ixiacom.com</a>
Australia	+61-742434942	<a href="mailto:support@ixiacom.com">support@ixiacom.com</a>
EMEA Support	+40 21 301 5699	<a href="mailto:support-emea@ixiacom.com">support-emea@ixiacom.com</a>
Greater China Region	+400 898 0598	<a href="mailto:support-china@ixiacom.com">support-china@ixiacom.com</a>
Hong Kong	+852-30084465	<a href="mailto:support@ixiacom.com">support@ixiacom.com</a>
India Office	+91 80 4939 6410	<a href="mailto:support-india@ixiacom.com">support-india@ixiacom.com</a>
Japan Head Office	+81 3 5326 1980	<a href="mailto:support-japan@ixiacom.com">support-japan@ixiacom.com</a>
Korea Office	+82 2 3461 0095	<a href="mailto:support-korea@ixiacom.com">support-korea@ixiacom.com</a>
Singapore Office	+656 494 8910	<a href="mailto:support@ixiacom.com">support@ixiacom.com</a>
Taiwan (local toll-free number)	00801856991	<a href="mailto:support@ixiacom.com">support@ixiacom.com</a>

# Contents

<b>Overview .....</b>	<b>5</b>
Document Purpose.....	5
Background .....	5
Technical Support .....	5
Documentation .....	5
<b>What's new in this release .....</b>	<b>6</b>
Customer Issue Resolutions .....	6
<b>Software Compatibility .....</b>	<b>7</b>
<b>Hardware Compatibility.....</b>	<b>8</b>
<b>Browser Compatibility.....</b>	<b>10</b>
<b>Upgrading to Release 9.20 .....</b>	<b>11</b>
Installation Notes.....	11
APS Systems installation steps .....	11
Systems running Native IxOS, BreakingPoint System Upgrade (PS One   XGS2-HS   XGS12-HS) .....	11
Update ATI Packages – applies to all BreakingPoint Versions .....	16
<b>Resolved Defects.....</b>	<b>18</b>
<b>Known Issues and Defects .....</b>	<b>19</b>
<b>Operational Considerations .....</b>	<b>25</b>

# Overview

## Document Purpose

This document provides information regarding the BreakingPoint 9.20 (Version: 9.20.115.12, Build: 422553) release, including information about new features, resolved SRs, known defects and workarounds (if available).

## Background

Powered by Application and Threat Intelligence, BreakingPoint enables companies to maintain resilient IT infrastructures against escalating threats. Only BreakingPoint security and performance testing products stress and optimize end-to-end IT infrastructures by creating real user actions with a blend of application and attack traffic including malware, mobile malware, DDoS, and more.

## Technical Support

To contact the BreakingPoint Support team, e-mail them at [support@ixiacom.com](mailto:support@ixiacom.com) or call them at 1-818 595 2599.

## Documentation

The listed BreakingPoint documentation can be obtained at:  
<https://support.ixiacom.com/user-guide> > **BreakingPoint**

- *Ixia BreakingPoint User Guide*
- *Ixia BreakingPoint Virtual Edition (VE) Installation Guide*
- *Ixia APS-M1010/APS-ONE-100 Installation Guide*
- *KCOS CLI Reference Guide for APS*

Documentation for, *PerfectStorm - XGS12 Chassis Platform Assembly Guide*, can be obtained at:

[http://downloads.ixiacom.com/library/user\\_guides/IxOS/8.00/EA\\_8.00\\_Rev\\_A/XGS12ChassisPlatformAssemblyGuide/XGS12ChassisPlatformAssemblyGuide.pdf](http://downloads.ixiacom.com/library/user_guides/IxOS/8.00/EA_8.00_Rev_A/XGS12ChassisPlatformAssemblyGuide/XGS12ChassisPlatformAssemblyGuide.pdf)

## What's new in this release

BreakingPoint 9.20 is an alignment release which adds multiple features and enhancements. This release consolidates all releases since last 9.10 alignment release, including the update and customer specific patch releases.

The new features in BreakingPoint 9.20 release are:

- Introduce Keysight's new APS-100-ONE Standalone next-generation network applications and security test platform. Each APS-ONE-100 appliance supports two native QSFP28 100GE active interfaces for test traffic generation.
- Added Support for Keysight's new CloudStorm-XP, 100GE 2-port load module
- TLS 1.3 PSK is now supported on all APS appliances
- Limited support for BPS Labs has been added for all APS versions, for more details please consult the UserGuide
- **Experimental feature (ALPHA level - not fully tested):** Added support for four native QSFP28 100GE for all APS-100-ONE appliances (connected to an APS-M1010 controller or Standalone)
- BreakingPoint VE has been updated to support the latest versions of popular virtualization platforms: VMware ESXi 7.x / VMware vCenter 7.x, KVM on CentOS 8.x / RHEL 8.x / Ubuntu 20.04 and OpenStack Wallaby
- Support for Intel E810 series NICs running in PCI-PT or SR-IOV was added for BreakingPoint VE platform
- Super Component for aggregating the resources of multiple ports under the same traffic component configuration is now available as a more user-friendly method to create complex traffic scenarios

## Customer Issue Resolutions

This release also addresses several important issues reported by BreakingPoint users. Please refer to the [Resolved Defects](#) section for the complete list.

## Software Compatibility

BreakingPoint 9.20 (Version: 9.20.115.12, Build: 422553) Firmware Release is a cross-platform release. Please review the following table to identify the software required for your hardware platform.

Platform	BreakingPoint Firmware	IxOS Software	FlixOS/KCOS Software
XGS12-HS chassis	BreakingPoint 9.20	IxOS 9.20	FlixOS for Native IxOS: 2021.1.84.1 (see the <a href="#">Product Compatibility Matrix</a> for the correct FlixOS version)
PerfectStorm ONE Fusion appliances	BreakingPoint 9.20	IxOS 9.20	FlixOS for Native IxOS: 2021.1.84.1 (see the <a href="#">Product Compatibility Matrix</a> for the correct FlixOS version)  Note: Starting with 8.13, PerfectStorm ONE does not support Windows-based software. To support 8.13 and higher releases, PerfectStorm ONE appliances need to be <a href="#">converted to Native IxOS</a> .
APS-M1010/APS-ONE-100	BreakingPoint 9.20	N/A	KCOS 9.20.12

## Hardware Compatibility

The BreakingPoint 9.20 release is supported on CloudStorm and PerfectStorm load modules, plus the new APS platform.

### APS System

Part Number	Description
941-0113-01	APS-M1010 Management Controller Node
941-0110-02	APS-ONE-100, Compute Node with 4x100GE front I/O ports for the APS-M1010 Management Controller

### 12-slot XGS12 Chassis and CloudStorm/PerfectStorm Fusion Load Module

Part Number	Description
940-0006	XGS12-HS 12-slot, Chassis Bundle
905-1016	CloudStorm 50GE FAN-OUT FACTORY INSTALLED option
905-1017	CloudStorm 50GE FAN-OUT-UPG UPGRADE Option
905-1029	CloudStorm 50G and 100GE Field upgrade option
905-1014	CloudStorm 25GE FAN-OUT FACTORY INSTALLED Option
905-1015	CloudStorm 25GE FAN-OUT-UPG FIELD UPGRADE Option
905-1018	CloudStorm 10GE FAN-OUT FACTORY INSTALLED Option
905-1019	CloudStorm 10GE FAN-OUT-UPG FIELD UPGRADE Option
905-1028	Field Hardware Upgrade from CloudStorm 10G to CloudStorm 10/40G
905-1030	Field Hardware Upgrade from CloudStorm 10/40G to CloudStorm 10/40/25G
905-1030	Field Hardware Upgrade from CloudStorm NonFusion to CloudStorm Fusion
944-1232	CloudStorm Fusion, 2-port 100GE Load Module (CS100GE2Q28NG), 40G Support with Upgrade license
944-1237	CS40GE2Q28NG: CloudStorm 40G fusion CloudStorm Fusion, 2-port 40GE Load Module (CS40GE2Q28NG), 100G Support with Upgrade license
944-1235	CS25GE8Q28NG: CloudStorm 25GE fusion 8-port 25GE Load Module



Part Number	Description
944-1233	CS100GE2Q28NGALL: CloudStorm 100GE fusion 2-port 100GE Load Module
944-1253	CSXP100GE2Q28ALL: CloudStorm-XP 100GE fusion 2-port 100GE Load Module
944-1201	PerfectStorm Fusion, 2-port 40/10GE QSFP+ Load Module (PS40GE2NG)
944-1200	PerfectStorm Fusion, 8-port 10/1 GE SFP+ Load Module (PS10GE8NG)
944-1209	PerfectStorm Fusion, 4-port 10/1 GE SFP+ Load Module (PS10GE4NG)
944-1210	PerfectStorm Fusion, 2-port 10/1 GE SFP+ Load Module (PS10GE2NG)
944-1202	PerfectStorm Fusion, 1-port 100GE CXP Load Module (PS100GE1NG)

### PerfectStorm ONE Fusion Appliances

Part Number	Description
941-0028	PerfectStorm ONE Fusion, 40GE 2-port QSFP+ appliance (PS40GE2NG)
941-0027	PerfectStorm ONE Fusion, 8-port 10/1 GE SFP+ appliance (PS10GE8NG)
941-0031	PerfectStorm ONE Fusion, 4-port 10/1 GE SFP+ appliance (PS10GE4NG)
941-0032	PerfectStorm ONE Fusion, 2-port 10/1 GE SFP+ appliance (PS10GE2NG)
941-0033	PerfectStorm ONE Fusion, 8-port 1 GE SFP+ appliance (PS1GE8NG)
941-0034	PerfectStorm ONE Fusion, 4-port 1 GE SFP+ appliance (PS1GE4NG)

For the PerfectStorm platform, please refer to the [Product Compatibility Matrix](#) available on Ixia's website. An Ixia website account is required before accessing.

## Browser Compatibility

The table below lists the HTML browsers supported by BreakingPoint. Browser versions that are more current than the versions listed in the table may work but have not been tested at this time. Beta versions of HTML browsers are not supported.

Browser	Recommendation for Windows	Recommendation for MAC
Google Chrome	96.0.4664.45 (64-bit)	96.0.4664.45 (64-bit)
Firefox	Firefox 94.0 (64-bit)	Firefox 94.0 (64-bit)
Microsoft Edge	96.0.1054.43	N/A
Safari	Not supported	15.1
Internet Explorer	Not supported	Not supported

**Note:** In BreakingPoint 3.5.1, and higher releases, logging in to the management UI will not be allowed from HTML browsers that have a maximum SSL version setting that is limited to only sslv3 (ssl3).

**Note:** Mac users with OS 10.8.2 can use Firefox or Google Chrome as their browser.

# Upgrading to Release 9.20

## Compatibility Matrix

BreakingPoint	9.20
IxOS	9.20
IxLoad	9.20
IxNetwork	9.20
Licensing	5.40

## Installation Notes

Specific instructions for installation on Keysight systems are contained in the sections below.

**Note:** The version numbers shown in the images below may not be the current version numbers, but the procedure is the same.

## APS Systems installation steps

Detailed steps dedicated to the APS platforms and more details can be consulted in the document available here:

[https://downloads.ixiacom.com/library/user\\_guides/breakingpoint/9.20/APS\\_Installation\\_Guide\\_9.20.pdf](https://downloads.ixiacom.com/library/user_guides/breakingpoint/9.20/APS_Installation_Guide_9.20.pdf)

## Systems running Native IxOS, BreakingPoint System Upgrade (PS One | XGS2-HS | XGS12-HS)

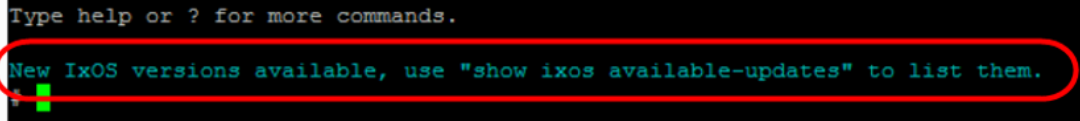
Ixia strongly recommends that you create backups of your system before upgrading to the BreakingPoint 9.20 Firmware release.

- **Upgrading IxOS on Native IxOS systems**

### Online:

1. Access the Ixia Chassis CLI - `ssh admin@<chassisIP> -p 22, password: admin`
2. Apply command "enter Chassis" to access to Chassis CLI

You will be notified through the CLI when new builds of IxOS (IxOS9.00) are available.



```
Type help or ? for more commands.
```

New IxOS versions available, use "show ixos available-updates" to list them.

The screenshot shows a terminal window with a black background and green text. A red oval highlights the message "New IxOS versions available, use 'show ixos available-updates' to list them."

3. Run the `install ixos <version>` command to perform the install. The build will be installed automatically from Ixia IxOS online repository (which is predefined in the OS).

**Offline:**

1. Download the IxOS build from <https://support.ixiacom.com/ixos-software-downloads-documentation>.
2. Use FTP to put the file on to the Chassis.

```
ftp://<chassisIP>  
user: admin  
password: admin
```

```
Put Ixia_Hardware_Chassis_XX.XX.XX-EA.tar.gz.gpg
```

4. Access the IxOS CLI - `ssh admin@<chassisIP> -p 22`, password: admin
5. Apply command "enter Chassis" to access to Chassis CLI
6. Run the `install ixos <version>` command to perform the install of the version that was downloaded.
7. Reboot the chassis.

## Upgrading the BreakingPoint System

- **BreakingPoint in Native IxOS:** ixia-web-platform-bps-xx.xx.xx.xx.el7.x86\_64.waf should be used for chassis or appliances running in a Native IxOS system. Depending on the BPS version running on the system, the user needs to follow one of the two upgrade procedures below:

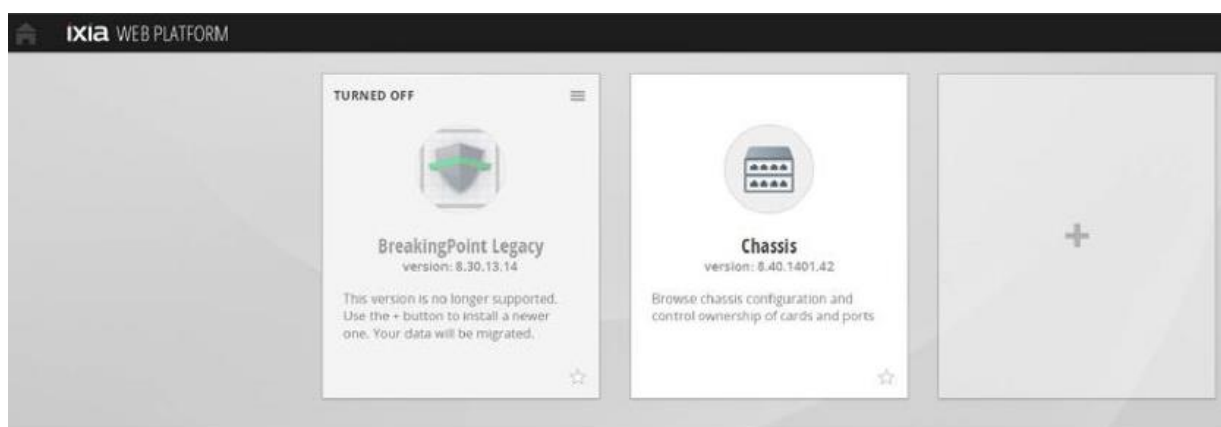
### 1. Systems running BreakingPoint 8.40 or newer

1. From IXIA BreakingPoint Page, click **Launch Administration**.
2. Click **BPS Software Update**
3. Click **UPDATE SYSTEM**
4. Click on the checkbox, "I created a backup ...."
5. Use BreakingPoint installer Package (ixia-webplatform-bps-9.20.110.25 ..waf) to upgrade to BreakingPoint 9.20 version. The installer package (ixia-webplatform-bps-9.20.110.25 ..waf) can be downloaded IXIA support download web page.

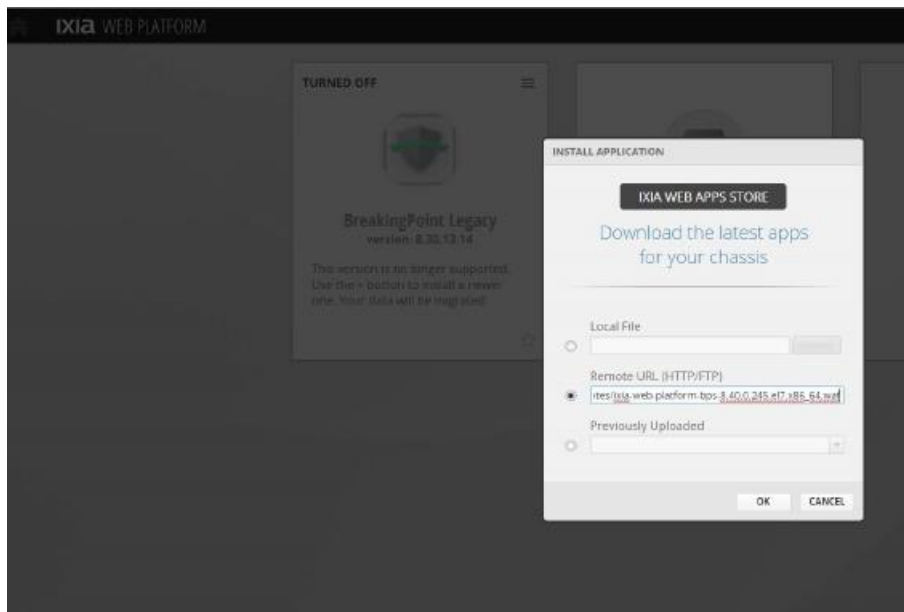
### 2. Systems running versions earlier than BreakingPoint 8.40

1. Once the IxOS installation is complete, connect to Chassis IP: <https://<Chassis IP>>.
2. Log in using user id: admin, password: admin.

After logging in, the WebPlatform Dashboard will display as shown in the image below.

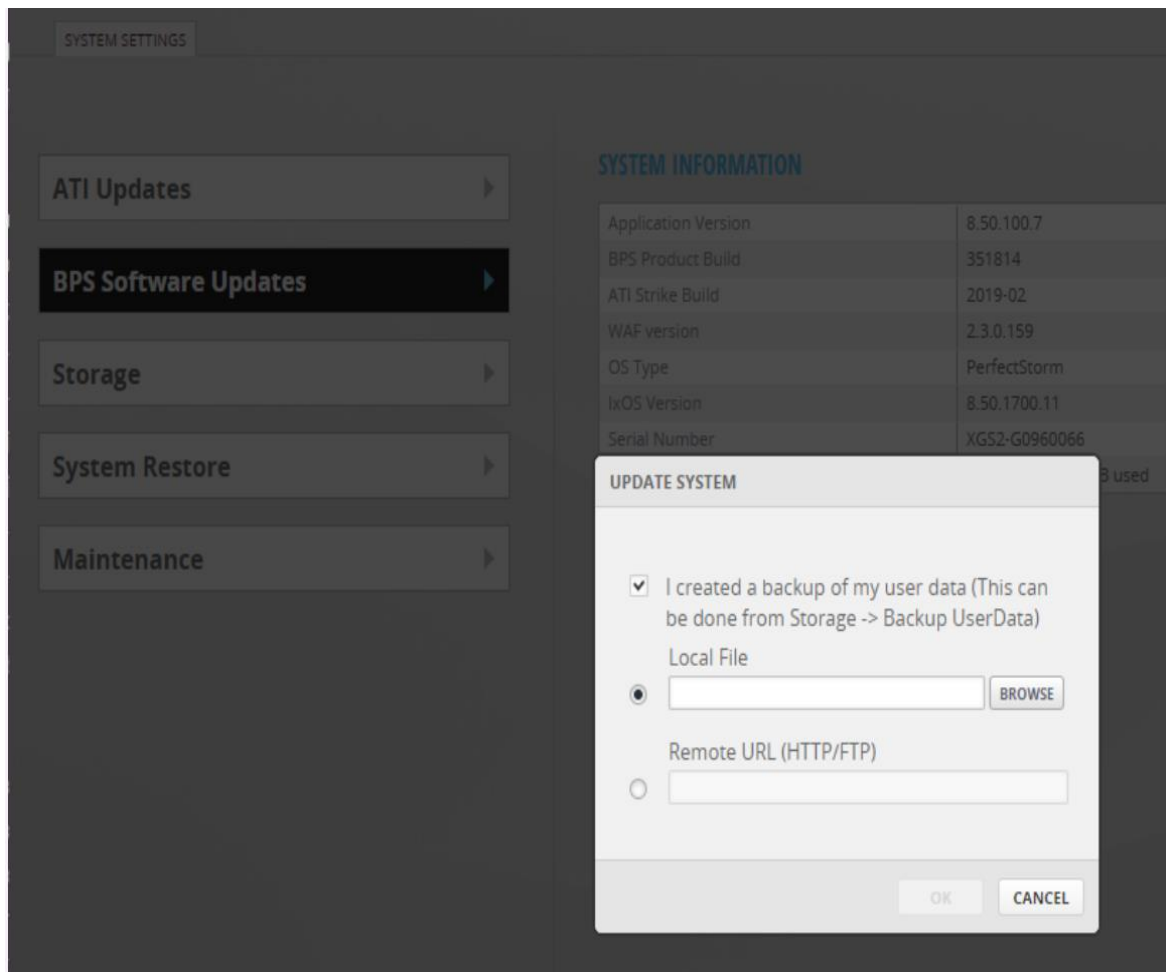


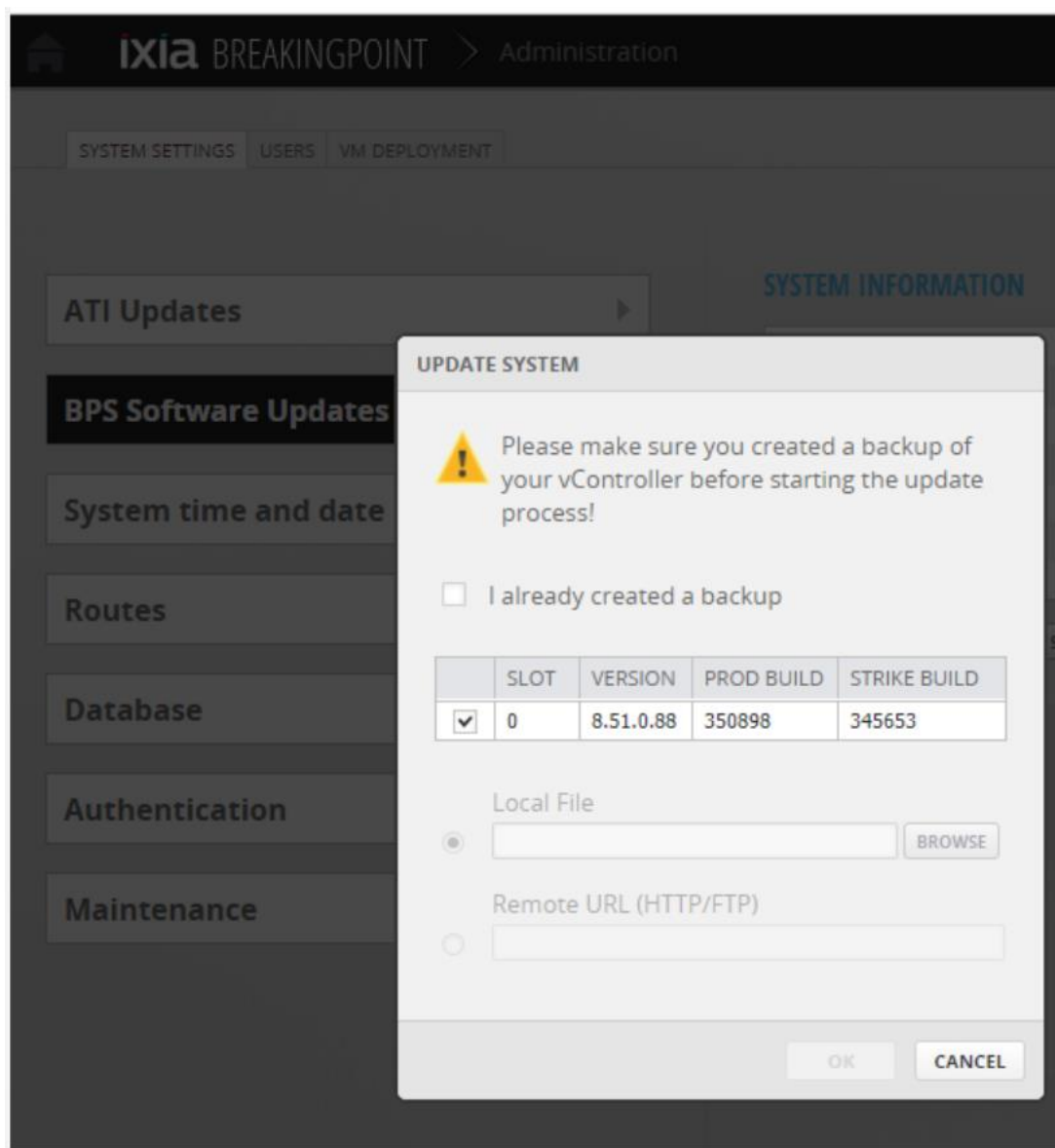
3. Click the **Install New Applications** icon (+) to install BreakingPoint using the BreakingPoint installer Package (ixia-webplatform-bps-9.20.110.25 ..waf). The installer package (ixia-webplatform-bps-9.20.110.25 ..waf) can be downloaded from the IXIA support download web page.
4. Select the Installer Package as shown in the image below. Then click **OK** to start the BreakingPoint installation.



5. After the installation is complete, log in using user id: admin and password: admin.
6. Click the **BreakingPoint Application** icon to launch BreakingPoint.

**Figure 1: BreakingPoint System Update Page:**





## Update ATI Packages – applies to all BreakingPoint Versions

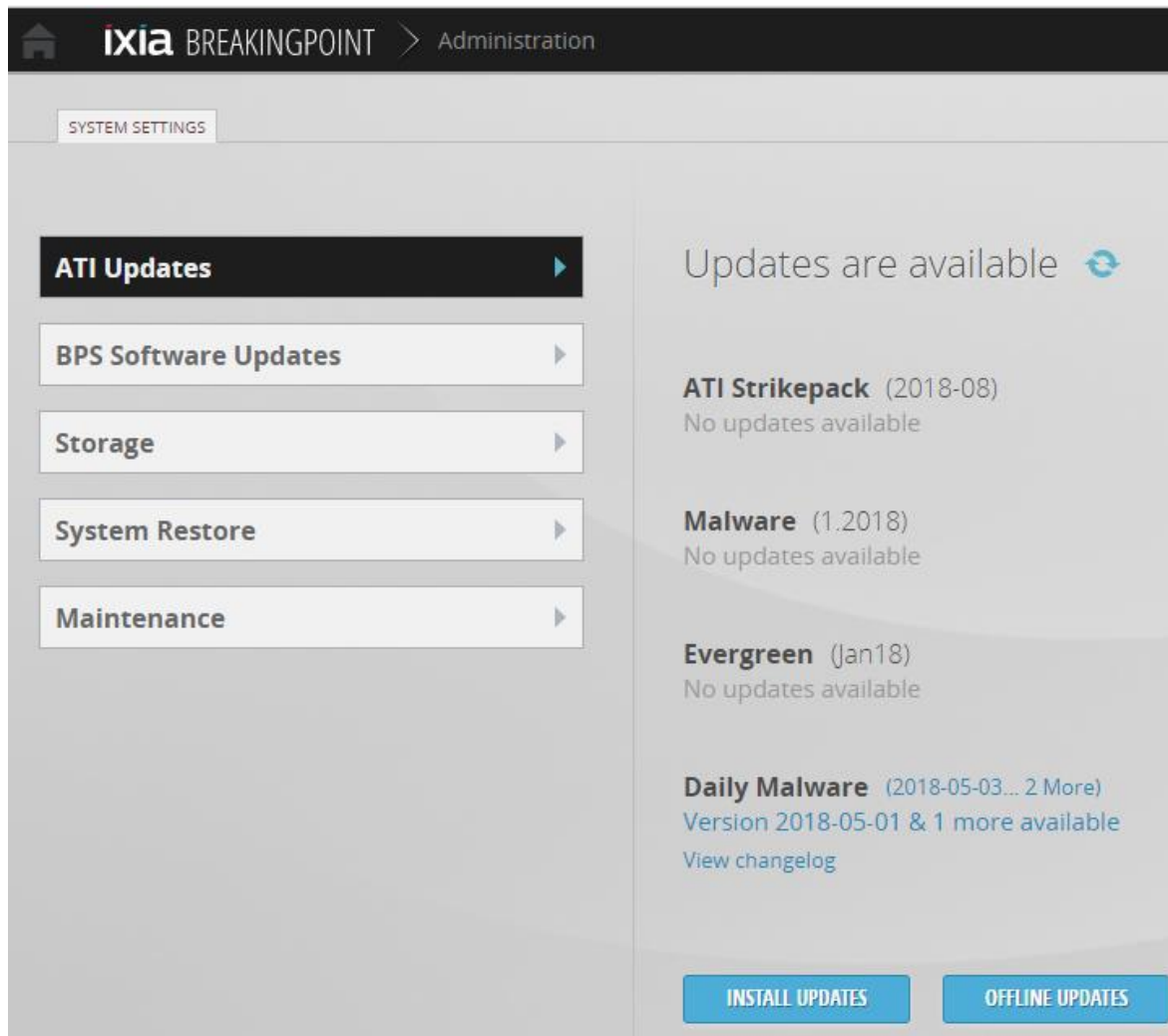
The Application and Threat Intelligence (ATI) program provides updates frequently to ensure the delivery of the industry's most up to date application and threat intelligence. Starting from this release, both Online and Offline ATI updates procedures are available. For Online update, user will be notified the availability of the Update right after logging into the BreakingPoint systems, please refer to Figure 1. Choose the package to be installed and click "INSTALL UPDATES".

For an Offline update, download ATI Update Packages from:

<https://support.ixiacom.com/support-overview/product-support/downloads-updates> , click **OFFLINE UPDATES**, please refer to Figure 3.



**Figure 3: Ixia WEB APPS Start Page**



## Resolved Defects

The following table lists defects from previous releases that have been resolved. If you have any concerns or questions regarding the defects listed here, please contact the BreakingPoint support team at [support@ixiacom.com](mailto:support@ixiacom.com) or call them at 1-818-595-2599.

CR ID #	Description
<b>BPS-2682</b>	A test which was configured to stop once the RX frames reached 300 remains stuck at 100% progress.
<b>BPS-2453</b>	User is unable to upload certificates/keys in Web Platform due to Permission denied error.
<b>BPS-555</b>	When using the command "enter bps", ssh/cli session to PS XGS system gets logged out.
<b>BPS-2359</b>	BPS TCL: exportPacketTrace returns "sync failed" when generating the default compressed .pcap.gz file
<b>BPS-2373</b>	When running a test with evasion profile -> http -> transport option=GET, there are situation when the test stops and ATI striketoflows errors are returned.

## Known Issues and Defects

**Note: To run IPsec tests, you must install the IPsec package.** The installation procedure is similar to a Strikepack installation. The IPsec package can be found at: <https://support.ixiacom.com/support-overview/product-support/downloads-updates/versions/185>.

The following section details the known issues and defects of Firmware Release 9.20. Workarounds are listed for each defect if they are available. If you have any concerns or questions regarding the defects listed here, please contact the BreakingPoint support team at [support@ixiacom.com](mailto:support@ixiacom.com) or call them at 1-818-595-2599.

### BreakingPoint Hardware:

Reference #	Description
<b>1522597</b>	Changing the card mode to BPSQT mode if BPSQT is not installed will lead to card instability.
<b>NA</b>	Even if break-out mode is available for Cloudstorm-XP cards, only 2 * 100GE mode is supported in BPS

### BreakingPoint Licensing:

Reference #	Description
<b>1353064</b>	"License statistics" does not show the actual hostname and IP of the controller checking out the licenses from the license server.

### BreakingPoint on APS platform:

Reference #	Description
<b>BPS-3356</b>	L23 implementation for APS platform is software based, so the performance is not optimal
<b>BUG1561205</b>	To avoid network errors and use the APS hardware at maximum performance, each test component requires its own pair of Virtual Routers in the Network Neighborhood. This is applicable for tests that require VR due to the availability of only two MAC addresses per port.
<b>BUG1537744</b>	For the APS platform, the maximum throughput is lower than the theoretical bidirectional line-rate.
<b>BUG1559262</b>	The APS-ONE-100 CPUs have variable frequency technology, meaning that after a period of inactivity they will go to low energy mode. This

Reference #	Description
	can cause the first test run after an idle period to have lower performance than expected – the workaround is to restart the test.
<b>BUG1566875</b>	The first port in BreakingPoint and KCOS with id 0 is corresponding to the first test interface port on the chassis labeled as 1. Similarly, port 1,2,3 corresponds to labels 2,3,4.
<b>BUG1548614</b>	Layer 2 latency has lower accuracy due to lack of latency hardware support.
<b>BUG1550746</b>	APS 100 ports will always use the VNIC MAC address regardless of the configuration in the network neighborhood.
<b>BUG1562466</b>	In BreakingPoint, the packet capture on the receiving port is executed on the application layer and are therefore observed as bigger aggregated segments, not what is actually sent/received on the wire. The packet capture on the transmitting data port reflects the correct packets.
<b>BUG1565231</b>	The software data capture will impact throughput performance.
<b>BUG1565281</b>	The checksum values are computed by the NIC hardware when they are sent. Currently, the software capture can't catch the packet as it goes out on the wire.
<b>BUG1565633</b>	For captures collected during back to back tests, the frames count and size is not always accurate.
<b>BUG1565851</b>	The progress bar will show 0% during the entire packet capture export process.
<b>BUG1567050</b>	When using Super Component with a custom load profile, some of the limits like data rate are not respected.
<b>BUG1559550</b>	In some scenarios the maximum throughput for IPSEC tests is limited to ~20Gbps.
<b>BUG1564708</b>	Attached rates may vary during the tests on APS platform. In most scenarios there are variations present towards the end of the test.
<b>BUG1564933</b>	The progress bar will show 0% during the entire diagnostics generation process.
<b>BUG1565705</b>	Link status cannot be changed on reserved ports. To change the link status, unreserve the port, change link status and reserve the port again.
<b>BUG1566133</b>	In some scenarios, the throughput will show a temporary increase in the ramp down phase. This is due to connections being torn down and test system resources being freed.

Reference #	Description
<b>BUG1566509</b>	The configured percentage of TLS session reuse is not always guaranteed to be maintained.
<b>BUG1560998</b>	KCOS Cloud Native Architecture approach limits the ability of changing the system date and time due to underlying Kubernetes architecture.
<b>BUG1561298</b>	Elephant Flow in proxy mode achieves lower performance due to the usage of proxy buffers.
<b>BUG1565283</b>	Sometimes an error can occur if a user tries to log in immediately after an upgrade. The workaround is to wait for a few minutes.
<b>BUG1565950</b>	When Proxy is enabled, Elephant flow will not have the max performance achievable without Proxy enabled.
<b>BUG1565995</b>	With the Elephant Flow test - running with a single or fewer connections - the test will sometimes run into some CPU core usage issues. Occasionally CPU usages shows unequal values throughout the cores.
<b>BUG1559900</b>	After a user with administrative permissions signs out from the Access Control page, the user is still connected in WAF. When this same user selects the Access Control option from WAF page again, they will be required to enter the credentials, while this was not initially required.
<b>BUG1562116</b>	When HTTPS and HTTP-Simulated is running within a single Super Flow, test shows cryptographic errors with HTTPS flows. The workaround is to remove the HTTP-simulated flows and run them separately.
<b>BUG1565217</b>	Reboot is required when creating a snapshot in order to ensure data consistency.
<b>BUG1565270</b>	xshell will not display progress correctly during the installation of new packages.
<b>BUG1565456</b>	DNS Perf QPS value is limited to 5.7M in the current release.
<b>BUG1565675</b>	Full DB restore functionality is no longer supported. With this architecture export/restore needs to be done separately for users and tests.
<b>BUG1566414</b>	For TLS mix with smaller handshake timeout under 30 seconds, some of the Super Flows can get expired causing handshake failures. A larger handshake timeout should be used as a workaround.
<b>N/A</b>	Each APS-ONE-100 node has 2 dual port Network Interfaces (NIC) for the test ports. Each NIC is capable of doing close to 100 Gbps in each direction. Running traffic using only the ports of a single NIC might have undesirable results and reduced performance. It is recommended to run tests on pair of ports, one from each NIC.

Reference #	Description
<b>BPS-3349</b>	<p>Updating the APS platform to the 9.20 release version will clear previous results database. This will be fixed in the next release.</p> <p>Users should take backup of the data or export individual reports if needed.</p>

### BreakingPoint Virtual Edition:

Reference #	Description
	<p><b>Google Cloud Platform limitations</b></p> <ul style="list-style-type: none"> <li>• Some attacks may get blocked by Google Cloud Infrastructure</li> <li>• MTU is limited to 1460 bytes</li> <li>• Some bad TCP packets are blocked by Google Cloud Infrastructure (bad L4 checksum, bad TCP header length, etc.)</li> </ul>
<b>BPS-3354</b>	The Stack Scrambler tests with IPv6 executed on SR-IOV/DPDK platforms will suffer a throughput degradation compared with previous releases. This will be addressed in a future build.
<b>BPS-3291</b>	On Breakingpoint VE deployments that are upgraded from older versions you will not be able to detach and re-attach a vBlade - this operation will fail resulting in permanently detached vBlade. New deployed setups with 9.20 version will not experience the same behavior.
<b>1527029</b>	In the GUI, the Port Capabilities from Port Information tab is not populated with the speed for Mellanox boards.
<b>1528057</b>	Hostname changes on the Virtual Controller and Virtual Blade are not supported in this release.
<b>1528058</b>	Cloud Init is not currently supported on Virtual Machines deployed through Microsoft Azure Public Cloud.
<b>1528272</b>	For instances running in Amazon AWS Public Cloud, the DPDK Performance Acceleration feature cannot be enabled on C5.XLARGE instance types. This is caused by the memory limit of the instance.
<b>1530388</b>	For instances running in Amazon AWS Public Cloud, you may occasionally experience a small packet loss for high throughput tests. This is caused by packet drops occurring at the AWS infrastructure level.
<b>1536838</b>	In Microsoft Azure Public Cloud, there are scenarios where the RX / TX statistics may be inaccurate due to the SO/LRO mechanism.

Reference #	Description
<b>1538040</b>	Strike attacks will be blocked on VMware ESXi hypervisors, where multicast promiscuous cannot be enabled in SR-IOV mode. This is a hypervisor documented behavior.
<b>1540536</b>	For instances running in Amazon AWS Public Cloud, if the test is using IPv6 address, RPC - Call packets are not reaching the server port.
<b>1543349</b>	Because the current release delivers a new base OS version, updating from previous versions on BreakingPoint is not supported. In order to use BreakingPoint 9.20 Virtual Edition a clean deployment is required.
<b>1543634</b>	For Mellanox ConnectX-5 100Gbps board the port speed is incorrectly displayed as 34464 in the TCL API and GUI.
<b>1545292</b>	If ports are not appearing in the Virtual Blade after enabling Performance Acceleration, please make sure that your VM compatibility is upgraded (on VMware setups).

### BreakingPoint SSL:

Reference #	Description
<b>BPS-3396</b>	In some scenarios when DUT policy was changed on the fly for TLS1.2 proxy with session reuse, the test port might run into instability.
<b>1536243</b>	Session resumption percentage will not function correctly when a low session capacity is configured.
<b>1542900</b>	DHE cypher is not supported in this release and will be addressed in a future version. In some SSL CC tests, this may cause test instability.
<b>1544479</b>	BreakingPoint SSL Server will not pick the minimum TLS version when there is a mismatch and the client is asking for a lower TLS version: <ul style="list-style-type: none"><li>• Downgrade to TLS1.0 from TLS1.1 is not supported</li><li>• Downgrade to TLS1.1 from TLS1.2 is not supported</li><li>• Downgrade to TLS1.0 from TLS1.2 is not supported</li></ul>
<b>1544621</b>	Session resumption percentage has limited statistics in this release.

## BreakingPoint Automation:

Reference #	Description
<b>1547292</b>	When requesting the latest values for real time stats using RESTv2, the list with stats values retrieved may be incomplete. To avoid this, the argument numdatapoints should be set to a value > 1, by default this value is 1. bps_connection.testmodel.realTimeStats(runid=test_id, rtsgroup="all", numSeconds= -1, numDataPoints=2)
<b>1547306</b>	When using RESTv2, the realtime stats operation is not retrieving a set of values for each second if numseconds = numdatapoint > 1.
<b>1533948</b>	When using RESTv2, when pulling the real time statistics available for a specific time interval, some stat names may not be retrieved.

## BreakingPoint Functionality:

Reference #	Description
<b>BPS-3324</b>	Sometimes, when exporting a test, the "GUI is using the wrong jsessionid" error is thrown. The workaround is to refresh the page and try again.
<b>BPS-3244</b>	On Cloudstorm-XP cards, the IPSEC tunnel capacity is limited to 250000 when using IKEv2.
<b>BPS-3180</b>	AppSim tests that use Recreate will experience flow errors in certain scenarios
<b>1541043</b>	Components (client Tags/server Tags) are not saved when using the new Multicomponent Edit functionality.
<b>1544481</b>	Running a high number of parallel performance tests (more than 12 instances) can create instability on some of the cards.
<b>1536140</b>	Occasionally L2-3 tests on CloudStorm cards are not responding to run time settings. Workaround: To work around this issue, Stop the test from the UI.
<b>BPS-3394</b>	SCTP Authentication containing reverse method in the setup request is not functional. This will be addressed in a future ATI update.
<b>BPS-3252</b>	Some scenarios simulating SCTP over GTP tests can run into port instability.



# Operational Considerations

## BPS on non-APS Platforms

Reference #	Description
<b>1486863</b>	<p>Be aware that when you are testing, NP assignment is driven by affinity. The affinity is established based on the order of the interface selection.</p> <p>In case of running on a CloudStorm fan-out card, the NP allocation is done dynamically, based on the resources needed. However, in order to ensure that all resources are allocated at all times, you need to select the client/server interfaces from different Resource Groups.</p>
<b>1427345</b>	<p>The available disk space on the chassis after Native IxOS conversion becomes limited. Up to 70% of the HDD contains information for restoring the chassis to Windows mode (undoing the Native IxOS conversion). We recommended that you reclaim this disk space by deleting the legacy BPS information (use IxOS CLI command: <code>uninstall bps legacy</code>) before running a long duration scaled test.</p>
<b>1425901</b>	<p>CloudStorm hardware interprets the increment/decrement port settings in a slightly different manner than earlier BPS blades. In both cases the user sets the "starting port number" and the "mask size". For example, consider an incrementing case where the mask is set to eight bits; In CloudStorm, the port numbers generated will increment from "starting port + 0" to "starting port + 255". In blades other than CloudStorm, using the same settings, the eight least significant bits in the starting port will be replaced by an incrementing value of 0 to 255. It should be noted that if the user sets the "starting port number" such that the masked bits are zero, the resulting port # sequences generated by both sets of hardware will be identical. This is likely the most common configuration as the masked bits in the "starting port number" are essentially ignored by legacy hardware. The newer mechanism gives more flexible control over the port ranges.</p>
<b>1425332</b>	<p>On CloudStorm for a Security/Security NP test in combination with other components such as AppSim or Routing Robot, adding a new component and changing the tags might take longer. The higher the number of components the longer the delay for the tag change.</p>
<b>1423380</b>	<p>Four AppSim components are required to achieve the Max GTP UE attached rate on CloudStorm.</p>
<b>1422408</b>	<p>The Delayed Start feature in Layer 2/3 on a CloudStorm blade has a +/- 10 second tolerance in this release.</p>
<b>1409901</b>	<p>The files created for backups of native IxOS databases vary in size, and can take more than an hour to backup or to restore. The main component of their size is the number and size of test reports included in the database files. If you wish to reduce the time taken by the</p>

Reference #	Description
	backup and restore functions, delete unneeded test reports prior to running the backup or restore.
<b>1398134</b>	Note that GTP tunnel creation is not dependent on the number of sessions. BPS creates tunnels irrespective of session rate.
<b>1309762</b>	When PerfectStorm is in L2/L3 mode, only one network processor is available to generate application traffic. Therefore, maximum performance/throughput is expected to be lower for L4/L7 test components while L2/L3 tests will perform as expected.

## BPS on APS Platform

Reference #	Description
<b>NA</b>	LR (long range) transceivers are not supported for this release, we recommend the use of SR (short range) transceivers with APS platform.
<b>BPS-3277</b>	<p>Starting with this release, similarly to other platforms, the user needs to reserve all (4) ports from one node to obtain maximum performance.</p> <p>When using 4x100GE multiport mode to run two tests in parallel, each with two ports, an execution of a test on the 2nd pair of ports will reduce the performance of a previous test on 1st pair of ports by 50%. Please note that running two tests in parallel on the same node is an experimental feature and can result in unexpected outcomes.</p>
<b>EAGLSWPLAT-1282</b>	After restarting the management node, it could take up to 5 minutes for the KCOS Shell to be ready in the background even though the login prompt is displayed. Console might not start, or authentication might fail during this time.
<b>EAGLSWPLAT-1272</b>	If the kcos-framework-v1-nfs-server-provisioner is deleted, BreakingPoint will need to be reinstalled as it will no longer start (attaching the nfs-storage will fail to attach and it will be visible in the BPS pod description).
<b>EAGLSWPLAT-1187</b>	During initialization, while the BreakingPoint application does not have all services ready, the system will return a 503 or 404 Error page when trying to connect to it with a web browser. In some rare scenarios, when database corrections need to be made, it can take up to 1 hour for the BreakingPoint page to display.
<b>EAGLSWPLAT-1163</b>	On rare occasions, some compute nodes may become stuck while rebooting. Please power cycle the node if it takes more than 30 minutes to complete the rebooting process.

Reference #	Description
<b>EAGLSWPLAT-785</b>	Compute nodes need to start up in managed mode. They may start in unmanaged mode if the management node is not ready when the compute node is started. Both managed and unmanaged modes display the same login prompt but the compute nodes, when in managed mode (correct mode), will not enter the KCOS CLI after login. Only a management node will allow KCOS CLI functionality as a central administration node.
<b>EAGLSWPLAT-1295</b>	During startup there will be a pciehp link status and cdrom mount failed messages. Please ignore these harmless messages and continue to wait for the login prompt. The system is starting up in the background even if there is no information displayed for several minutes.
<b>EAGLSWPLAT-1296</b>	Setting the date back to earlier than September 2021 from the KCOS CLI will result in the system not being able to start again. Note that the user will not be able to reset the date as the CLI will not be accessible.