BreakingPoint Firmware Release Notes

Release 3.4.2, May 2015

Release Notes Version 1.2

Corporate Headquarters	Ixia Worldwide Headquarters 26601 W. Agoura Rd. Calabasas, CA 91302 USA +1 877 FOR IXIA (877 367 4942) +1 818 871 1800 (International) (FAX) +1 818 871 1805 sales@ixiacom.com	Web site: www.ixiacom.com General: info@ixiacom.com Investor Relations: ir@ixiacom.com Training: training@ixiacom.com Support: support@ixiacom.com +1 818 595 2599 For the online support form, go to: http://www.ixiacom.com/support/inquiry/
BreakingPoint Systems	Ixia BreakingPoint Systems 8310 N. Capital of Texas Hwy. Bldg 2, Ste. 100 Austin, TX 78731 USA +1 877 367 4942 info@breakingpoint.com	Web site: www.breakingpoint.com General: http://www.ixiacom.com/products Support: support-bps@ixiacom.com + 1 818 595 2599
EMEA	Ixia Technologies Europe Limited Part 2nd Floor Clarion House, Norreys Drive Maidenhead, UK SL6 4FL +44 (1628) 408750 FAX +44 (1628) 639916 salesemea@ixiacom.com	Support: eurosupport@ixiacom.com +40 21-3015699 For the online support form, go to: http://www.ixiacom.com/support/inquiry/?location=emea
Asia Pacific	Ixia Pte Ltd 210 Middle Road #08-01 IOI Plaza Singapore 188994	Support: support-asiapac@ixiacom.com +65 6332125 For the online support form, go to: http://www.ixiacom.com/support/inquiry/
Japan	Ixia Communications KK Nishi-Shinjuku Mitsui Bldg 11F 6-24-1, Nishi-Shinjuku, Shinjuku-ku Tokyo, 160-0023 Japan	Support: support-japan@ixiacom.com +81 3 5326 1948 For the online support form, go to: http://www.ixiacom.com/support/inquiry/
India	Technologies Pvt Ltd Tower 1, 7th Floor, UMIYA Business Bay Cessna Business Park Survey No. 10/1A, 10/2, 11 & 13/2 Outer Ring Road, Varthur Hobli Kadubeesanahalli Village Bangalore East Taluk Bangalore-560 037, Karnataka, India +91 80 42862600	Support: Support-India@ixiacom.com +91 80 49396400 For the online support form, go to: http://www.ixiacom.com/support/inquiry/?location=india

Table of Contents

Overview

Document Purpose

These release notes provide new information regarding the Breaking Point 3.4.2 release. This includes 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 or call them at 1-818 595 2599.

Documentation

The following table lists the latest documentation for all BreakingPoint products.

Document	Location
Ixia BreakingPoint Storm Installation Guide	https://strikecenter.ixiacom.com/docs/BPS_Storm_InstallationGuide_3.4.2
Ixia BreakingPoint Storm User Guide	https://strikecenter.ixiacom.com/docs/BPS_UserGuide_3.4.2.pdf
Ixia BreakingPoint FireStorm Installation Guide	https://strikecenter.ixiacom.com/docs/BPS_FS_InstallationGuide_3.4.2.pdf
Ixia BreakingPoint FireStorm User Guide	https://strikecenter.ixiacom.com/docs/BPS_FS_UserGuide_3.4.2.pdf
Ixia BreakingPoint FireStorm ONE Installation Guide	https://strikecenter.ixiacom.com/docs/BPS_FS_ONE_InstallationGuide_3.4.2.pdf
Ixia BreakingPoint FireStorm ONE User Guide	https://strikecenter.ixiacom.com/docs/BPS_FS_ONE_UserGuide_3.4.2.pdf
Ixia BreakingPoint 20 Installation Guide	https://strikecenter.ixiacom.com/docs/BPS_20_InstallationGuide_3.4.2.pdf

Ixia BreakingPoint 20 User Guide	https://strikecenter.ixiacom.com/docs/BPS_20_UserGuide_3.4.2.pdf
Ixia BreakingPoint PerfectStorm Fusion User Guide	https://strikecenter.ixiacom.com/docs/PS_UserGuide_3.4.2.pdf
Ixia BreakingPoint Virtual Edition (VE) Installation Guide	https://strikecenter.ixiacom.com/docs/BPS_VE_Install_Guide_3.4.2.pdf
Ixia BreakingPoint Virtual Edition (VE) User Guide	https://strikecenter.ixiacom.com/docs/BPS_VE_UserGuide_3.4.2.pdf

New Features

BreakingPoint 3.4.2 Firmware Release targets cross-platform (Storm, Firestorm and PerfectStorm, PerfectStorm ONE) quality improvements and introduces the following enhancements:

BreakingPoint VE (Virtual Edition) – Phase 2

Ixia's BreakingPoint VE provides scalable real-world application and threat simulation in an elastic deployment model by leveraging virtualization and industry-standard hardware platforms. This is the second major release of BreakingPoint VE which is focused on delivering a more robust deployment, expanded hypervisor support and performance optimization.

- 50% reduction of BPS-VE OVA size (8GB to ~4GB)
- KVM hypervisor support over CentOS and Ubuntu
- 40% improvement in performance of key metrics such as throughput, CPS, etc.
- More robust deployment with better error handling and tighter communication between the BreakingPoint vController and vBlade

Software Compatibility

BreakingPoint 3.4.2 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	Flix OS Software
Firestorm chassis (Storm, Firestorm, Firestorm20)	BreakingPoint 3.4.2	Not applicable	
Firestorm ONE appliance	BreakingPoint 3.4.2		
XGS12-HS chassis (PerfectStorm Load Modules)	BreakingPoint 3.4.2	IxOS 6.80 EA SP1	Flix OS 2.0.0.1
PerfectStorm ONE Fusion appliances	BreakingPoint 3.4.2	IxOS 6.80 EA SP1	Flix OS 2.0.0.1
BreakingPoint Virtual	BreakingPoint 3.4.2	Not Applicable	

Hardware Compatibility

The BreakingPoint 3.4.2 Release is supported on all hardware platforms and BreakingPoint VE.

3-slot Firestorm Chassis and Firestorm ONE appliance

Part Number	Description
981-0001	BreakingPoint Firestorm, 3-slot chassis
981-0058	BreakingPoint Firestorm ONE, 4-port 10/1 GigE SFP+ appliance
982-0001	BreakingPoint Firestorm 4-port 10/1GigE SFP+ blade
982-0021	BreakingPoint System Controller
982-0037	BreakingPoint Storm, 1 GigE 4-port blade
982-0026	BreakingPoint Storm, 1 GigE 8-port blade
982-0027	BreakingPoint Storm, 10 GigE 4-port blade
982-0040	BreakingPoint Firestorm 20, 20-port 10/1GigE SFP+ blade

12-slot XGS12 chassis and PerfectStorm Fusion Load Modules

Part Number	Description
940-0006	XGS12-HS 12-slot, Chassis Bundle
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 PerfectStorm platform, please refer to the Product Compatibility Matrix available on Ixia's website. An Ixia website account is required before accessing.

Browser Compatibility

Firmware Release 3.4.2 continues Ixia's transition to an HTML5-based architecture for the Ixia BreakingPoint user interface. Because earlier versions of Internet Explorer (versions 9 and below) have limited support for HTML5, Release 3.4.2 and later requires Internet Explorer users to use version 10 or higher.

Additionally, Safari 6.0.2 on Mac OS 10.8.2 and Safari for Windows are not supported. Mac users with OS 10.8.2 can use Firefox or Google Chrome as their browser. Ixia recommends that users of Firefox use version 18 or higher.

Opera is not supported.

Browser	Recommendation for Windows	Recommendation for Mac OS
Internet Explorer	Version 10 or higher	Not supported
Google Chrome	Version 36 or higher	Version 36 or higher
Firefox	Version 18 or higher	Version 31 or higher
Safari	Not supported	Not supported

Upgrading to Release 3.4.2

Before you upgrade to a new firmware release, please create a backup of your current system.

General Notes

Specific instructions for installation on PerfectStorm and FireStorm systems are contained in the sections below.

Backing Up the Ixia BreakingPoint to a NFS Server

This example uses an Ubuntu Linux computer and the Ixia BreakingPoint system.

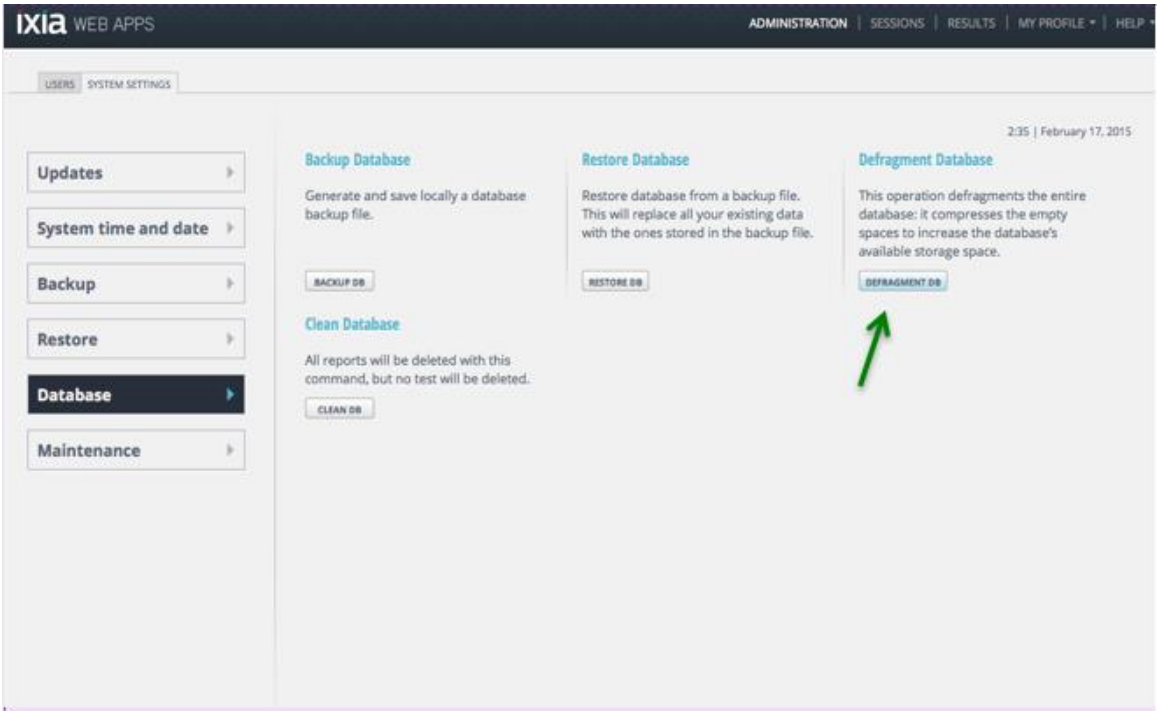
<u>Starting from the Linux computer:</u>

1. Download the required software
    a. sudo apt-get install nfs-kernel-server portmap
    b. sudo /etc/init.d/nfs-kernel-server start
2. Export the shared directory
    a. sudo mkdir /var/nfs/
    b. sudo chown nobody:nogroup /var/nfs

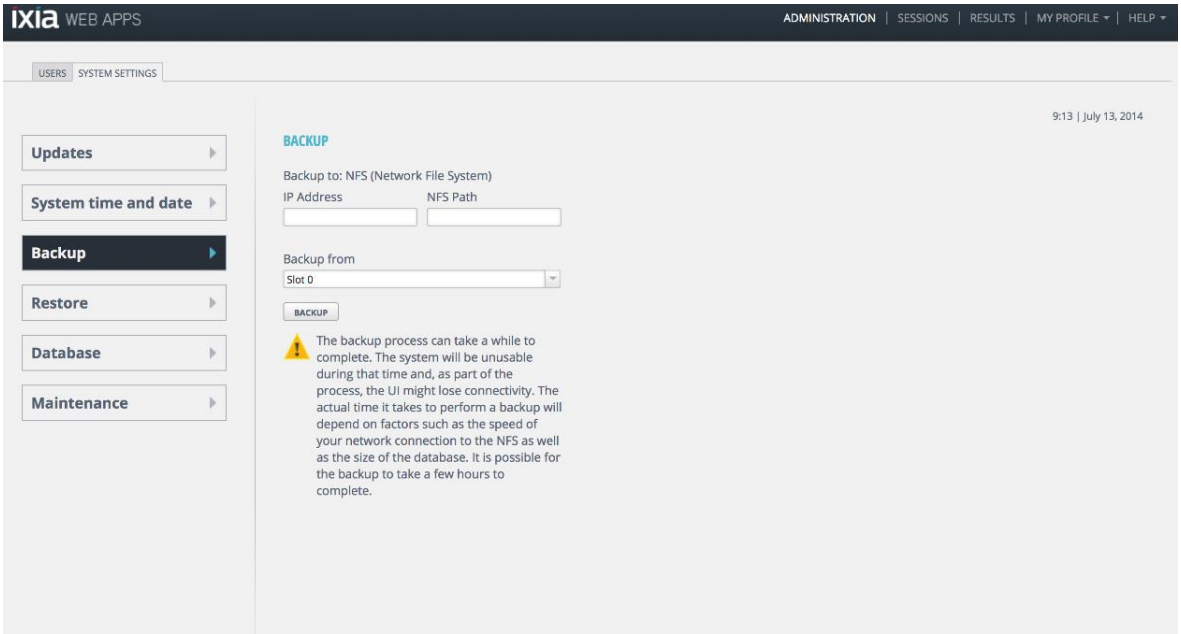
   c. sudo chmod 777 /var/nfs
3. Allow Directory Exporting
   a. sudo vi /etc/exports
4. Add the Following Line to /etc/exports
   a. /var/nfs 12.33.44.555(rw,sync,no_subtree_check)
5. Export the Shared Directory
   a. sudo exportfs -a

<u>Setup NFS Backup on the Ixia BreakingPoint System</u>

1. Log in to the Ixia BreakingPoint and navigate to **Database** within the Ixia Web Apps (Administration > System Settings).
2. Run the **Defragment Database** option (this may take some time to complete).

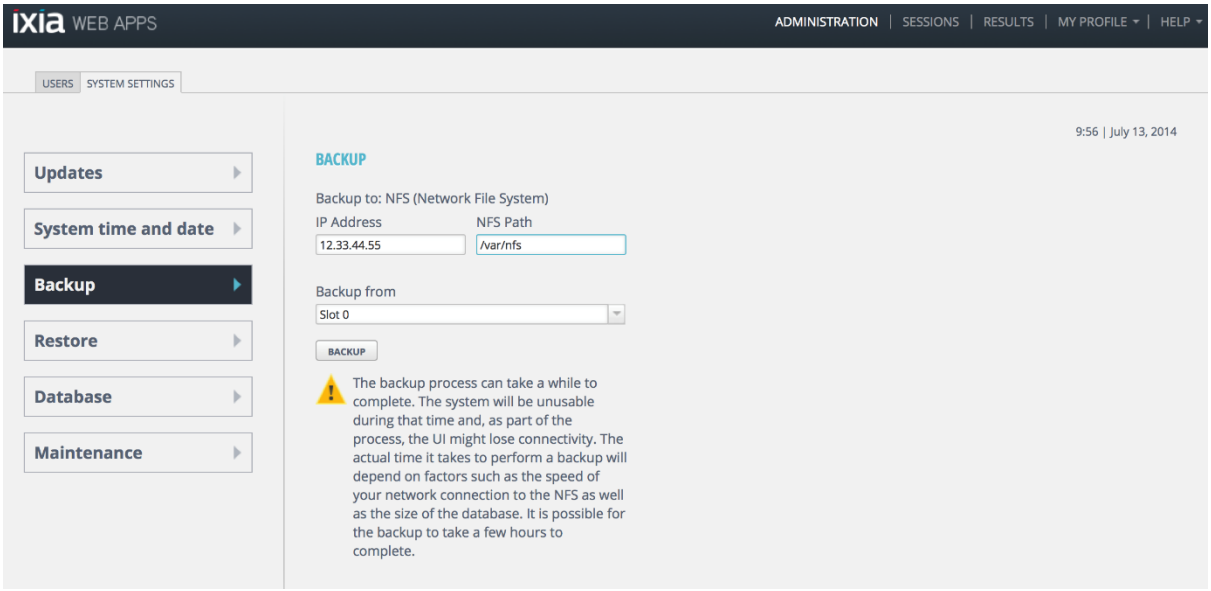


3. Log in to the Ixia BreakingPoint and navigate to **Backup** within the Ixia Web Apps:



4. Enter the IP address of the NFS Server and the Location of the Shared Directory:

    a. (example) IP Address: 12.33.44.55
    b. (example) NFS Path: /var/nfs
    c. (example) Backup From: Slot 0



Installation on BreakingPoint FireStorm

Ixia strongly recommends that you create backups of your system before upgrading to the 3.4.2 Firmware release *and* after upgrading to the 3.4.2 Firmware release.

Note: After upgrading to 3.4.1 and above, Backup and Restore to USB is supported on Firestorm and Firestorm ONE.

The table below describes the steps that are required to upgrade to 3.4.1 from earlier BPS Firmware releases.

Current BPS Firmware	Upgrade Path to BPS 3.4 Firmware
-> 3.4.1	-> 3.4.2
->3.4	->3.4.2
3.2, 3.3 or 3.3.1	-> 3.4.2
3.1	-> 3.3.1 -> 3.4.2
3.0	-> 3.2 -> 3.4.2

Note: During an update from 3.0, the user may encounter the following system error: "Nov 21 16:03:54 localhost [dbchecker] database connection not functional, restarting". This is a normal occurrence. Ignore the message and continue with the upgrade.

After upgrading the FireStorm system to version 3.4.2, you must restart the system. If you do not restart the system and run a test, the following error message displays: "`Could not open connection to sc0:aggregate_statistics`"

Upgrading multi-blade FireStorm systems to Release 3.4.2, requires installation of the new firmware to all Firestorm blades. For example, if the Ixia BreakingPoint software needs to upgrade a Firestorm in slots 0, 1, and 2, all blades must be checked before upgrading. The FireStorm in slot 0 will upgrade at a relatively shorter time than the Firestorms in slots 1 and 2.

Installation on XGS12-HS Chassis and PerfectStorm ONE Fusion Appliances

To install BreakingPoint 3.4.2, you must perform the following steps:

1. Upgrade the FLIX OS to version 2.0.0.1.
2. Upgrade the IxOS version 6.80 EA SP1.
3. Upgrade BreakingPoint software to firmware 3.4.2.
4. After the BreakingPoint software upgrade has completed, apply the Backup and Restore functionality command.

Note: This step is required for Backup and Restore functionality in BreakingPoint System 3.4.2.

a. ssh to the chassis WEB IP address and log in as `user: ixia, password: ixia`
b. run the following command:

```
sudo yum -y --disablerepo=* localinstall /home/ixia/flix/update/ixia-brsrv-patch-1.0.0-80.el6.noarch.rpm
```

Upgrading FLIX OS

In order to install BreakingPoint 3.4.2 on a XGS12-HS chassis the operating system running the chassis controller must be updated to FLIX OS 2.0.0.1. The update procedure is described in a document named "XGS12-HS FLIX OS Updatev2" which is available on the StrikeCenter BPS OS Updates site.

Note: New PerfectStorm and PerfectStorm ONE systems currently shipped to customers do not require a FLIX OS update. The systems ship with the latest FLIX OS version. Customers who currently use the PerfectStorm system must upgrade the FLIX OS.

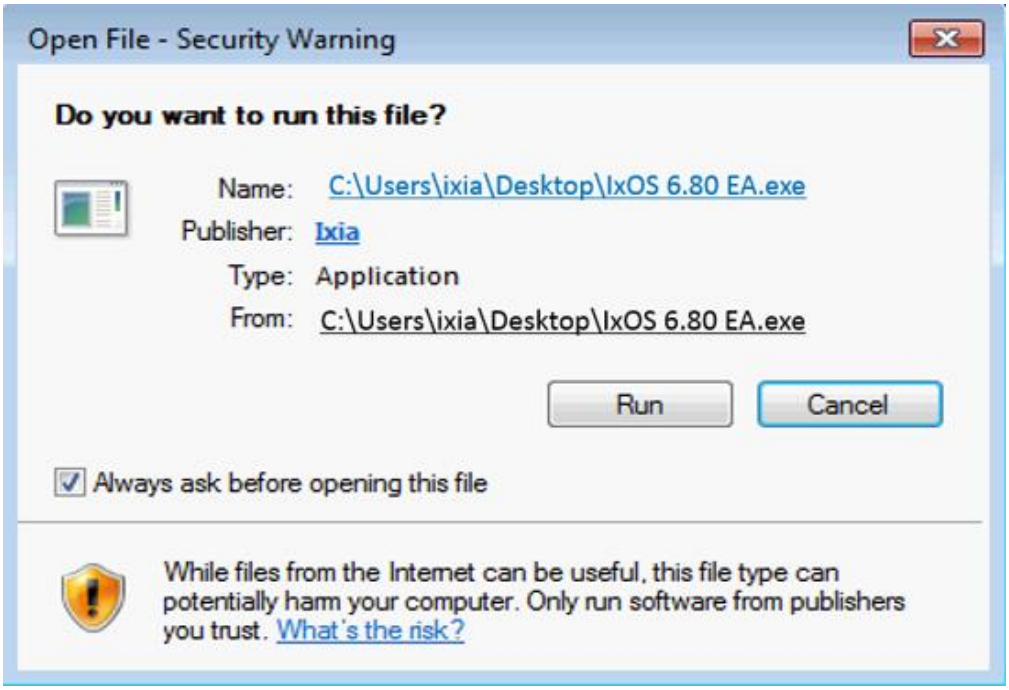
Upgrading IxOS 6.80 EA SP1

Software and Installation Instructions are located at the following location: http://www.ixiacom.com/support-overview/product-support/downloads-updates/versions/21

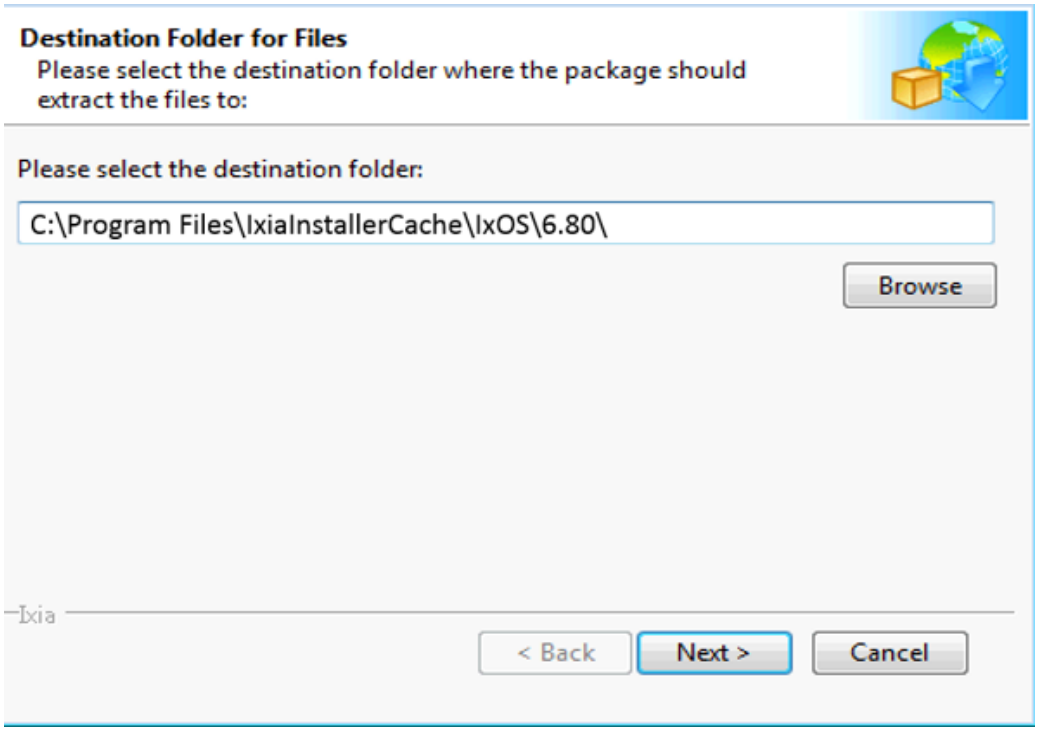
Note: The version numbers displayed in the images below may differ from the version numbers that are displayed when you upgrade IxOS 6.80 EA SP1.

Starting From the Windows VM:

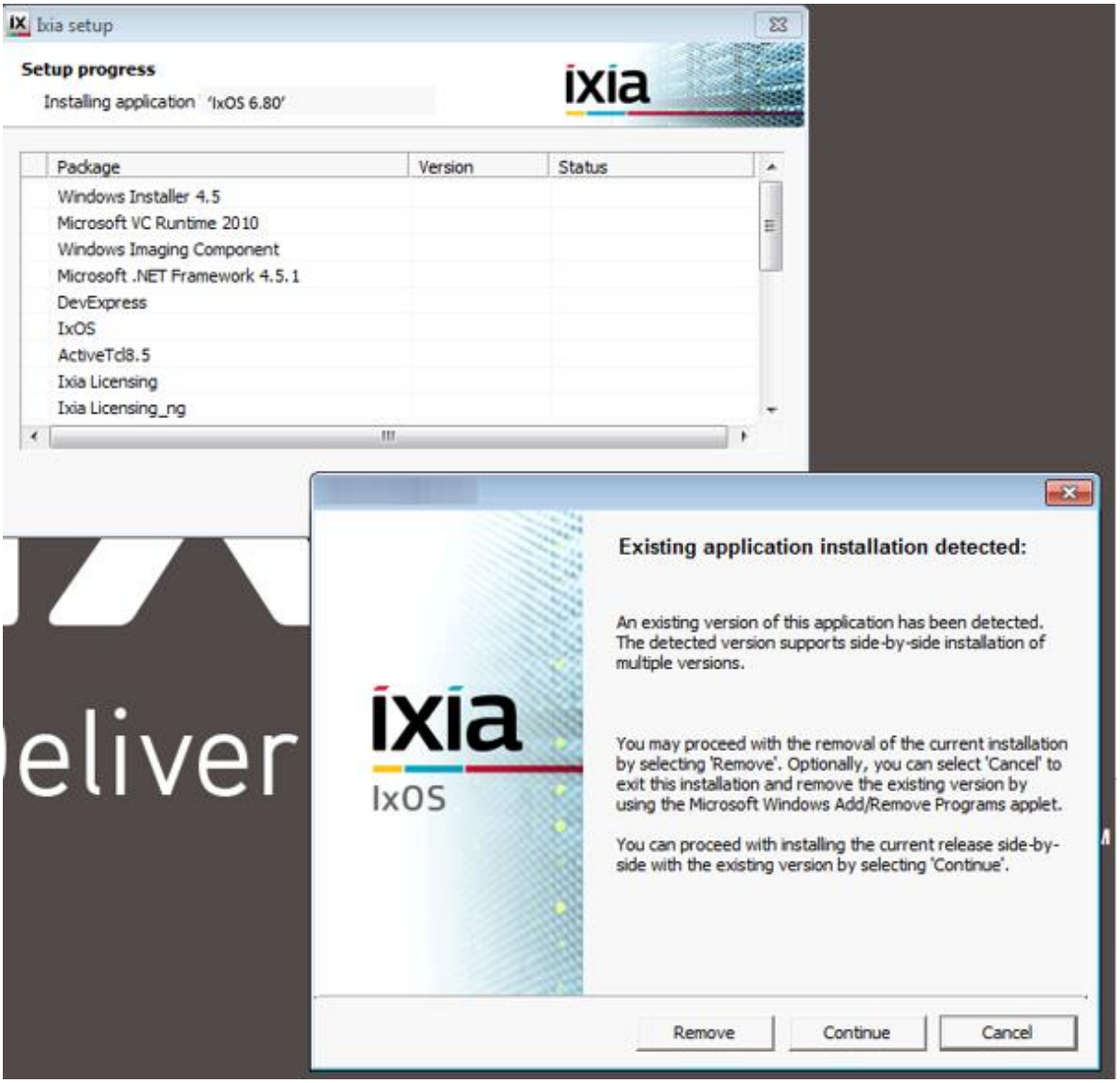
1. Open Remote Desktop and Login to the Ixia Windows VM.
2. Copy the IxOS executable to the Desktop.
   a. You may need to copy the *.exe file onto the Ixia Windows VM.
   b. The file can be directly downloaded on the VM using the link above.
   c. If no direct network access to ixiacom exists, then a shared file system with the Ixia Windows VM is needed to gain access to the VM.
3. Stop IxExplorer and IxServer.
   a. Use a graceful shutdown, File -> Exit
4. Run *.exe.



5. Click the **Run** button.

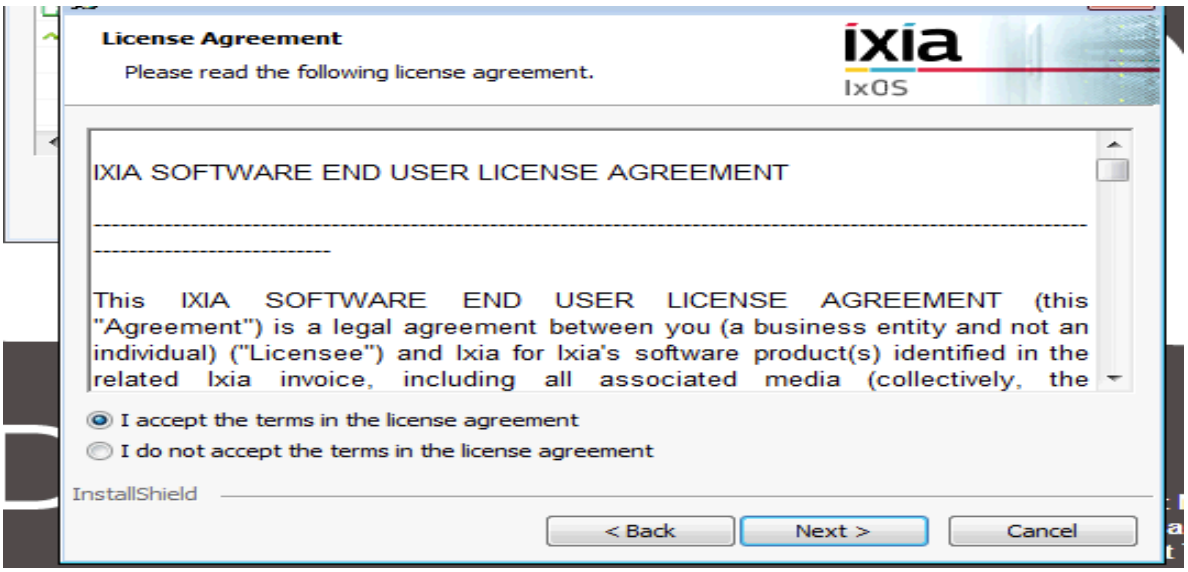


6. Accept the Default Destination Folder for the Installation. Click **Next**.

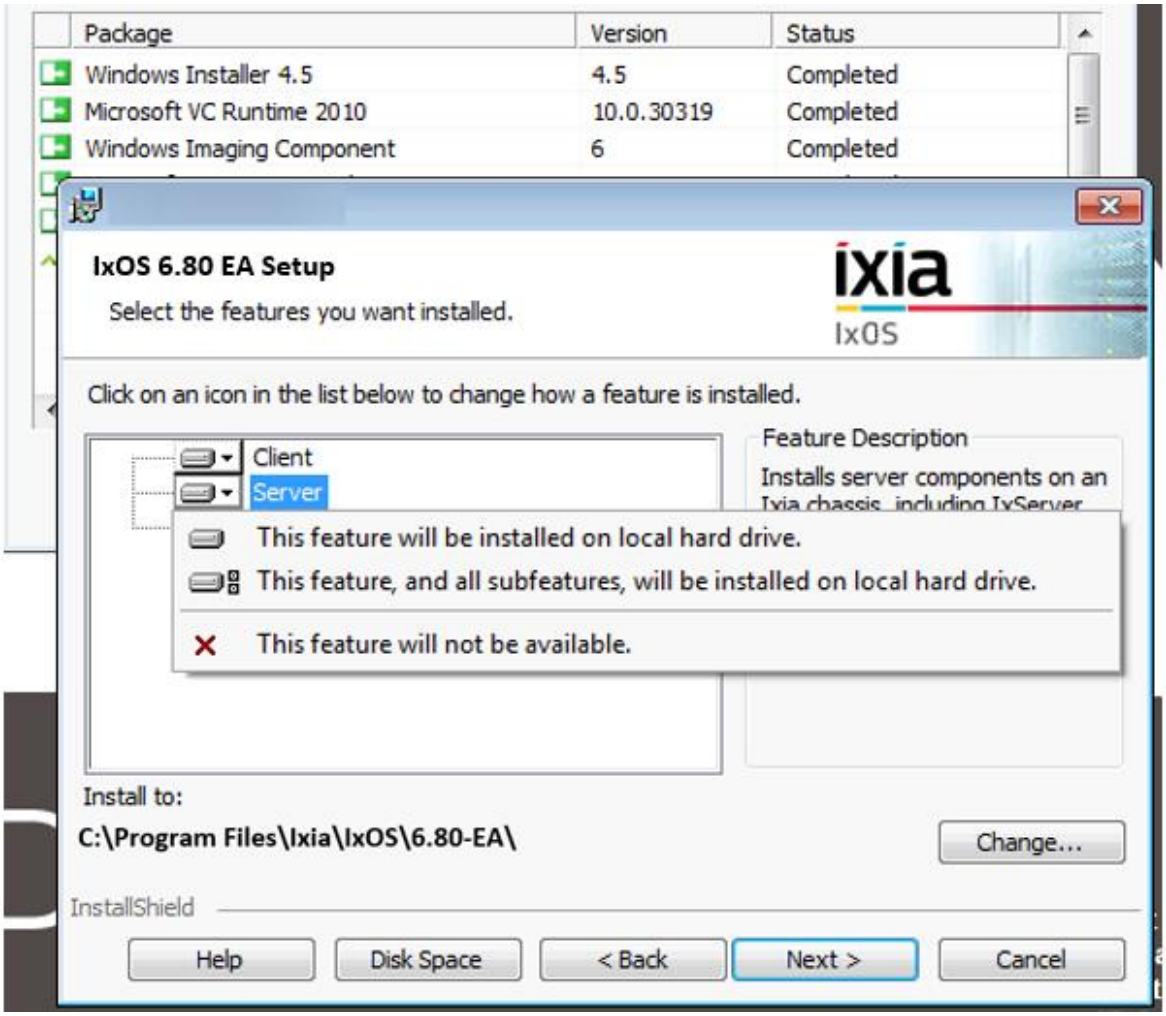


a. Select **Continue** on the "**Existing application Installation detected**:" window.

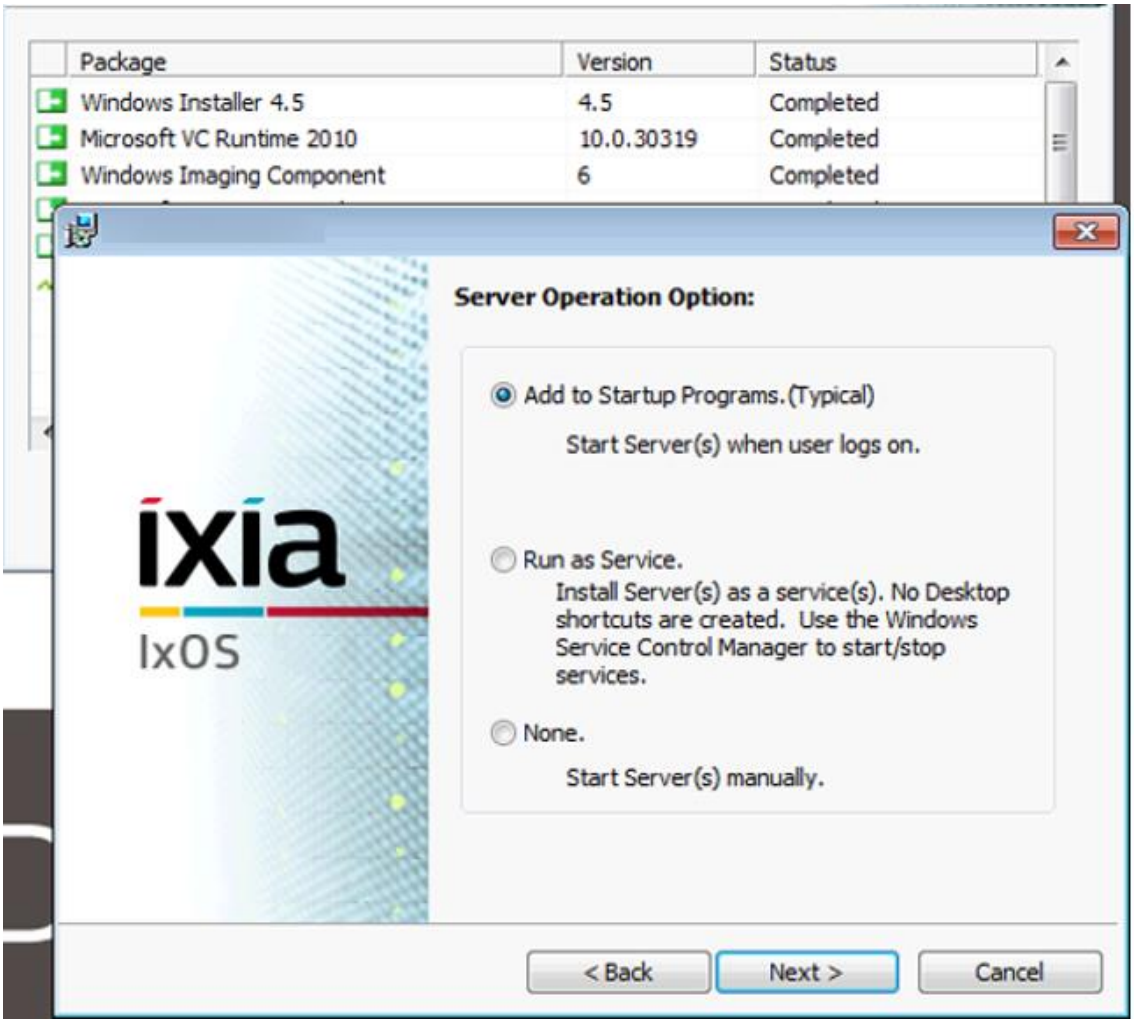
7. Click **Next** on the "**Welcome to the Setup for IxOS 6.80..**" window.



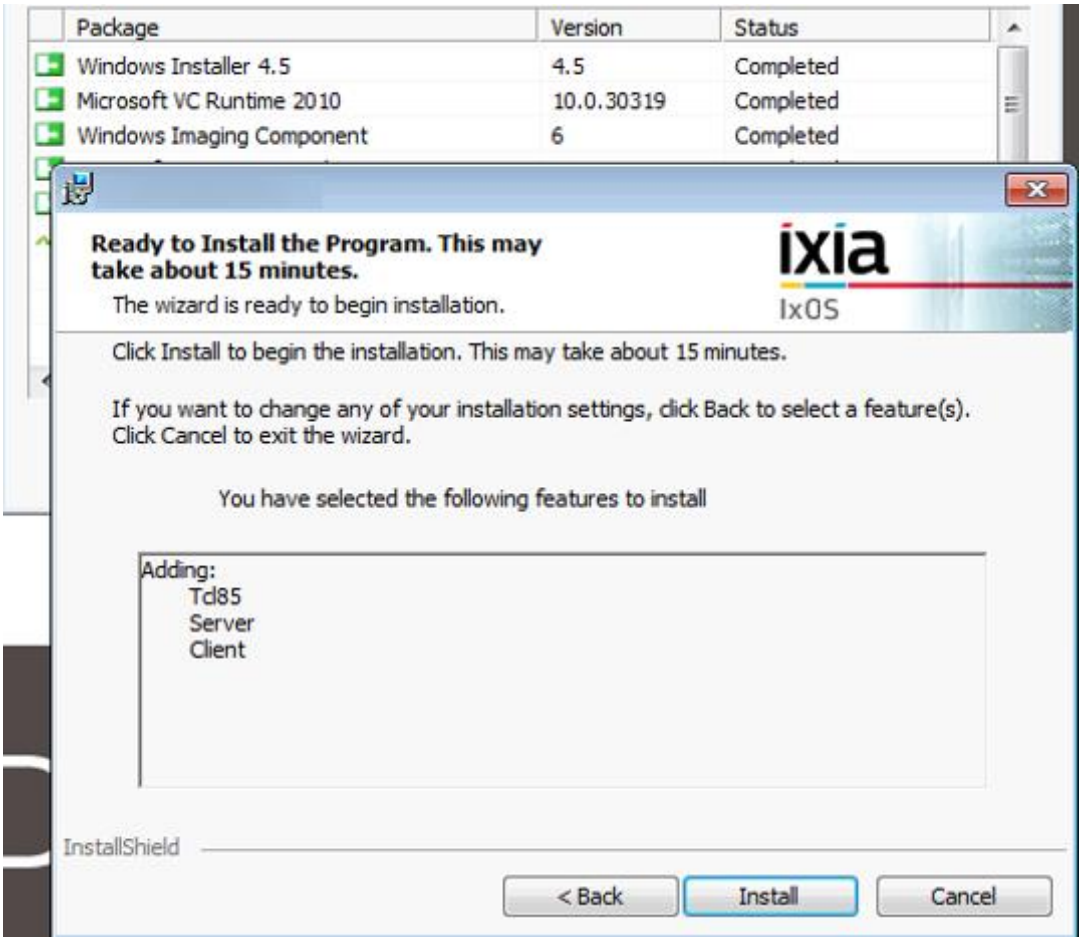
8. Accept the License Agreement, then select **Next**.



9. Set Client and Server to install and "**This feature, and all subfeatures, will be installed on local hard drive**", then select **Next**.
    a. Note: TCL server install is optional.



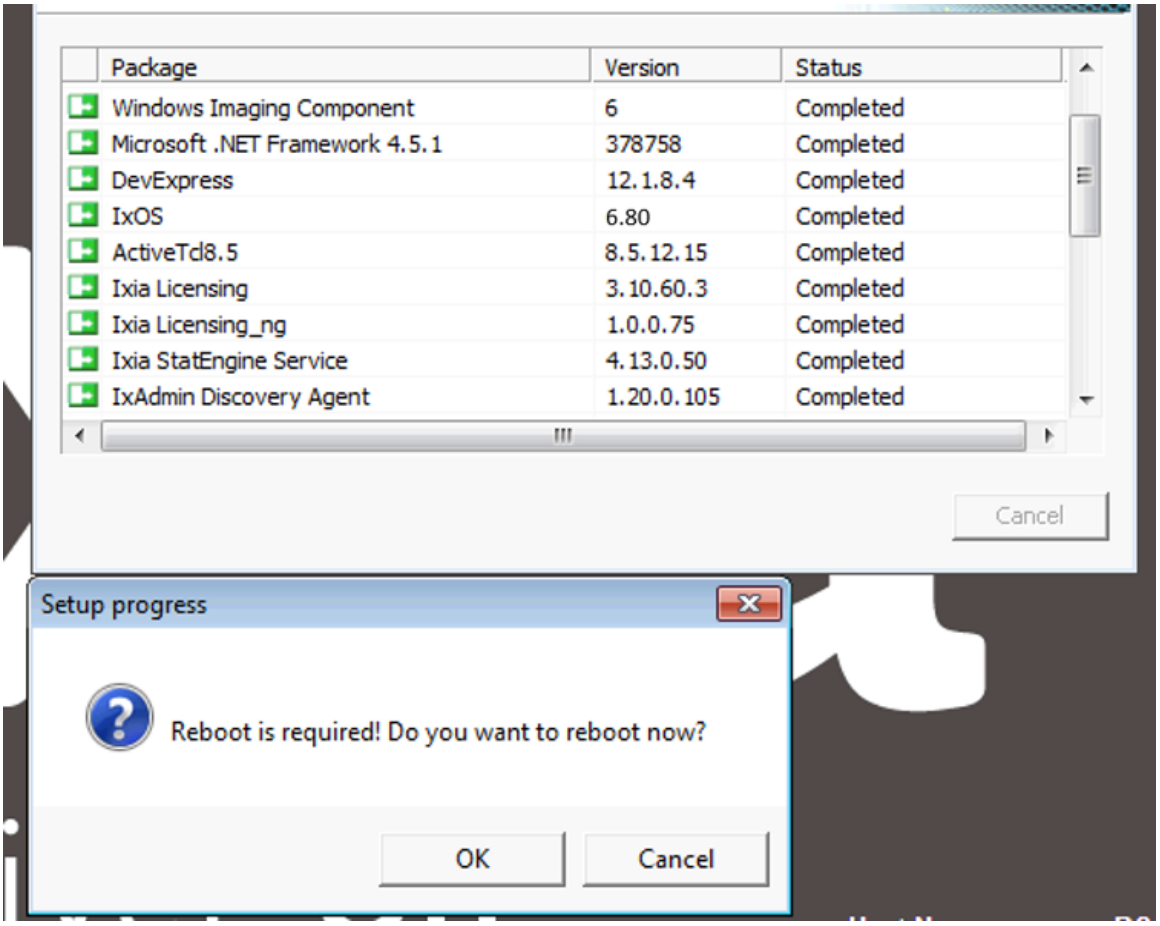
10. Select the following option: "**Add to Startup Programs.(Typical)",** then click **Next**.



11. After some essential components complete installation, the IxOS server will be ready to install, select **Install**.

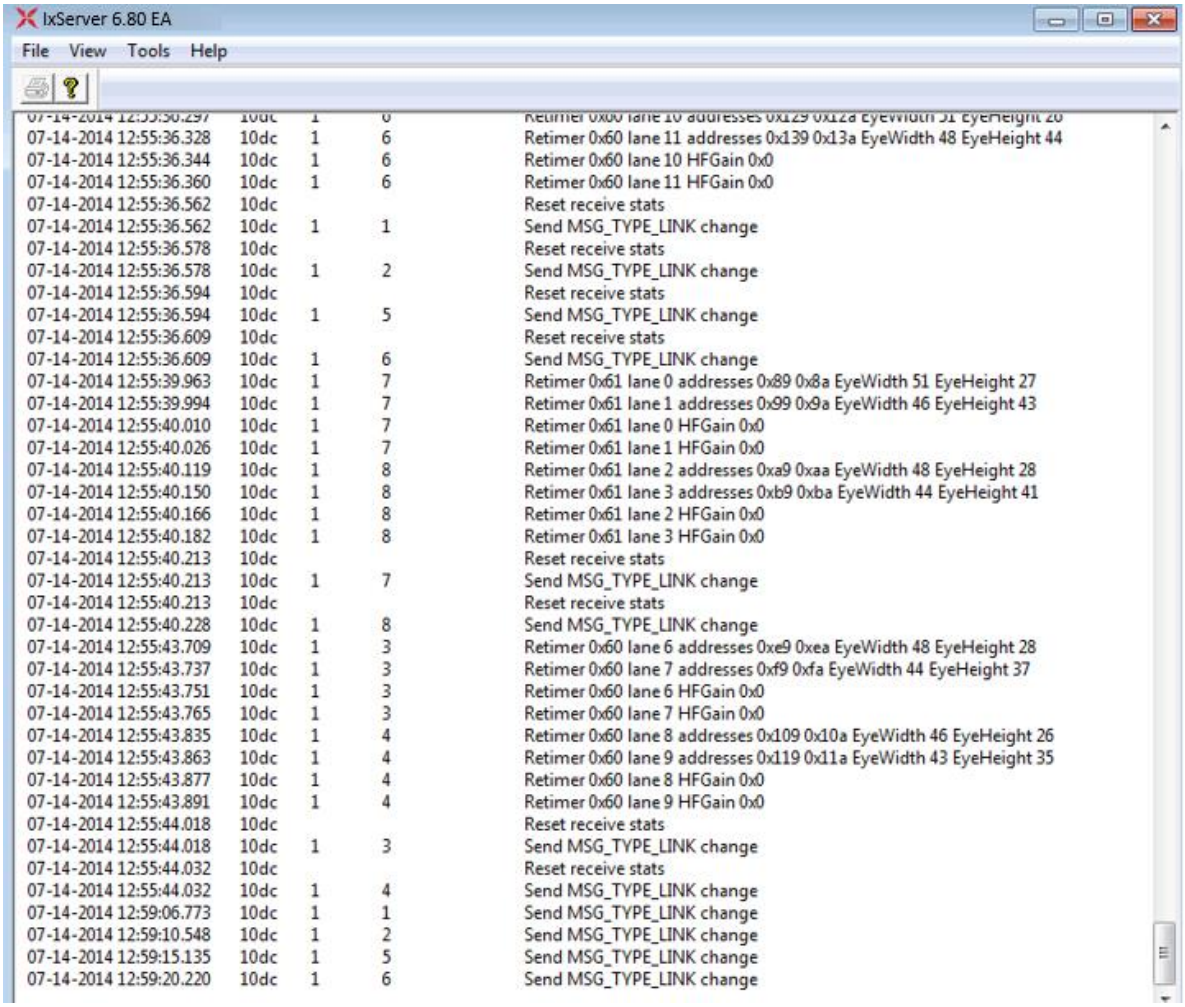
12. After several minutes of installation, new IxOS application links will be copied to the desktop.

13.After the installation has completed, click **Finish**.



14. The system will ask the user to reboot the Windows VM.
15. After the Windows VM reboots IxServer will start automatically and will continue setting up the system hardware.

    a. Note: Starting IxServer the first time after installation will be slower and may take more than 10 minutes for each slot to be prepared to run with the new IxOS version.

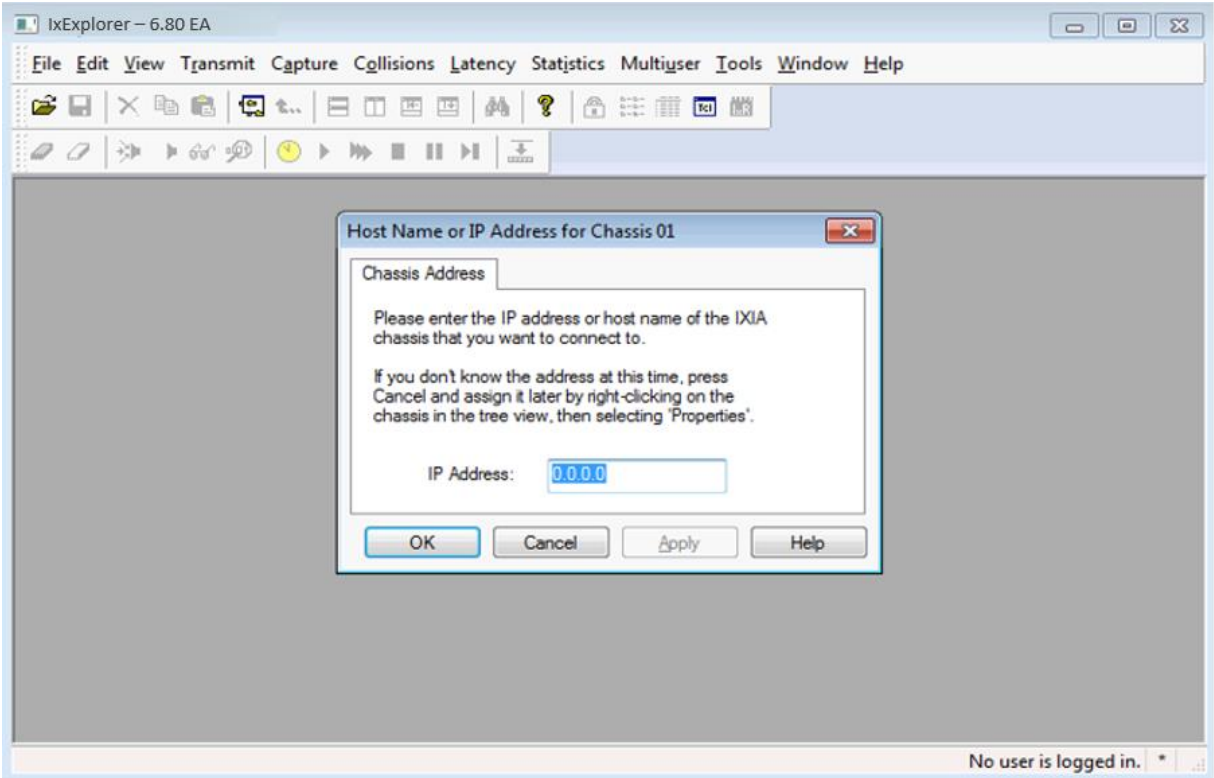


IxServer 6.80 EA

File View Tools Help

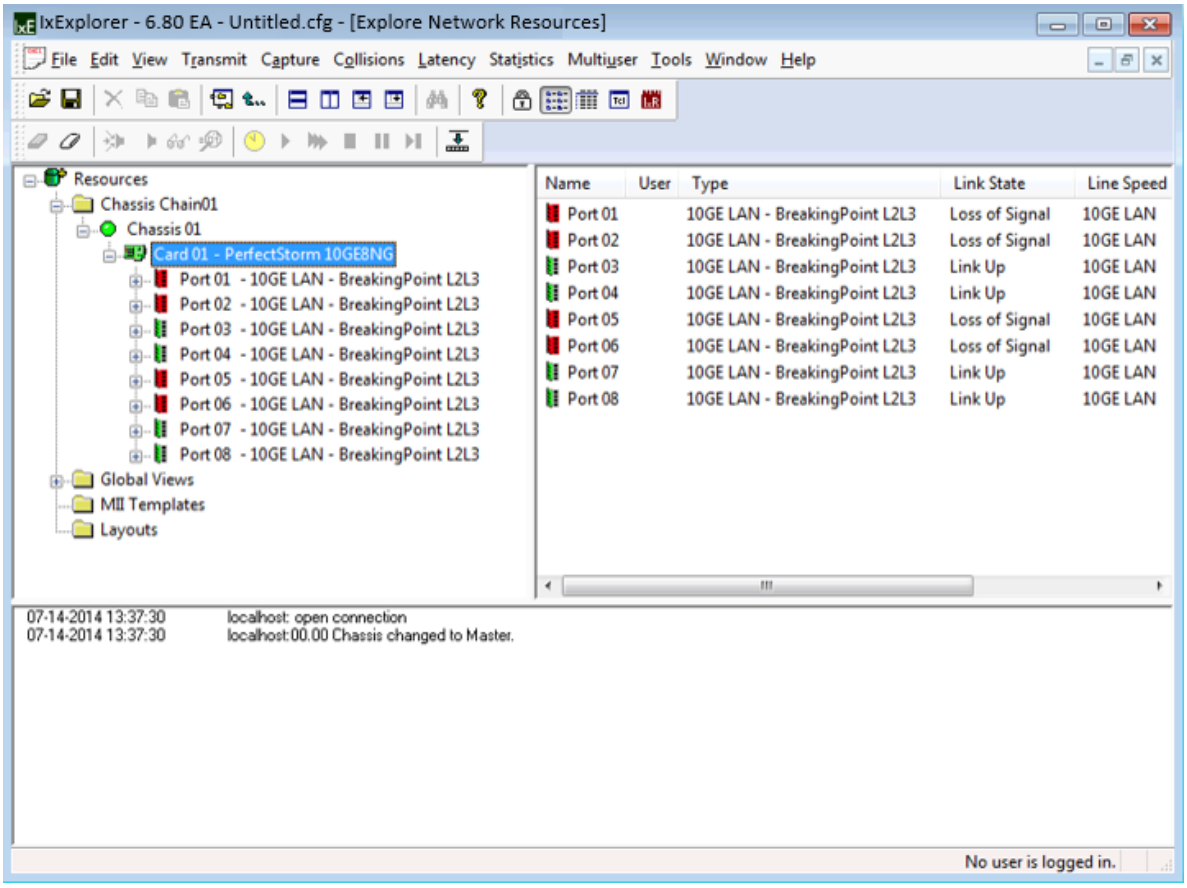
07-14-2014 12:55:36.297	10dc	1	6	Retimer 0x60 lane 10 addresses 0x129 0x12a EyeWidth 51 EyeHeight 26
07-14-2014 12:55:36.328	10dc	1	6	Retimer 0x60 lane 11 addresses 0x139 0x13a EyeWidth 48 EyeHeight 44
07-14-2014 12:55:36.344	10dc	1	6	Retimer 0x60 lane 10 HFGain 0x0
07-14-2014 12:55:36.360	10dc	1	6	Retimer 0x60 lane 11 HFGain 0x0
07-14-2014 12:55:36.562	10dc			Reset receive stats
07-14-2014 12:55:36.562	10dc	1	1	Send MSG_TYPE_LINK change
07-14-2014 12:55:36.578	10dc			Reset receive stats
07-14-2014 12:55:36.578	10dc	1	2	Send MSG_TYPE_LINK change
07-14-2014 12:55:36.594	10dc			Reset receive stats
07-14-2014 12:55:36.594	10dc	1	5	Send MSG_TYPE_LINK change
07-14-2014 12:55:36.609	10dc			Reset receive stats
07-14-2014 12:55:36.609	10dc	1	6	Send MSG_TYPE_LINK change
07-14-2014 12:55:39.963	10dc	1	7	Retimer 0x61 lane 0 addresses 0x89 0x8a EyeWidth 51 EyeHeight 27
07-14-2014 12:55:39.994	10dc	1	7	Retimer 0x61 lane 1 addresses 0x99 0x9a EyeWidth 46 EyeHeight 43
07-14-2014 12:55:40.010	10dc	1	7	Retimer 0x61 lane 0 HFGain 0x0
07-14-2014 12:55:40.026	10dc	1	7	Retimer 0x61 lane 1 HFGain 0x0
07-14-2014 12:55:40.119	10dc	1	8	Retimer 0x61 lane 2 addresses 0xa9 0xaa EyeWidth 48 EyeHeight 28
07-14-2014 12:55:40.150	10dc	1	8	Retimer 0x61 lane 3 addresses 0xb9 0xba EyeWidth 44 EyeHeight 41
07-14-2014 12:55:40.166	10dc	1	8	Retimer 0x61 lane 2 HFGain 0x0
07-14-2014 12:55:40.182	10dc	1	8	Retimer 0x61 lane 3 HFGain 0x0
07-14-2014 12:55:40.213	10dc			Reset receive stats
07-14-2014 12:55:40.213	10dc	1	7	Send MSG_TYPE_LINK change
07-14-2014 12:55:40.213	10dc			Reset receive stats
07-14-2014 12:55:40.228	10dc	1	8	Send MSG_TYPE_LINK change
07-14-2014 12:55:43.709	10dc	1	3	Retimer 0x60 lane 6 addresses 0xe9 0xea EyeWidth 48 EyeHeight 28
07-14-2014 12:55:43.737	10dc	1	3	Retimer 0x60 lane 7 addresses 0xf9 0xfa EyeWidth 44 EyeHeight 37
07-14-2014 12:55:43.751	10dc	1	3	Retimer 0x60 lane 6 HFGain 0x0
07-14-2014 12:55:43.765	10dc	1	3	Retimer 0x60 lane 7 HFGain 0x0
07-14-2014 12:55:43.835	10dc	1	4	Retimer 0x60 lane 8 addresses 0x109 0x10a EyeWidth 46 EyeHeight 26
07-14-2014 12:55:43.863	10dc	1	4	Retimer 0x60 lane 9 addresses 0x119 0x11a EyeWidth 43 EyeHeight 35
07-14-2014 12:55:43.877	10dc	1	4	Retimer 0x60 lane 8 HFGain 0x0
07-14-2014 12:55:43.891	10dc	1	4	Retimer 0x60 lane 9 HFGain 0x0
07-14-2014 12:55:44.018	10dc			Reset receive stats
07-14-2014 12:55:44.018	10dc	1	3	Send MSG_TYPE_LINK change
07-14-2014 12:55:44.032	10dc			Reset receive stats
07-14-2014 12:55:44.032	10dc	1	4	Send MSG_TYPE_LINK change
07-14-2014 12:59:06.773	10dc	1	1	Send MSG_TYPE_LINK change
07-14-2014 12:59:10.548	10dc	1	2	Send MSG_TYPE_LINK change
07-14-2014 12:59:15.135	10dc	1	5	Send MSG_TYPE_LINK change
07-14-2014 12:59:20.220	10dc	1	6	Send MSG_TYPE_LINK change

16. The image above shows an example of an IxServer that has completed initialization.



17. Then open IxExplorer and make sure that it is the same version as IxServer.
    a. In the **IP Address** field, type: `localhost`
    b. **Click OK.**

    Saving the configuration for a later time is optional, we selected **No** for this example.



18. IxExplorer will show the status of the blades connected to the chassis along with the mode they are running in.

    a. Seeing a green status indicator for Chassis indicates the blade is communicating with IxServer.
    b. Green Ports indicate Link Up status.
    c. Red Ports indicate Link Down status.

Upgrading Breaking Point System

To update the Ixia BreakingPoint System.

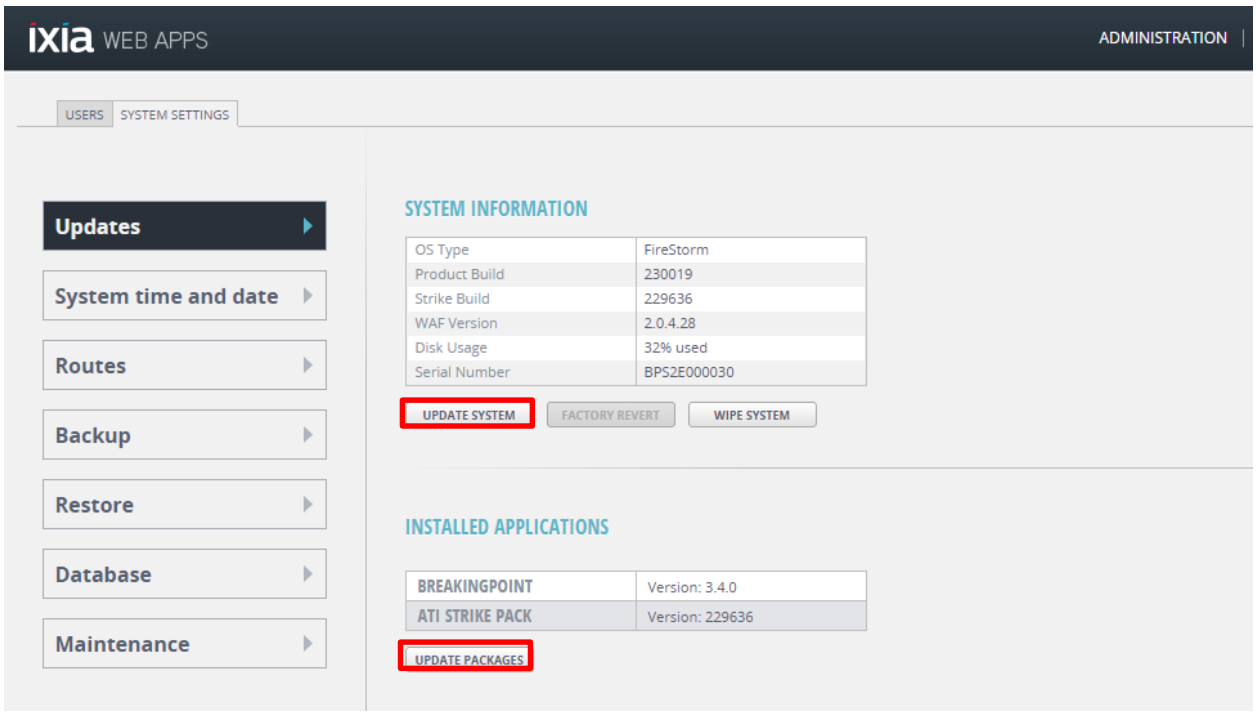
1. Download the required Ixia BreakingPoint image.
2. Login to the Ixia BreakingPoint System.
3. Navigate to **ADMINISTRATION -> SYSTEM SETTINGS -> Updates**.
4. Select **UPDATE SYSTEM** (see **figure 1** below).
5. Browse to the location of the BPS update file and select **OK**.
6. The BPS update will take 30-45 minutes to complete.

Update Packages

The Application and Threat Intelligence (ATI) program provides updates every 2 weeks ensuring delivery of the industry's most up to date application and threat intelligence.

We recommend that customers install the latest ATI update since some BPS issues are resolved by installing ATI updates (see **Update Packages** in **figure 1** below). ATI Update Packages are obtained from the ATI Strike Center at: https://strikecenter.ixiacom.com/bps/strikepacks.

Figure 1: Ixia WEB APPS Start Page



Switching to BreakingPoint Mode

All PerfectStorm Fusion load modules (blades) are capable of operating in IxLoad or BreakingPoint mode. When booting up, all PerfectStorm Fusion load modules default to IxLoad mode.

Note: Load modules retain the mode they were in prior to being rebooted.

On PerfectStorm (XGS12-HS), a red square in the upper right corner of the load module on the Device Status screen indicates that the module is in IxLoad mode. A green square indicates that the module is in BreakingPoint mode. On PerfectStorm ONE, the text "IxLoad Mode" at the bottom left side of the chassis on the Device Status screen indicates that the unit is in IxLoad mode. The text "Settings" indicates that the PerfectStorm ONE unit is in BreakingPoint mode.

To transition from IxLoad mode to BreakingPoint mode:

1. Click a port on the load module to begin the transition process. The **Reboot Slot** window will display.
2. Change the Slot Option setting to **Mode**. Select **BreakingPoint Mode** or **BreakingPoint L2/L3 Mode**.
3. Click **Apply** and wait for the mode change to complete.

Note: The transition from IxLoad mode to BreakingPoint mode takes approximately three minutes for each load module.

Note: To transition multiple load modules to BreakingPoint mode on PerfectStorm, each load module must be allowed to completely transition before the mode change process for the next load module can begin. Transitioning multiple modules simultaneously is prohibited.

Resolved Defects

The following tables list 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 or call them at 1-818 595-2599.

Table: Resolved Defects 3.4.2 Release

SR #	Description
651560	Resolved the issue where sending IPv6 traffic (specifically Router Advertisements) over an IPv4-only network degraded IPv4 traffic causing retransmissions and flow exceptions due to "too many retries".
660371	Fixed the issue where the Labs section in Admin only provides a Session Sender lab.
654618	Resolved the issue where Virtual Blade/ports cannot be seen on the Device Status screen after taking 3-5 minutes to successfully deploy.
649865	Resolved the issue that caused "Closed while expecting data" exceptions during loopback tests when the Delayed ACK option was enabled.
653633	Resolved the issue that caused "Gateway to Destination Unreachable" exceptions when running loopback tests on a blade in L2/L3 Mode.
641157	A force option has been added to the **chassis reservePort** Tcl command allowing the reservation of a port to be forced even if it is currently reserved.
658546	Fixed the issue where client tags configured with DHCP will not allow a connection from a client IP address to another IP address in the client's subnet.
651560	The large spike in CPU utilization that would occur while no BreakingPoint VE tests were running, has been dramatically reduced.

Known Defects

BreakingPoint Virtual Edition

The following section details the known defects of Firmware Release 3.4.2. 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 or call them at 1-818 595 2599.

Defect #	Description
BUG1341883	Network Configuration interfaces are not available when attempting to deploy a BreakingPoint VE vBlade on a KVM on CentOS. **Workaround:** The brctl command must be made available on the hypervisor in order for the available interfaces to be listed during vBlade deployment.
BUG1339594	On a KVM deployment, Reports do not display values for some Stack Scrambler statistics
BUG1338895	Initial attempt to get an IP address during vBlade deployment fails on a KVM. **Workaround:** Retry deployment. An IP address can be acquired upon retry.
BUG1345389	On a KVM deployment, Reports display RxFrameData & TxFrameData statistics that are not equal when they should be.
BUG1345446	On a KVM deployment, Maximum Throughput cannot be reached for Application Simulator SSL tests with jumbo frames.
BUG1346292	On a KVM deployment, tests that are configured with interfaces that have disabled MAC addresses or promiscuous mode disabled, can pass traffic when they should not be able to pass traffic.
BUG1343456	After the initial deployment of a vBlade on KVM, the default Transmit Queue Length (txqueuelen) value of the vBlade's virtual network is 12,000. Upon reboot of the vBlade, or deployment of additional vBlades, the txqueuelen value changes from 12,000 to 500 for all vBlade virtual networks. **Workaround:** Manually set the txqueuelen value to 12,000 using the ifconfig command.
BUG1343686	On a KVM deployment, after deleting a vBlade from the Administration menu in the BPS User Interface (UI), the option to "Remove virtual blades from selected slots" should not be available.
BUG1335470	The Security test component does not support IPv6 addresses starting with “0” in the first IP octet.
BUG1334581	IPv6 Virtual Router it is supported only in VMWare configurations that have the vSwitch configured with *promiscuous mode = accept*
BUG1334131	A manual reboot of the virtual machines associated with the vBlades may be required immediately after deployment if the vChassis fails to display the newly deployed blades.

BUG1333017	*ICMP Host Unreachable* errors are visible in test scenarios where a security test component is mixed with other test components. **Workaround**: Configure all test components to share the same virtual blade.
BUG1332493	No traffic generated when "Duplicate MAC Address" setting is disabled for interfaces configured to use VLAN **Workaround**: Enable the "Duplicate MAC Address" setting for interfaces that use a VLAN.
BUG1332358	While using certain pre-defined application superflows (e.g., BreakingPoint Bandwidth Netflix) the user may notice "Router Discard" messages reported (see Router Summary section of the BreakingPoint test report). These messages are due to a limitation of fragmented packet handling on the raw socket on the VMXNET3 driver.
BUG1332330	In some scenarios, the Administration tab will "gray out" when the user switches between the view of a currently running test and the Administration tab. **Workaround**: The user can access the Administration tab from the main menu or re-launch the BreakingPoint user interface.
BUG1331590	Given same test configuration, some test may result in longer start and stop times while using the BreakingPoint VE platform compared to the hardware platforms
BUG1328837	Harmless errors may be reported while loading a test configuration with features and test components that are not supported on BreakingPoint VE platform.
BUG1335470	The Security test component does not support IPv6 addresses starting with "0" in the first IP octet.
BUG1334581	IPv6 Virtual Router it is supported only in VMWare configurations that have the vSwitch configured with *promiscuous mode = accept*
BUG1334131	A manual reboot of the virtual machines associated with the vBlades may be required immediately after deployment if the vChassis fails to display the newly deployed blades.
BUG1333017	`ICMP Host Unreachable` errors are visible in test scenarios where a security test component is mixed with other test components. **Workaround**: Configure all test components to share the same virtual blade
BUG1332493	No traffic generated when "Duplicate MAC Address" setting is disabled for interfaces configured to use VLAN. **Workaround**: Enable the "Duplicate MAC Address" setting for interfaces that use VLAN.
BUG1332358	While using certain pre-defined application superflows (e.g., BreakingPoint Bandwidth Netflix) the user may notice "Router Discard" messages reported (see Router Summary section of the BreakingPoint test report). These messages are due to a limitation of fragmented packet handling on the raw socket on the VMXNET3 driver.

BUG1332330	In some scenarios, the Administration tab will “gray out” when the user switches between the view of a currently running test and the Administration tab. **Workaround**: The user can access the Administration tab from the main menu or re-launch the BreakingPoint user interface.
BUG1331590	Given same test configuration, some test may result in longer start and stop times while using the BreakingPoint VE platform compared to the hardware platforms.
BUG1328837	Harmless errors may be reported while loading a test configuration with features and test components that are not supported on BreakingPoint VE platform.
BUG1325399	In situations where the vSwitch detects a “link down” event triggered by an external device, BreakingPoint reports, `“Packet receive for Unconfirmed Address”. This condition is due to the vSwitch being configured to send notifications when links goes down.”` **Workaround**: The errors can be eliminated by configuring the vSwitch connecting the BreakingPoint vPorts to suppress the notification for link down. To change the setting, using vSphere set Notify Switches property to No (vSwitch Properties->NIC Teaming -> Notify Switches To "No").
BUG1321176	In a virtual environment where the vSwitch is configured with “Promiscuous Mode” set to “Accept” can result in situations where the reported TX bandwidth is much lower than RX bandwidth, while the test reports large number of TCP resets sent and received. This condition is triggered by the IP packets being broadcasted by the vSwitch to all interfaces. **Workaround**: This condition can be avoided by configuring the vSwitch with “Promiscuous Mode” set to “Reject” and by configuring the BreakingPoint Network Neighborhood to use “Duplicate MAC Address” option.
BUG1318949	While using Stack Scrambler component configured to generate IP packets corrupting the *IPv4 header length* field, the VM kernel drops IP packets for situations where the *IP header length* value is higher than the actual header data present in the buffer. For this situation, BreakingPoint cannot increment the *routerBadIPHeaderLength* statistic. In case of IPv4 header length corruption, there are 3 ways the header can be corrupted, and this condition is seen only in case 3: 1. IP header length is less than the RFC specified minimum IP header value 2. IP header length is more than the RFC specified maximum IP header value 3. IP header length is more than the actual header data present in the buffer.

BUG1135467	In reference to the RTP "Stream" actions in Application Manager process, the transaction flags can be described as: • Start - The transaction flag is applied to the first RTP packet in the stream. • End - The transaction flag is applied to the last RTP packet in the stream. • StartEnd - The Start transaction flag is assigned to the first RTP packet in the stream while the End transaction flag is assigned to the last RTP packet in the stream. When continuous mode is enabled on any RTP stream action, transactions are affected such that any End transaction flag will not be counted unless the stream is interrupted by way of the shared Stop RTP action.

PerfectStorm and PerfectStorm ONE Platforms

This section includes the list of known issues specific to PerfectStorm ONE Fusion appliances and XGS12-HS 12-slot chassis for PerfectStorm Load Modules.

Defect #	Description
BUG1332661	After changing the Internal Network from 10.0.x.x using IxExplorer, the user must restart the system using the BPS Web Interface Administration menu option available at: Administration -> System Settings -> Maintenance.
BUG1331965	For the same test configuration, the *SSL handshake* rate may translate in lower performance compared to previous releases due to the incorrect *TCP Delayed ACK* behavior seen in the previous releases.
BUG1328561	A single Routing Robot or Bit Blaster component can generate up to 10 Gbps. To achieve line rate on native 40GE QSFP+ interfaces, you must configure the test to include four test components. It is also recommended that the user selects *IP Address Algorithm* as *Performance* or *Increment* in the Routing Robot test settings.
BUG1322724	On PerfectStorm/PerfectStorm ONE 40GE hardware, *Routing Robot* and *Bit Blaster* tests cannot achieve line rate (80 Gbps) while using configuration settings that result in transmission of Ethernet frame with a size of 65, 66, 67 or 9000 bytes. In such conditions, the bandwidth will range between 77.7 to 79.9 Gbps depending on the configured frame size. Except for the four frames listed as an exception, the 2x40GE PerfectStorm hardware can achieve line rate 80 Gbps for all frame sizes including 64 byte frames

BUG1309644	The *Backup and Restore* of the BreakingPoint system may take several hours and its duration is directly dependent on the database size. Ixia recommends that you have at least a 1GE bandwidth link to the NFS Server.
ENH1326643	While using *card reboot* and/or *mode change* operations on PerfectStorm/PerfectStorm ONE the user receives no feedback regarding the progress of the operation. **Workaround:** After performing one of those operations, it is recommended to allow up to 3 minutes for the card to resume to its normal operation mode, before taking another action.
BUG1309768	Occasionally, after upgrading a PerfectStorm ONE Fusion appliance or an XGS12-HS 12-slot chassis to the latest IxOS version, the BreakingPoint Device Status screen may result in a condition where the interfaces are not displayed **Workaround**: Initiate a system reboot using *Administration -> System Settings -> Maintenance -> Restart System* option available in the web user interface

IPv6 Transitioning Protocols (DHCPv6, IPv6 SLAAC, DSLite)

Bug ID	Description
BUG1331106	For DHCPv6 server, when IAPD is selected, the start pool address should be configured with a valid DHCPv6 PD prefix (Example: 3001:1::).
BUG1329907	Multiple DHCPv6 servers cannot be directly connected to the same interface. However, multiple DHCPv6 serves can be directly connected to the same interface if each server is included in a different VLAN container.
BUG1329870	When using DHCPv6 Client, you might encounter TCP flows failures only if traffic is being sent before receiving Router Advertisements messages.
BUG1321500	Git Superflows over DS-lite elements are not supported.

Network Address Traversal

Bug ID	Description
BUG1327289	Certain flows when run through a DUT with a NAT configuration, will report flow failures (unsuccessful) in the Real Time statistics (RTS). Please contact Customer Support to get the full list of flows which are not currently supported with NAT configuration.
BUG1325110	The *Behind NAT* options in Network Neighborhood is not supported on BreakingPoint VE platform
BUG1324423	SIP/RTP, SIP/RTSP, FTP, AOL Mail Login/Logout, Amazon application Superflows and or protocols are not supported in NAT scenarios Please contact customer support for the full list of flows and protocols that experience this issue.