BreakingPoint Firmware Release Notes

Release 3.4, Jan. 2015

Release Notes Version 1.4

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 4

Document Purpose 4

Background 4

Technical Support 4

Documentation 4

New Features 5

BreakingPoint VE (Virtual Edition) 5

NAT/CGNAT and SLB Enhancements 6

Platform Enhancements 7

IPv6 Transitioning Protocols 8

Improved Threat Modeling Using Strike Variants 8

User Interface Enhancements 9

Automation Enhancements 9

Report Enhancements 10

Application and Threat Intelligence (ATI) 10

ATI: BreakingPoint 3.4, Application Support 10

ATI: New Predefined Superflows 11

Software Compatibility 12

Hardware Compatibility 12

Browser Compatibility 13

Upgrading to Release 3.4 14

General Notes 14

Upgrading Breaking Point System 30

Switching to BreakingPoint Mode 30

To transition from IxLoad mode to BreakingPoint mode: 30

Resolved Defects 31

Known Defects 33

BreakingPoint Virtual Edition 33

PerfectStorm and PerfectStorm ONE Platforms 36

IPv6 Transitioning Protocols (DHCPv6, IPv6 SLAAC, DSLite) 37

Network Address Traversal 37

Overview

Document Purpose

These release notes provide new information regarding the Breaking Point 3.4 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.pdf
Ixia BreakingPoint Storm User Guide	https://strikecenter.ixiacom.com/docs/BPS_UserGuide_3.4.pdf
Ixia BreakingPoint FireStorm Installation Guide	https://strikecenter.ixiacom.com/docs/BPS_FS_InstallationGuide_3.4.pdf
Ixia BreakingPoint FireStorm User Guide	https://strikecenter.ixiacom.com/docs/BPS_FS_UserGuide_3.4.pdf
Ixia BreakingPoint FireStorm ONE Installation Guide	https://strikecenter.ixiacom.com/docs/BPS_FS_ONE_InstallationGuide_3.4.pdf
Ixia BreakingPoint FireStorm ONE User Guide	https://strikecenter.ixiacom.com/docs/BPS_FS_ONE_UserGuide_3.4.pdf
Ixia BreakingPoint 20 Installation Guide	https://strikecenter.ixiacom.com/docs/BPS_20_InstallationGuide_3.4.pdf

Ixia BreakingPoint 20 User Guide	https://strikecenter.ixiacom.com/docs/BPS_20_UserGuide_3.4.pdf
Ixia BreakingPoint PerfectStorm Fusion User Guide	https://strikecenter.ixiacom.com/docs/PS_UserGuide_3.4.pdf

New Features

BreakingPoint 3.4 Firmware Release targets cross-platform (Storm, Firestorm and PerfectStorm, PerfectStorm ONE) quality improvements and introduces the following enhancements:

BreakingPoint VE (Virtual Edition)

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.

BreakingPoint VE – Platform Features

- VMware ESX/ESXi 5.5 hypervisor support
- Simple OVA deployment model
- HTML5 User Interface and Restful API support for vBlades deployment
- vBlades (Virtual Blades) configurable with up to 8 test interfaces per blade
- Up to 12 vBlades per vChassis (Virtual Chassis) / up to 96 virtual test interfaces
- vChassis supports vBlades deployed across multiple physical hosts
- 64-bit architecture
- Same ease of use workflow

BreakingPoint VE – Licensing Features

- Floating, annual subscription license sold in 1 Gbps increments, unlocks all supported features during active subscription term
- Elastic licensing model allows functional tests and performance tests
- Flexibility to quickly and easily move licenses between virtualized environments
- HTML 5 support for license management

BreakingPoint VE – Network Elements, Test Components and Labs

- Test Components
  - Application Simulator
  - Client Simulator
  - Session Sender
  - Security
  - Security NP
  - Stack Scrambler

- Network Neighborhood Elements
  - IPv4 Static Hosts
  - IPv6 Static Hosts
  - IPv4 External Hosts
  - IPv6 External Hosts
  - VLAN
  - IPv4 Router
  - IPv6 Router

- Session Sender Lab
- Software Packet Capture

NAT/CGNAT and SLB Enhancements

All BreakingPoint platforms benefit from multiple architectural improvements targeting NAT/CGNAT and SLB test scenarios.

- Optimizes the internal architecture of the connection table and flow look up mechanism to use full tuple instead of half tuple as used in previous releases, delivering the following benefits:

  - Eliminates wrong matches between packets and flows in some conditions, therefore eliminating the unnecessary resets and exceptions
  - Guarantees the new connections no longer wrongly match and disrupt existing established flows
  - Improved bandwidth performance, comparable to non-NAT scenario
  - The connection tuples can now be guaranteed to be unique and can be used to create, insert and lookup connections

- Better user-experience by eliminating the need to set the "Behind NAT" flag in Network Neighborhood for NAT scenarios

- Major flow scalability improvements that significantly reduces the number of IP addresses required to stress test devices such as firewalls

- Optimizes the connection table look up hash function to find the flow entries faster by performing a single full tuple look up instead of three
- Fixes to the TCP state machine to properly handle specific error scenarios in which the TCP state machine was not aging out certain entries, resulting in large number of stale entries, leading to scalability issues with load-balanced related tests

- Fixes to the TCP state machine to correct error scenarios in which the TCP state machine generated incorrectly RESET packets in certain states, resulting in large number of flow exceptions

Platform Enhancements

Security Fixes for All Hardware Platforms

- Security improvements for ShellShock vulnerability (CVE-2014-6271, CVE-2014-7169)

USB Factory Revert for Firestorm and Firestorm ONE

The 3.4 firmware enables the user interface functions to specify USB as the location of the backup image for the backup and restore functions. The option enables customers to:

- Use the USB via the TCL shell and the web user interface
- Perform a factory revert by performing a USB restore from a USB flash drive that contains a factory revert image.

PerfectStorm and PerfectStorm ONE – Platform Enhancements

Together with the Flix OS 2.0.0.1 and IxOS 6.80 EA releases, PerfectStorm (XGS12-HS chassis) and PerfectStorm ONE customers can benefit from the following platform enhancements:

- Optimized hardware access performance to significantly reduce the time of several common user operations including boot time, card reboot time and swap time operations
- Eliminated the restriction to use the 10.0.0.0/16 for chassis management, allowing users to configure the IxRemote IP network to x.y.0.0/16 using the IxExplorer application; networks 10.1.1/24 and 10.1.2/24 must still be avoided
- Added option to Flix OS administration menu to set system's time zone Flix OS admin menu > Set System Date and Time > Set timezone manually

- Improved "local" and "remote" Ixia account login
- Admin account improvements
- Fixes for setting times/dates starting with '8', '9'
- Fix to "halt system (graceful/forced)" operations – the network reconfiguration now re-asserts disabled of Wake-on-LAN)
- The NTP service no longer hangs if NTP server cannot be contacted or resolved

Full FPGA-based Features Parity for PerfectStorm / PerfectStorm ONE while Operating in Native 40GE QSFP+ Mode

BreakingPoint 3.4 Firmware Release closes the L23 feature gap for native 40GE interface, by adding the following capabilities:

- Bit Blaster
- Routing Robot
- RFC 2544 Lab
- Multicast Lab
- Resiliency Score Lab

BreakingPoint Firmware 3.3 release enabled this feature set for all hardware variants, including 10GE fan-out mode of the PerfectStorm PS40GE2NG load module and PerfectStorm ONE.

Network Impairment for PerfectStorm/PerfectStorm ONE

This release enables the legacy impairment features that are available on Storm/Firestorm product lines to all PerfectStorm Fusion load modules and PerfectStorm ONE Fusion appliances.

IPv6 Transitioning Protocols

All PerfectStorm Fusion and PerfectStorm ONE Fusion variants support the following IPv6 transitioning technologies:

- IPv6 SLAAC
- DSLite (Dual Stack Lite), B4 network element
- DSLite (Dual Stack Lite), Address Family Translation Router (AFTR) network element
- DHCPv6 client
- DHCPv6 server

Improved Threat Modeling Using Strike Variants

This release expands the support to control the behavior of a security strike by introducing *Strike Variants* group under *Security Evasion Profiles.* The new settings provide the following benefits:

- Better threat modeling by allowing execution of all strike variants in a single test
- Allows control of the strike payload ahead of execution
- Provides controls to run strike variants sequentially
- Expands threat realism by providing option to shuffle strike variants at runtime
- Allows selection of a subset of strike variants to be run (useful setting for strikes that support a high variant count – some strikes allows up to 300,000 unique strike variants)

To enable this feature you must have BreakingPoint 3.4 Firmware Release and ATI-2015-01 strike pack update or later.

User Interface Enhancements

HTML 5 User Interface

This release continues the transition to HTML 5 for several user interface screens including:

- Strike List Manager
- RFC 2544 Lab
- Session Sender Lab
- Test Criteria
- Administration page (Control Center)

Strike List Manager Enhancements

- Exposed strike severity and added option to search by severity
- Display and search for new strike variant metadata attribute
- Improved usability by allowing operations with groups of strikes (strike multi-selection, add/remove strike selection, add/remove all strikes)
- Added support to search for strike variants

Other User Interface Enhancements

- Added option to save and manage Session Sender Labs
- Added option to save and manage RFC 2544 Labs
- Added option to RFC 2544 Lab to start with “Maximum Throughput” test first
- Added option to minimize results data collection by controlling the statistics polling interval
- Added option to update settings simultaneously across multiple test components
- Added option to quickly enable/disable multiple test components
- Added option to display the PerfectStorm ONE serial number
- Added preset value of 40 Gbps for the "Device Capacity" field for Resilience Lab

Automation Enhancements

- Restful API support for BreakingPoint VE deployment
- TCL support to allow user to create custom report for section ID’s

Report Enhancements

- Added *% of packets* in addition to raw numbers to Routing Robot test reports
- Added per interface stats for data rate summary section
- Update reporting for "Strike Variants" feature

Application and Threat Intelligence (ATI)

The Application and Threat Intelligence (ATI) program provides comprehensive and current application protocols and attacks. This year, the ATI program enabled customers with an active ATI subscription to have timely access to:

- 60 new applications
- 571 new strike attacks
- 400 additional malware strikes (live malware strikepacks)
- Monthly updates for "Evergreen Applications"

BreakingPoint 3.4 firmware release provides access to:

- 38,238 strikes (malware and exploits)
- 3,283 predefined application superflows
- 290 applications

The Ixia BreakingPoint Application and Threat Intelligence (ATI) program provides bi-weekly updates of the latest application protocols and attacks for use with Ixia platforms. Leverage ATI subscription service to stay ahead of attacks and use the latest application definitions.

ATI: BreakingPoint 3.4, Application Support

- 050 plus
- Dropbox
- DTLS
- Hulu Desktop
- Instagram (version 6.2.0 for iOS 8.1)
- Multicast DNS (Apple Bonjour)
- MXIT Desktop (Desktop version of South African Mobile Social Network)
- Port Control Protocol v2 (PCPv2)
- SOCKS 5
- Team Viewer
- World of Warcraft

ATI: New Predefined Superflows

The ATI selection included with this release note is a subset of all the features and enhancements published through our ATI program on a bi-weekly basis. For a complete list, please review the individual release notes for each ATI update posted to https://strikecenter.ixiacom.com/

Key Highlights

- Hulu Desktop
- Dropbox Demo Superflow
- Dropbox Sync/Get New File
- Dropbox Sync/Upload New File
- Dropbox Initial Client Setup and Synchronization
- Google Calendar Aug 14
- SharePoint Sep 2014
- TeamViewer Initial Startup
- TeamViewer Remote Desktop Session
- Instagram Nov. 2014
- DNS Fast Flux superflow
- PCPv2 Map Request
- PCPv2 Map Request Prefix64
- RADIUS IPv4 and IPv6
- Mxit Desktop File Transfer
- Mxit Desktop Multiple Status Messages
- Mxit Messenger For Windows PC
- FTP Extended Passive Over NAT with ALGS check
- SOCKS 5 Connect No User Authentication
- SOCKS 5 Connect with User Authentication
- DTLS 1.0 Simple Session
- DTLS 1.2 Simple Session
- Multicast DNS Demo Superflow
- 050 Plus Call
- 050 Plus Unanswered Call
- ClientSim RADIUS CHAP Authentication
- World of Warcraft
- World of Warcraft Patch Update
- GTPoIPSec HTTP LTE
- GTPoIPSec HTTP Simple

Software Compatibility

BreakingPoint 3.4 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	Not applicable	
Firestorm ONE appliance	BreakingPoint 3.4		
XGS12-HS chassis (PerfectStorm Load Modules)	BreakingPoint 3.4	IxOS 6.80 EA	Flix OS 2.0.0.1
PerfectStorm ONE Fusion appliances	BreakingPoint 3.4	IxOS 6.80 EA	Flix OS 2.0.0.1
BreakingPoint Virtual	BreakingPoint 3.4	Not Applicable	

Hardware Compatibility

BreakingPoint 3.4 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)

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 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 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

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

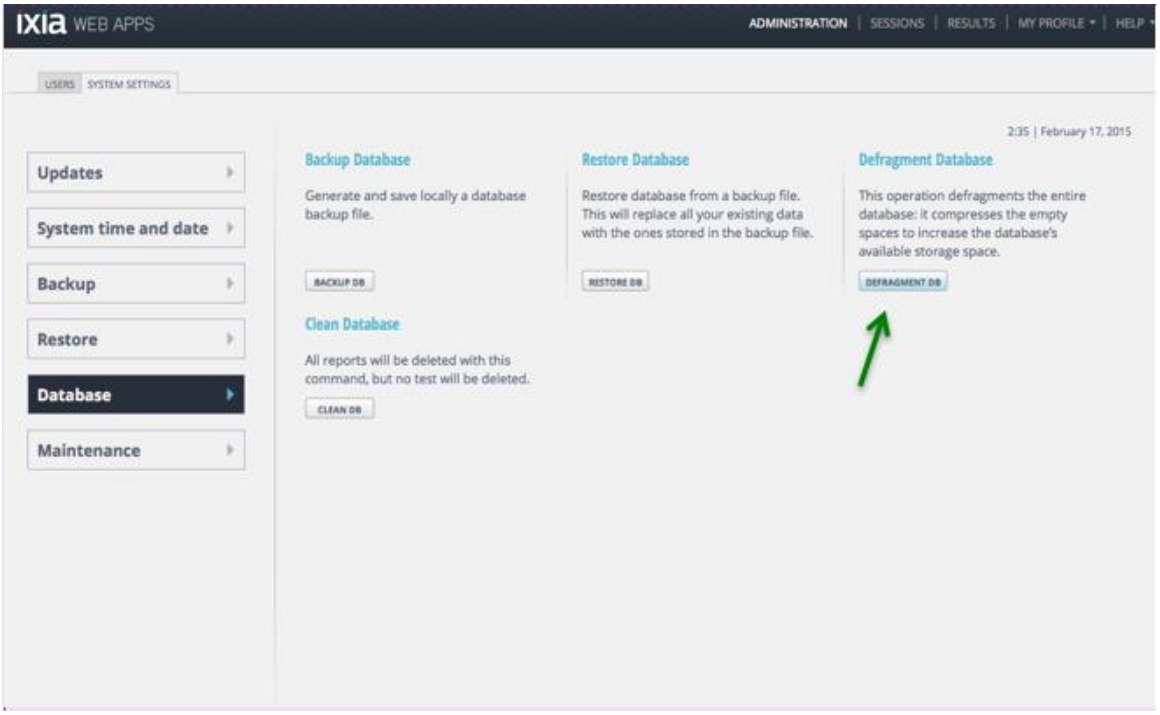
This example uses an Ubuntu Linux computer and the Ixia BreakingPoint system.

Starting from the Linux computer:

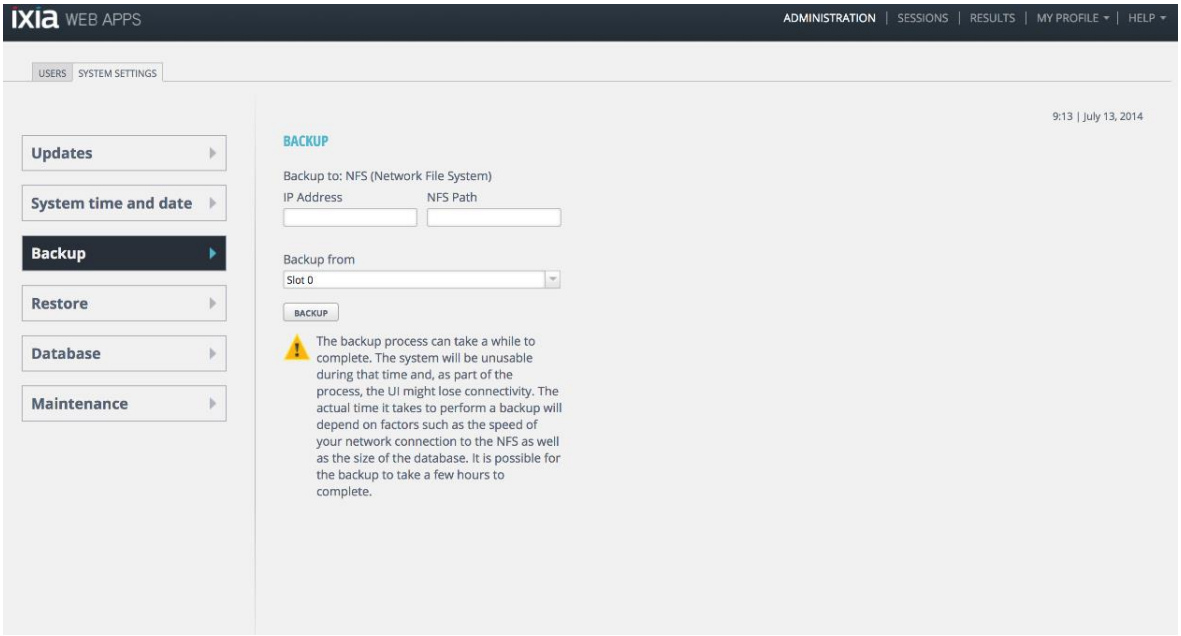
1. Download the required software
    a. sudo apt-get install nfs-kernel-server portmap
    b. sudo /etc/init.d/nfs-kernel-server start
2. Export the shared directory
    a. sudo mkdir /var/nfs/
    b. sudo chown nobody:nogroup /var/nfs
    c. sudo chmod 777 /var/nfs
3. Allow Directory Exporting
    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

Setup NFS Backup on the Ixia BreakingPoint System

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).

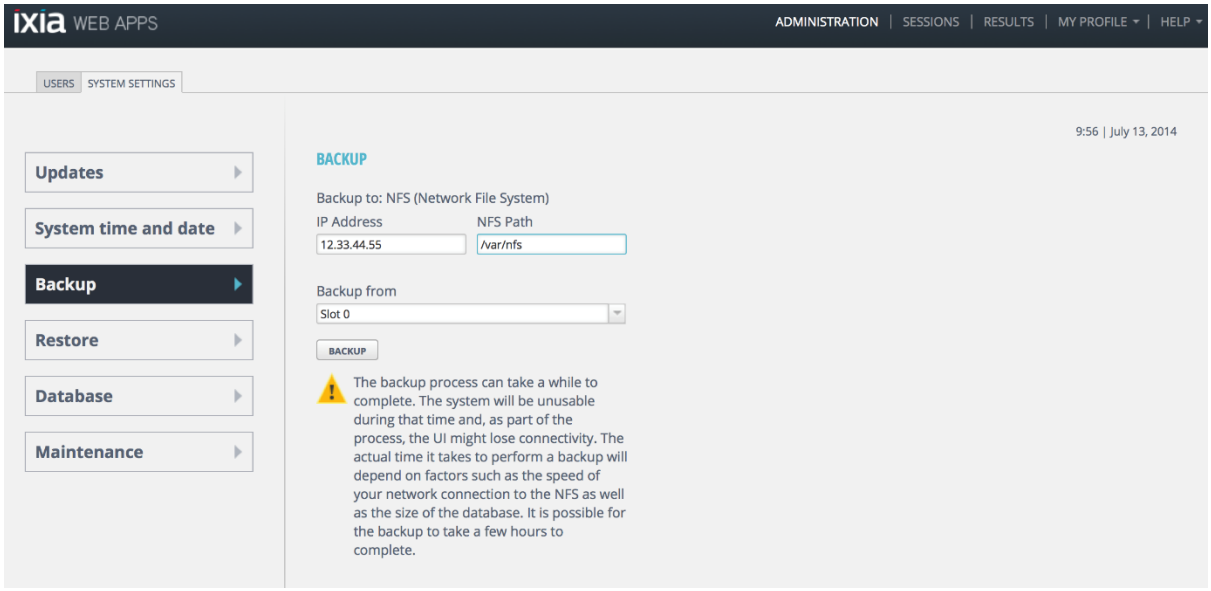


3. Log in to the Ixia BreakingPoint and navigate to **Backup** within the Ixia Web Apps:



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 Firmware release *and* after upgrading to the 3.4 Firmware release.

Note: After upgrading to 3.4, 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 from earlier BPS Firmware releases.

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

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, 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, 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, you must perform the following steps:

1. Upgrade the FLIX OS to version 2.0.0.1.
2. Upgrade the IxOS version IxOS 6.80 EA
3. Upgrade BreakingPoint software to firmware 3.4.
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.

   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 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.

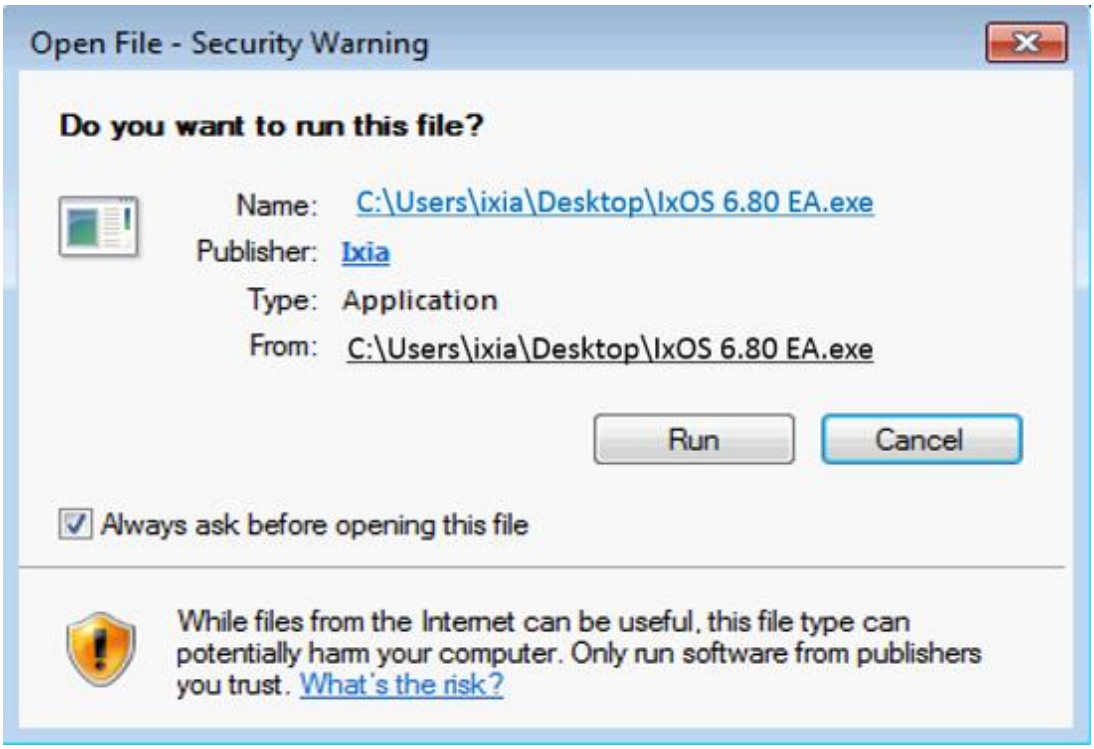
Upgrading IxOS 6.80 EA

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

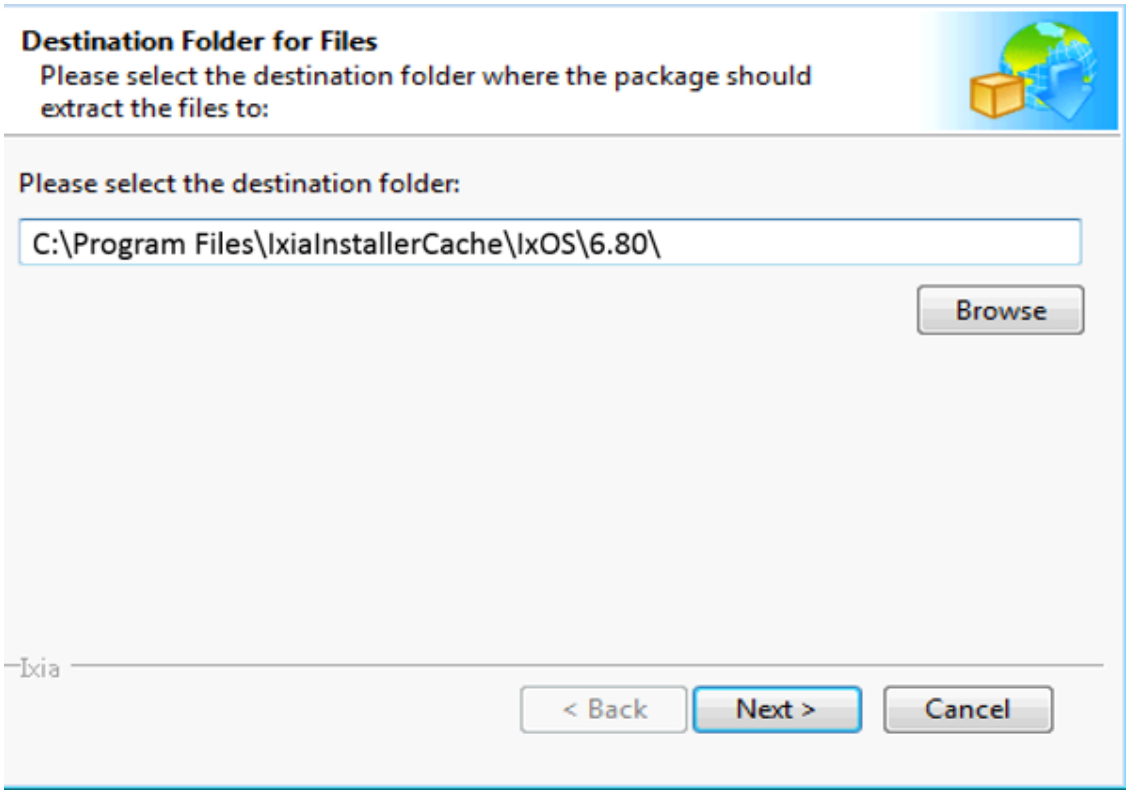
Note: The version numbers displayed in the images below may differ from the version numbers that are displayed when you upgrade IxOS 6.80 EA.

Starting From the Windows VM:

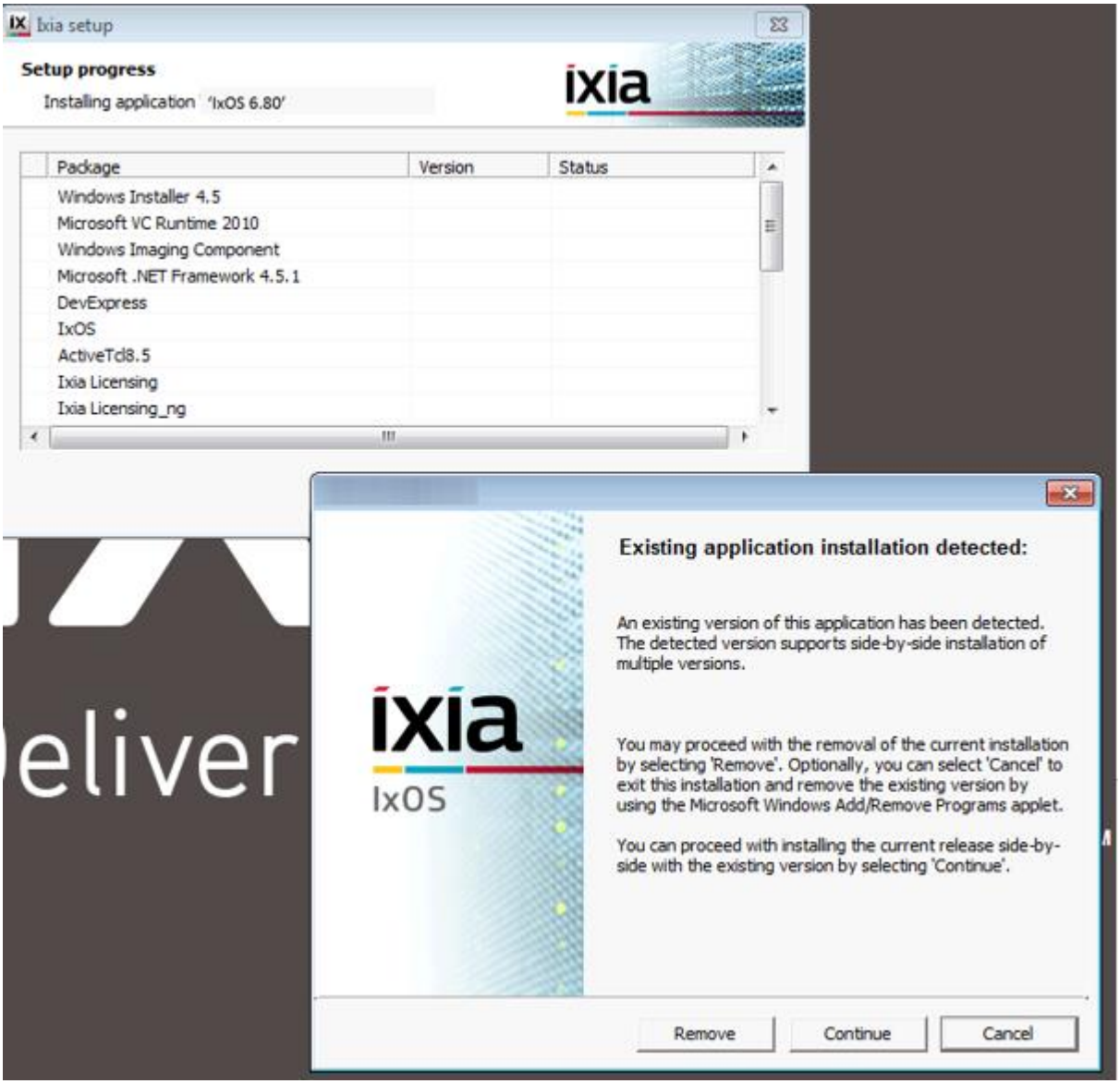
1. Open Remote Desktop and Login to the Ixia Windows VM.
2. Copy the IxOS executable to the Desktop.
    a. You may need to copy the *.exe file onto the Ixia Windows VM.
    b. The file can be directly downloaded on the VM using the link above.
    c. If no direct network access to ixiacom exists, then 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.



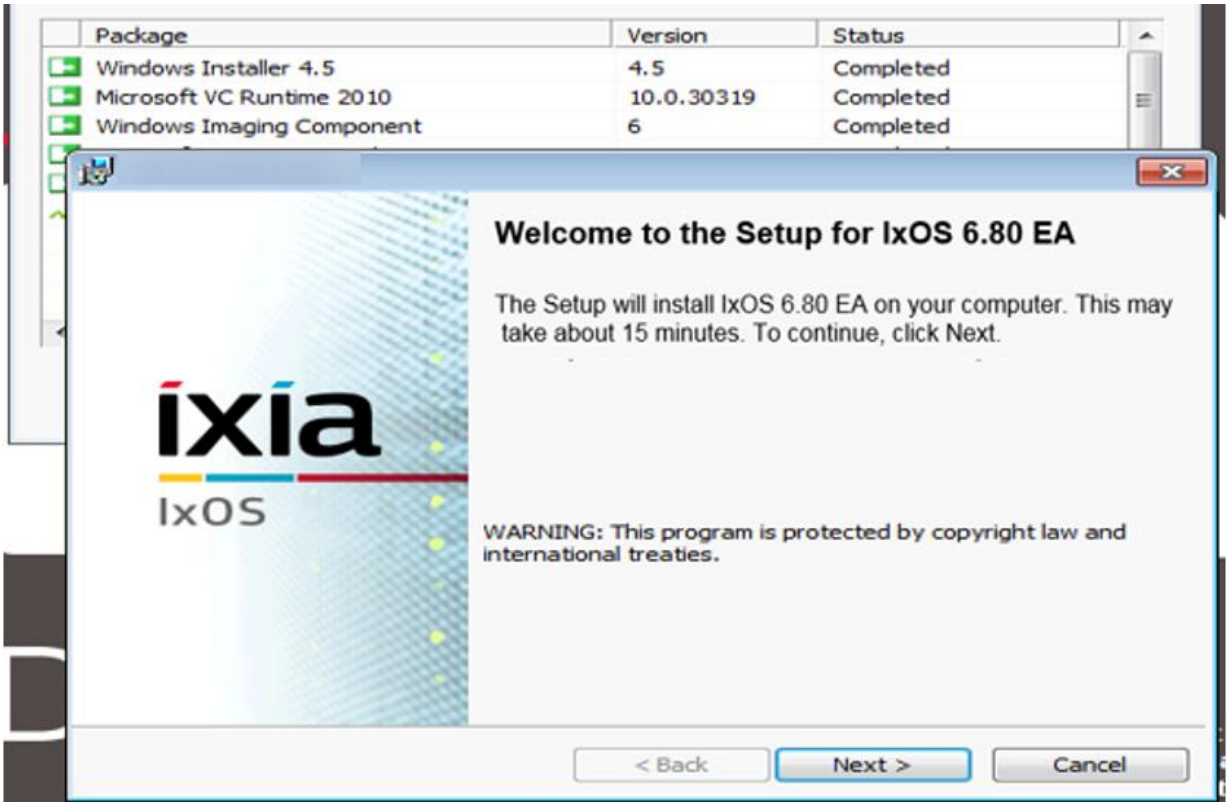
5. Click the **Run** button.



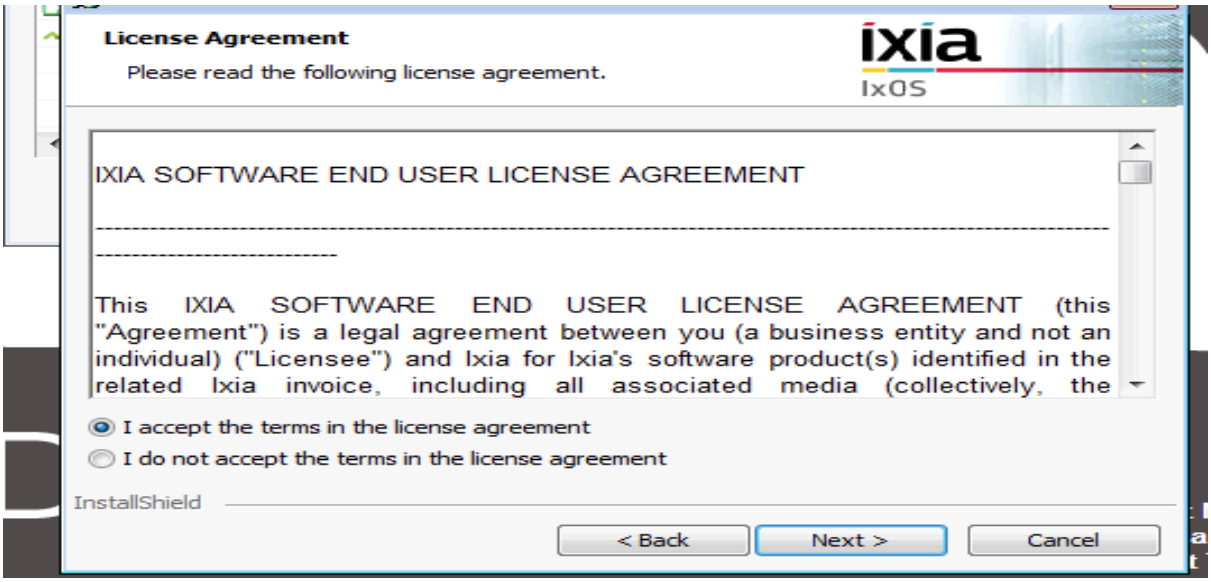
6. Accept the Default Destination Folder for the Installation. Select **Next**.



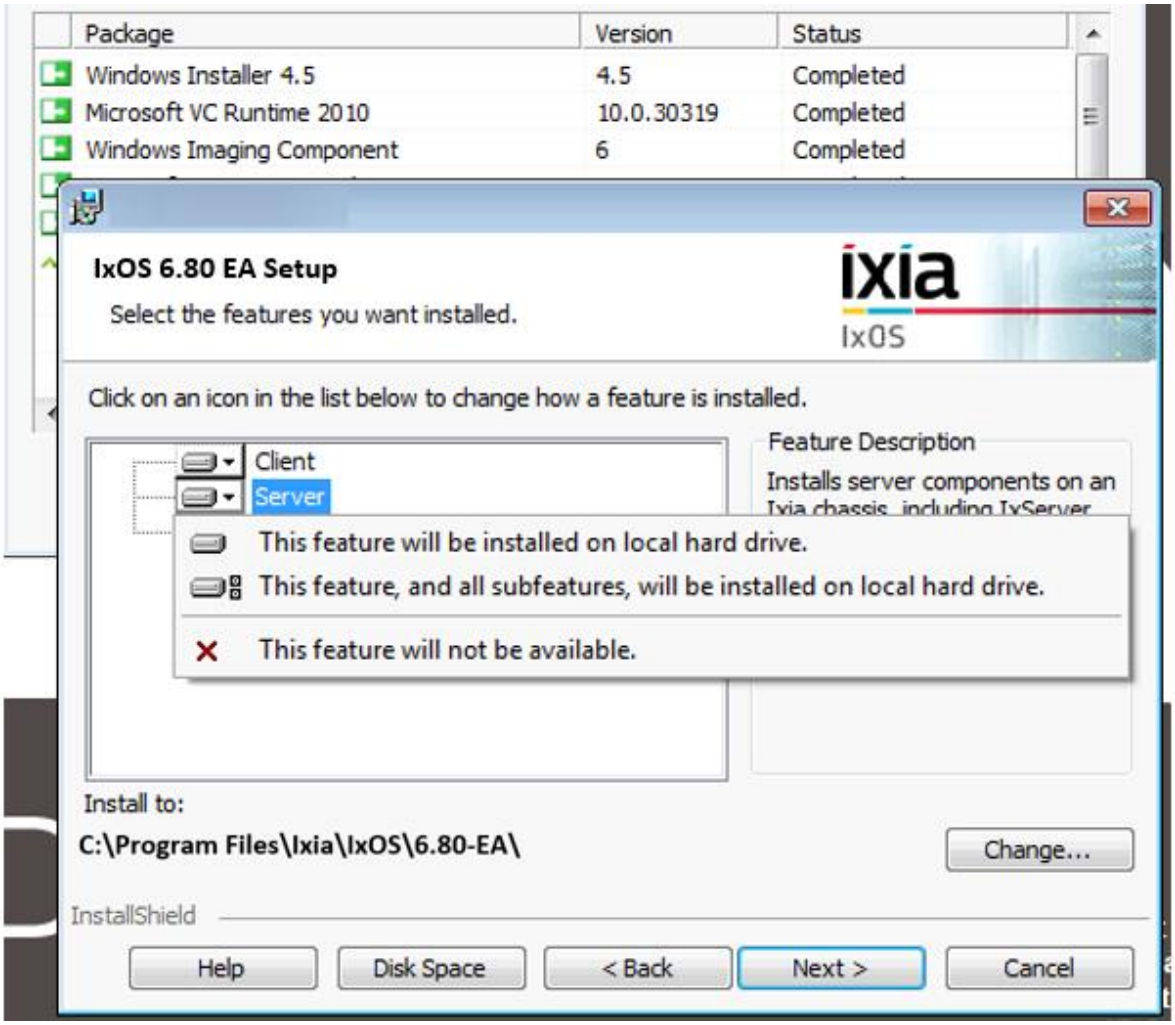
a. Select **Continue** on the "**Existing application Installation detected**:" window.



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

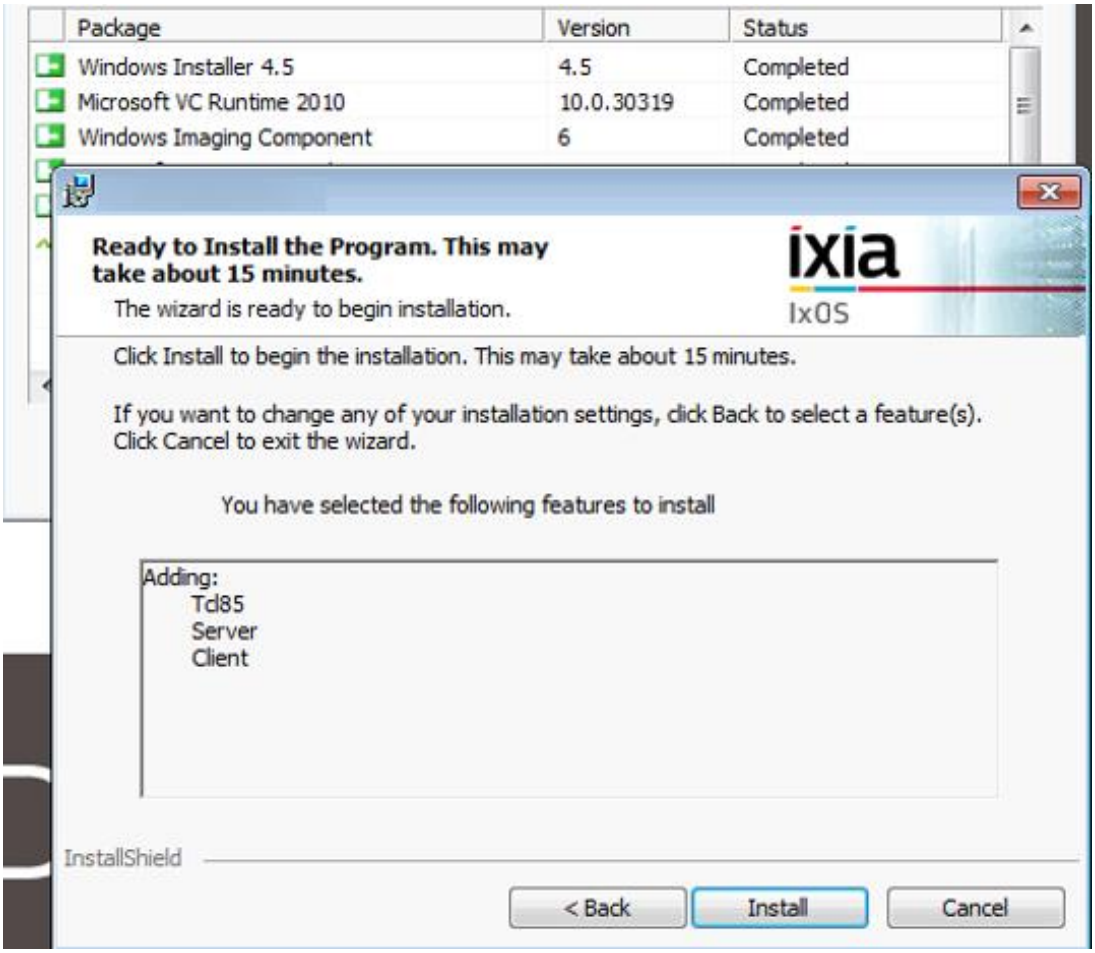


8. Accept the License Agreement, then select **Next**.



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.

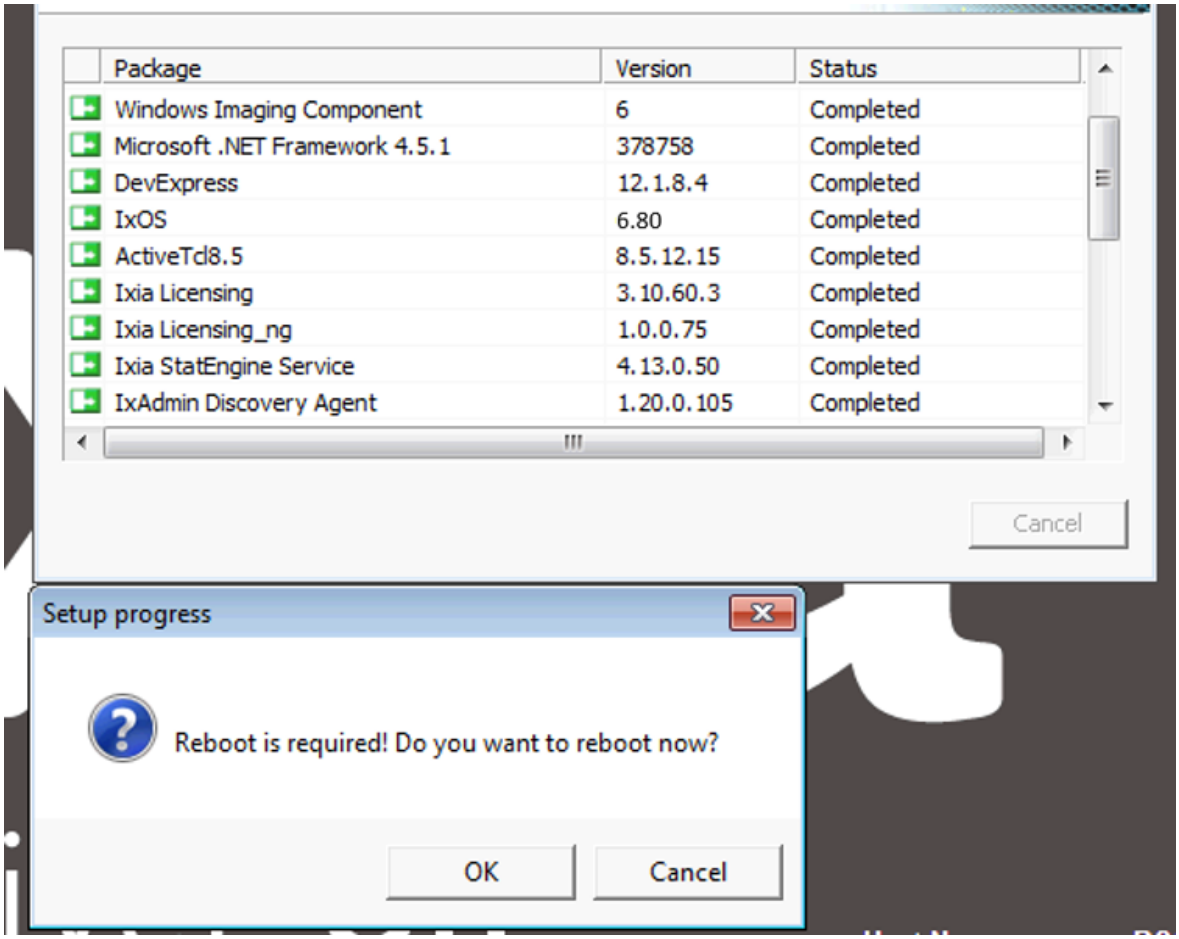
10. Select the following option: "**Add to Startup Programs.(Typical)",** then select **Next**.



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

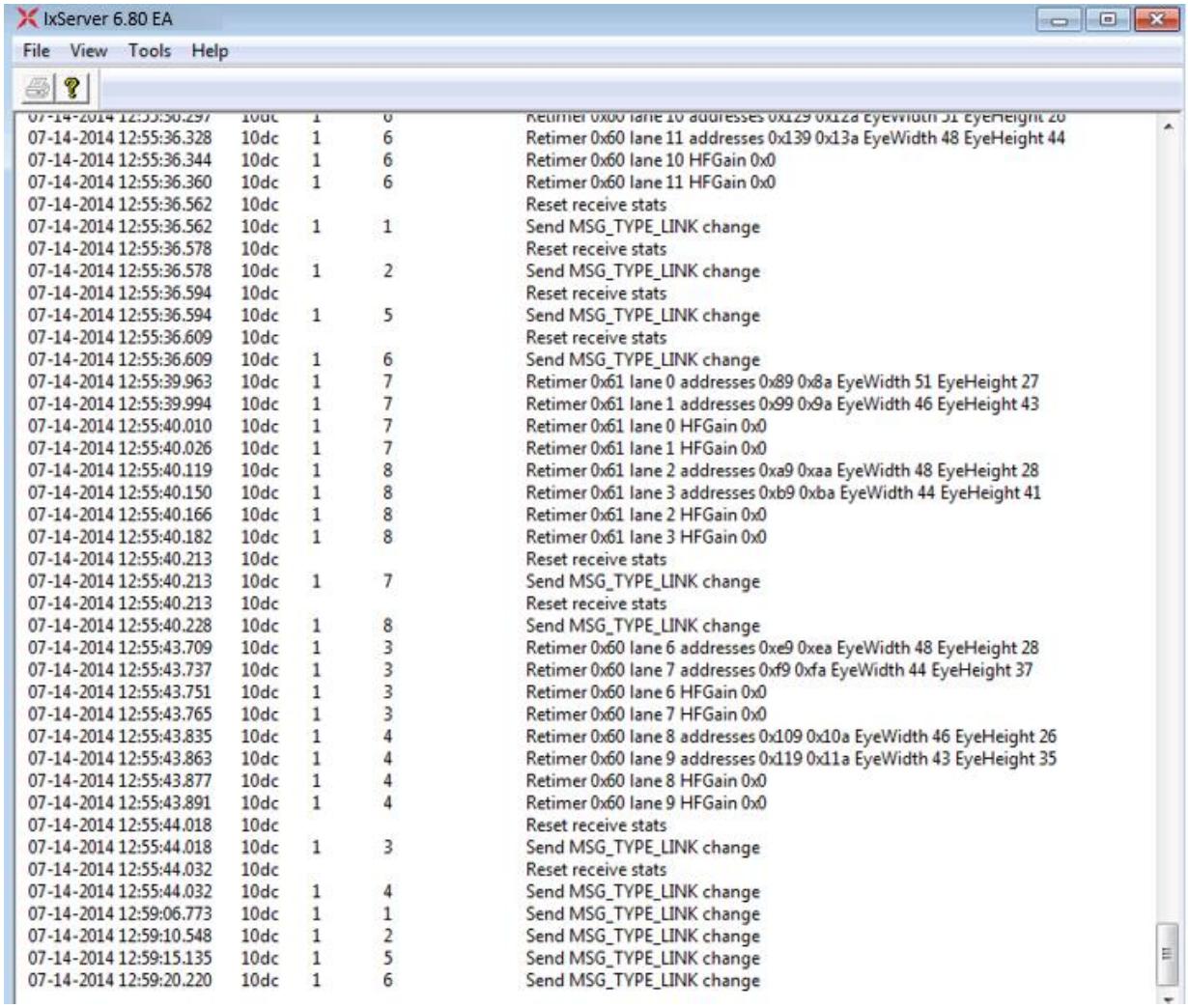
12. After several minutes of installation, new IxOS application links will be copied to the desktop.

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

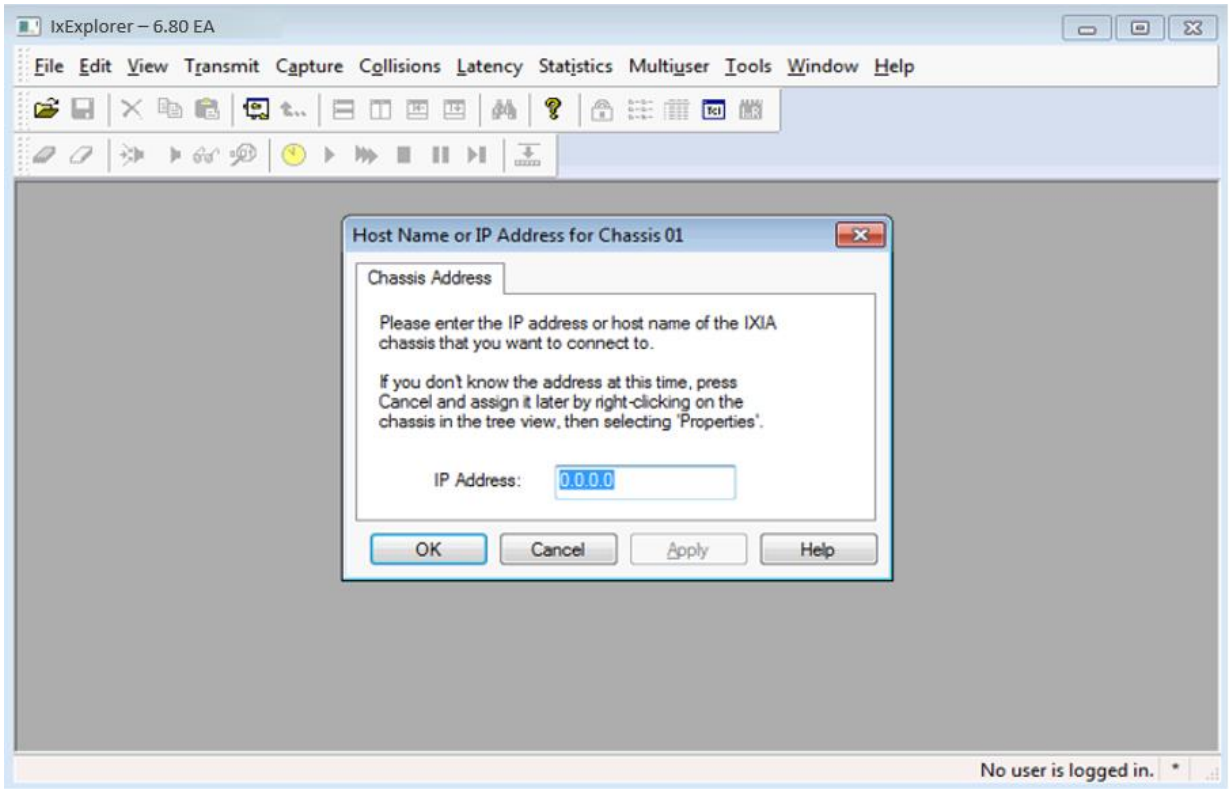


14. The system will ask the user to reboot the Windows VM.
15. After the Windows VM reboots IxServer will start automatically and will continue setting up the system hardware.

    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.

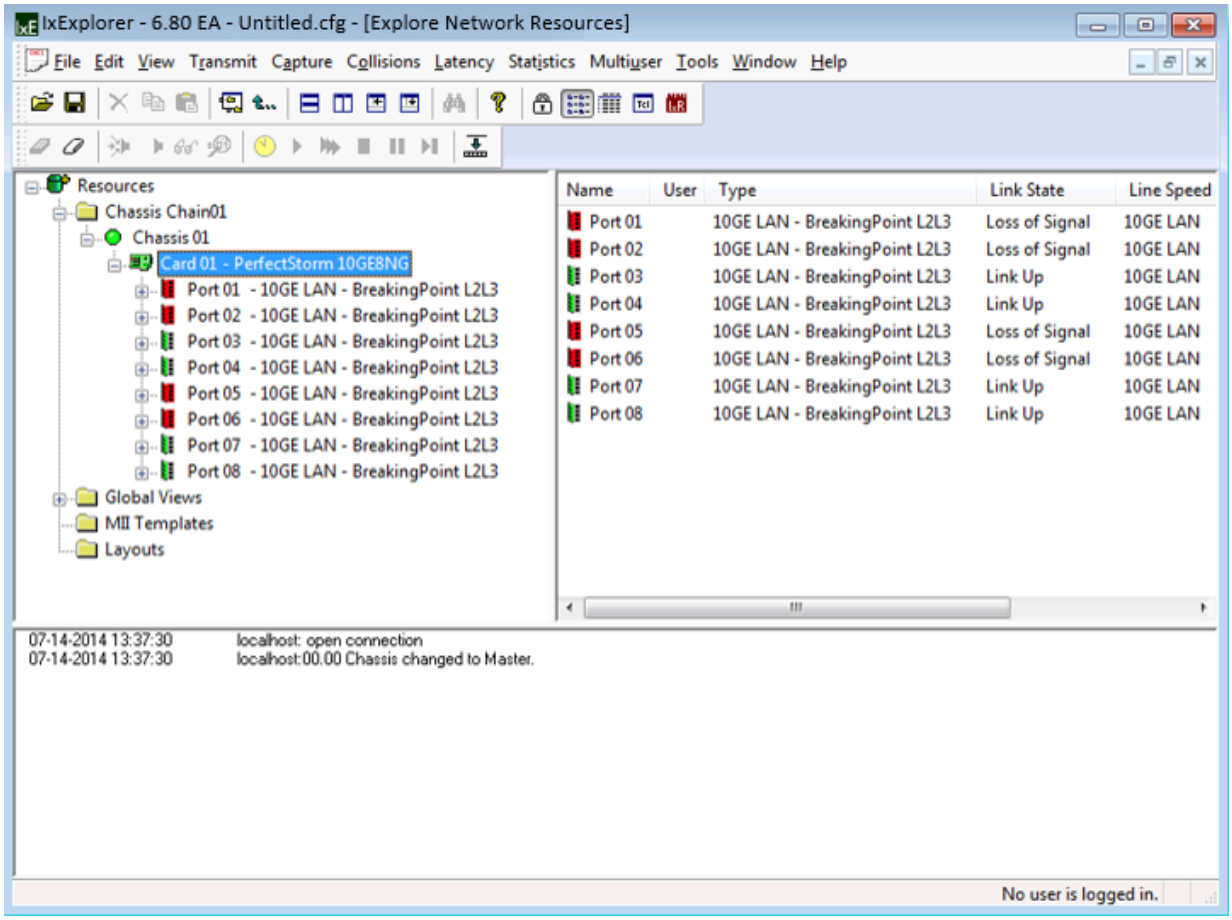


16. The image above shows an example of an IxServer that has completed initialization.



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.



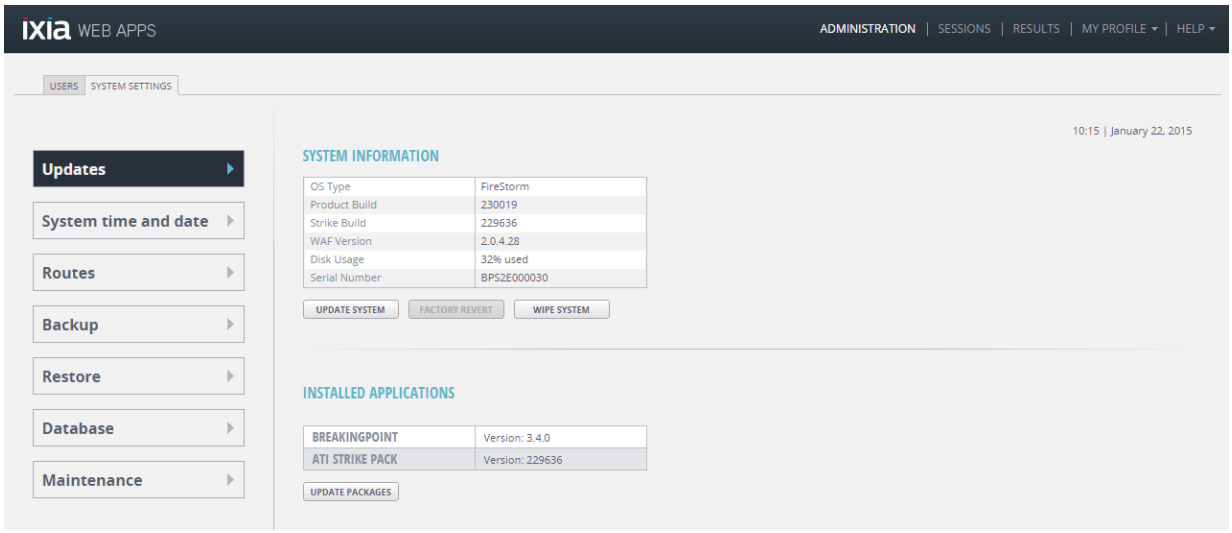
18. IxExplorer will show the status of the blades connected to the chassis along with the mode they are running in.

    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**



5. Browse to the location of the BPS update file and select **OK**.
6. The BPS update will take 30-45 minutes to complete.

Switching to BreakingPoint Mode

All Fusion 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. 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.

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

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

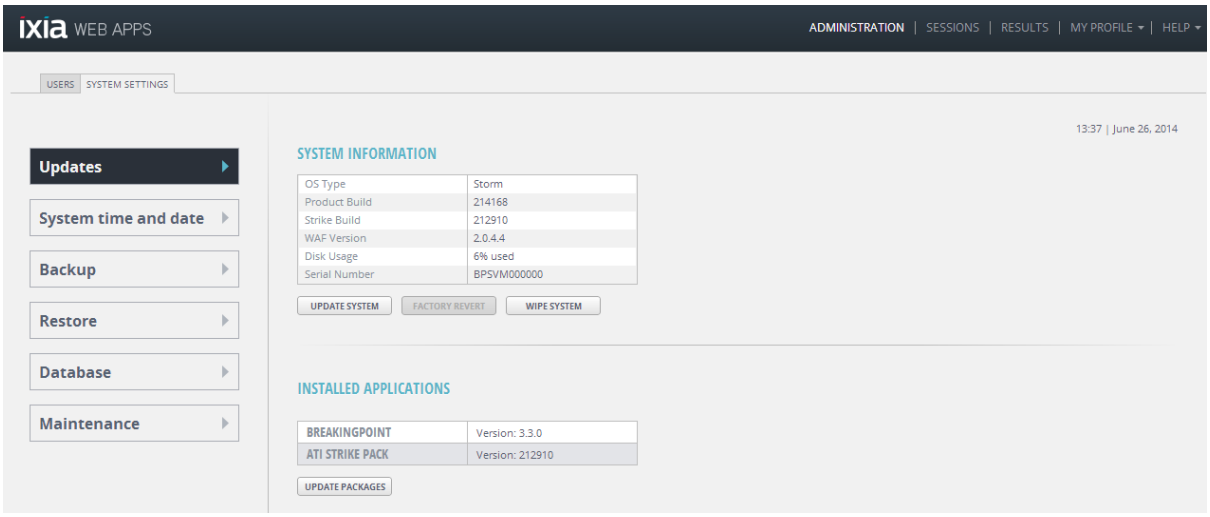
To transition from IxLoad mode to BreakingPoint mode:

1. Click a port on the load module to be transitioned. A message asking if you want to switch to BreakingPoint mode will be displayed.
2. Click **Yes** on the message that is displayed.
3. Wait until a green square is displayed in the upper right corner of the load module. Once the green square is displayed, you can begin using the load module or you can begin the transition process for another load module.

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

After you have successfully installed Firmware Release 3.4, all subsequent upgrades will be performed by accessing the Administration tab on the Ixia Web Apps Start page.

Figure 1: Ixia Web Apps Start Page



From there, select the System Settings tab and click on the Update System button and follow the instructions on your screen. To upgrade BreakingPoint Firmware, click on **Update System**. To upgrade your ATI Update or to install the Malware package, click **Update Packages**.

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 from Previous Releases

SR #	Description
635765	Fixed the accuracy of the strike level statistics.
626807	Fixed inconsistency in the number of strikes included in the "Security All Strikes" test.
632383	Fixed the "Allocation Rate" option of the IPv4 DHCP Hosts element so that it no longer causes DHCP discover messages to be sent at unacceptable rates.
643334	Fixed the SSL behavior in certain loopback scenarios where a Close Notify message was not properly sent from all servers.
633827	Fixed the CheckPoint test so that it now ends properly.

632193	Fixed the feature that allows packet captures to be exported from BP Storm 1G/10G while a test is running.
404455	Fixed the issue that prevented IPv6 DNS Traffic (from Application Simulator) to be sent from port 1 at the same time as IPv6 Attack Traffic (from Routing Robot).
238903	Fixed the reporting feature so that Real Time Statistics displays all of the Regexs used in a test.
625568	Attempting to edit the 331 action in a FTP flow no longer locks up the Superflow manager (which required a reboot to clear).
616472	SSL Cryptographic Errors are now returned on the client and server side when the DUT is connected to certain load balancers.
631078	Fixed the issue that caused the name of test that contained a large number of characters to be truncated.
616883	After a single TCP session finishes correctly with RST, BPS no longer sends illegitimate RST messages for other TCP sessions.
623609	Fixed the issue that caused packets to be dropped when some firewall DUTs were deployed between BPS client and server ports.
628740	Fixed the issue where SSL would reuse the same Session ID when different clients connected to the same destination IP address.
629540	Fixed the issue that prevented a Dictionary from being added to a Super Flow.
635484	Fixed the statistics issue that prevented Application Concurrent Flows to be reported correctly when running a test in loopback.
625227	Fixed the issue where transmit and receive statistics were not matching due to packet drop in Firewall.
61554	A test no longer stops cycling through connections once it gets between 20 and 21 Million TCP connections and the TCP Connection Rate stays at 0.
601679	Fixed the Real-Time Statistics issue where GTP Tunnels statistics were mistakenly labeled as Mobile Session Statistics.
404144	Fixed the issue where Tests fail with the error message, "Fatal error: Caught Address error".
640700	Fixed the issue where the Web UI was not accessible from MAC OS X Chrome browser version 39.0.2171.71.
404073	Fixed the issue where running a test without NAT in the configuration produces a data rate higher than a configuration with NAT enabled.
636880	Fixed the issue where Security Tests that have been saved with BreakingPoint reserved words in their name, prevents a Tcl shell from starting.
637695	Fixed the issue that caused the PerfectStorm One chassis to produce less throughput than the FireStorm chassis when the units were using identical test configurations.
604159	Fixed the issue that caused the Firestorm chassis to report SSL cryptographic error messages during the handshake phase when SSL Inspection/Decryption is enabled on the DUT.
633015	Fixed the issue that caused a slight bandwidth/frame rate decrease in test performance after upgrading from 3.2 to 3.3.1.

Known Defects

BreakingPoint Virtual Edition

The following section details the known defects of Firmware Release 3.4. 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
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.
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.