TEST REPORT

Tolly.

#224125

July 2024

Commissioned by Extreme Networks

Extreme Networks:

ExtremeCloud IQ Site Engine Interoperability Evaluation

EXECUTIVE SUMMARY

IT organizations deal with constant change but, along with the new, many must still manage a legacy infrastructure of switches, WLAN APs, and other devices during the transition. Because of a lack of integration across vendors, coupled with a lack of operational automation, such an environment can increase operational complexity and cost.

ExtremeCloud™ IQ Site Engine (Site Engine) simplifies and streamlines IT operations. It provides end-to-end network management, task automation, analytics, service assurance, and orchestration. Site Engine supports cloud-native, legacy Extreme Networks, and third-party devices, and facilitates the transition to cloud-based management.

Extreme Networks commissioned Tolly to evaluate the interoperability of its management solution with a variety of third-party network infrastructure devices. The evaluation included a range of management and automation functions related to configuration changes, firmware upgrades, backup/restore, and more.

Site Engine proved able to exercise a broad range of functions on devices from Cisco Systems, HPE Aruba Networking, Juniper Networks, and others. The Extreme Networks solution leverages open technologies to provide integrated access to a wide range of third-party systems. See Table 1 for an interoperability summary.

THE BOTTOM LINE

The ExtremeCloud IQ Site Engine illustrated interoperability with Cisco, Aruba, Juniper & other third-party devices in the following areas:

1. Device discovery
2. Device archive/restore
3. Firmware upgrade
4. Device monitoring
5. Device configuration

ExtremeCloud IQ Site Engine Management Interoperability with Cisco Systems, HPE Aruba Networking, & Juniper Networks Switches

Areas	Features		
Device Discovery	SNMP Profile	LLDP Interoperability	Topology Maps
Device Archive	Create Backup	Alarm on Config Mismatch	Archive Restore
Firmware Upgrade	Firmware Upload to Site Engine	Firmware Download to Device	Firmware Download Schedule
Device Monitoring	Syslog	Traps	Custom Alarms
Device Configuration	CLI Scripting	Workflows	Web Access/Terminal Access

Note: Each feature confirmed across representative switches from Cisco Systems, HPE Aruba Networking, Juniper Networks, and other devices.

Source: Tolly, March 2024

Table 1

Environment

Site Engine implements standards-based networking protocols to support open networking and provide support for third-party devices in customer networks.

Tests were conducted in a microcosm of an enterprise environment. This environment consisted of Extreme Networks LAN switches along with various current and older LAN switches from vendors such as Cisco Systems, HPE Aruba Networking, and Juniper Networks. The environment had more than a dozen switches, including older 3Com and Cabletron switches, various WLAN access points (APs) along with related networking infrastructure devices.

Site Engine Building Blocks

To understand the test results it is important to understand the methods that Extreme Networks uses to implement broad third-party support.

Extreme Networks leverages open, long-standing protocols to accomplish the communication between the Site Engine management system and devices.

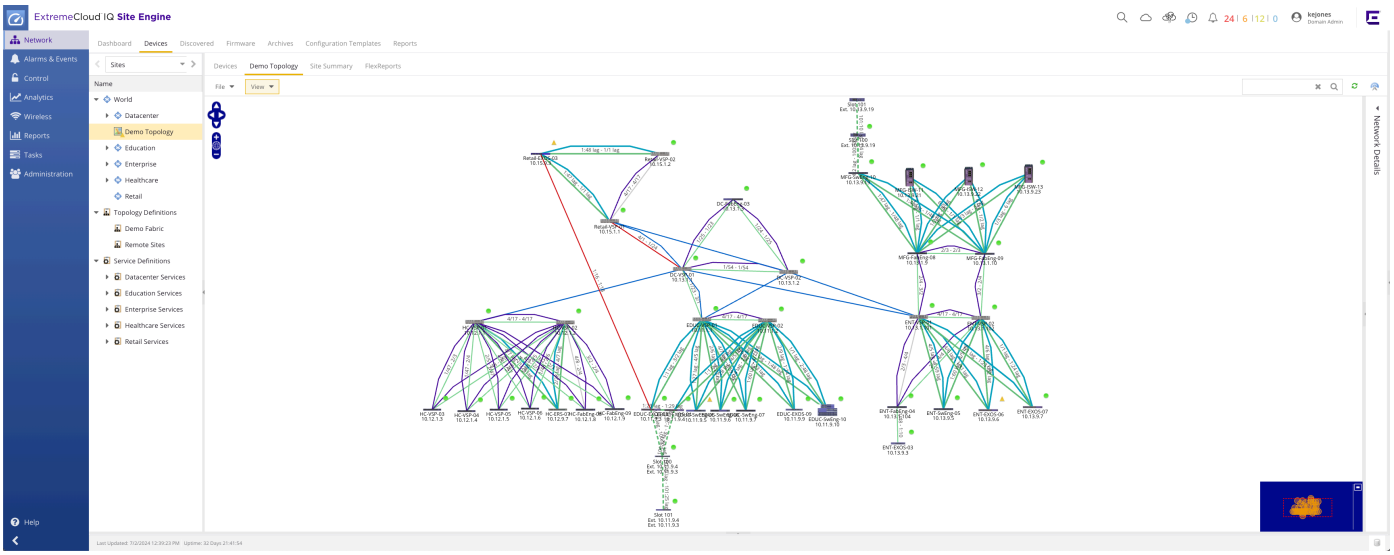
Every device, old and new, supports communications via Secure Shell (SSH) and/or Telnet, and/or Trivial FTP (TFTP). Similarly, most devices support SNMP and provide Management Information Base (MIB) details back to Site Engine. More recent switches, routers, and access servers will support the Link Layer Discovery Protocol (LLDP) which dynamically provides topology and capability information back to Site Engine.

The functional capabilities described in the Test Results section below are enabled by the aforementioned tools and protocols.

Test Results

Site Engine successfully demonstrated all of the areas/features listed in Table 1 not only for the Cisco Systems, HP Aruba Networking, and Juniper Networks switches tested but also for other third-party devices spot-checked by Tolly. Table 2, near the end of the report, provides more details on how each feature is used by Site Engine.

ExtremeCloud IQ Site Engine Dynamic Topology Map



Source: Tolly, March 2024

Figure 1

Device Discovery

Site Engine begins its device discovery by using the PING command to identify IP stations on any network segment that it is managing.

Customers can control which devices are discovered by creating SNMP profiles. (For example, the customer might not want to discover/manage every IoT device or WLAN AP on their network with Site Engine.)

Using LLDP discovery, Site Engine can gather basic information about various networking devices (e.g., system and port names, IP management address, MAC address, VLANs, etc).

Using customer-supplied device credentials, Site Engine can log in and initiate a user session to gather more information or, later, to control and configure the device.

Figure 1 shows an example topology map, created dynamically, that provides a high-level view into the network being managed by Site Engine.

Device Archive

Think of this capability as configuration backup and restore — and more. Site Engine logs in to the device and uses TFTP, SCP, and/or SFTP to back up (archive) the configuration to the Site Engine system for storage in the Site Engine database. This configuration can then be compared to any prior configuration file.

Figure 2, on the left side, shows a sample of a script used to archive the configuration from a Cisco Systems switch. On the right side is the output of a comparison of two configuration files noting the differences (in line 477) of the configuration).

Extreme Networks

ExtremeCloud IQ Site Engine

Network Device Interoperability Evaluation

Tolly. Certified

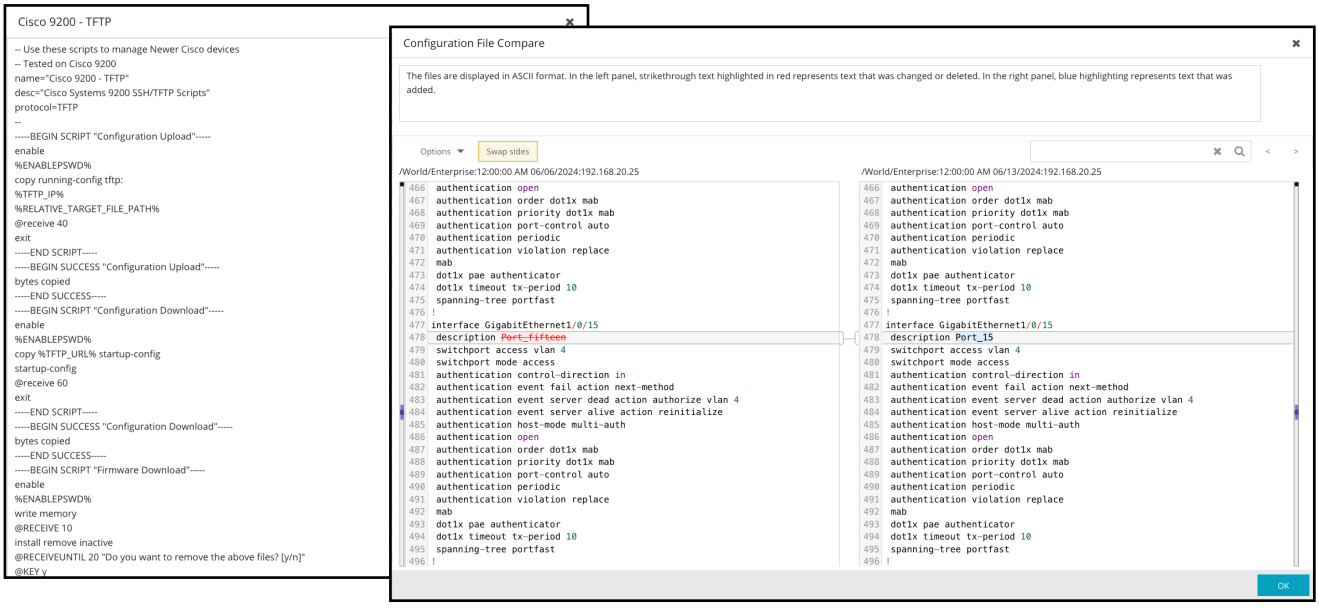
Tested March 2024

Site Engine can also restore any backup configuration to the device. The Site Engine database allows the user to store as many backup versions as required with no practical limit.

Firmware Upgrade

Using the same toolset and approach, Site Engine provides management for firmware upgrades.

ExtremeCloud IQ Site Engine Configuration Archive and File Compare



Source: Tolly, March 2024

Figure 2

Firmware for any and all devices can be downloaded from the network vendor website and uploaded and stored in the Site Engine database. Firmware can then be downloaded to one or more devices either on demand or on a scheduled basis.

Device Monitoring

In addition to the aforementioned information discovered by Site Engine, more granular device monitoring is easily implemented.

Devices can be configured to send syslog information to Site Engine that can then be monitored and acted upon automatically by Site Engine. Similarly, traps on devices can be used to notify Site Engine of any error or system condition desired by the user (e.g., temperature thresholds reached, authentication failures).

Site Engine allows the configuration of custom alarms and alerts to be automatically triggered when certain conditions occur. Figure 3 shows the Site Engine "Alarm & Events" screen with the pop-up illustrating how a custom alarm can be configured.

Device Configuration

Site Engine provides multiple methods of device configuration to suit your operational requirements, from manual to automated.

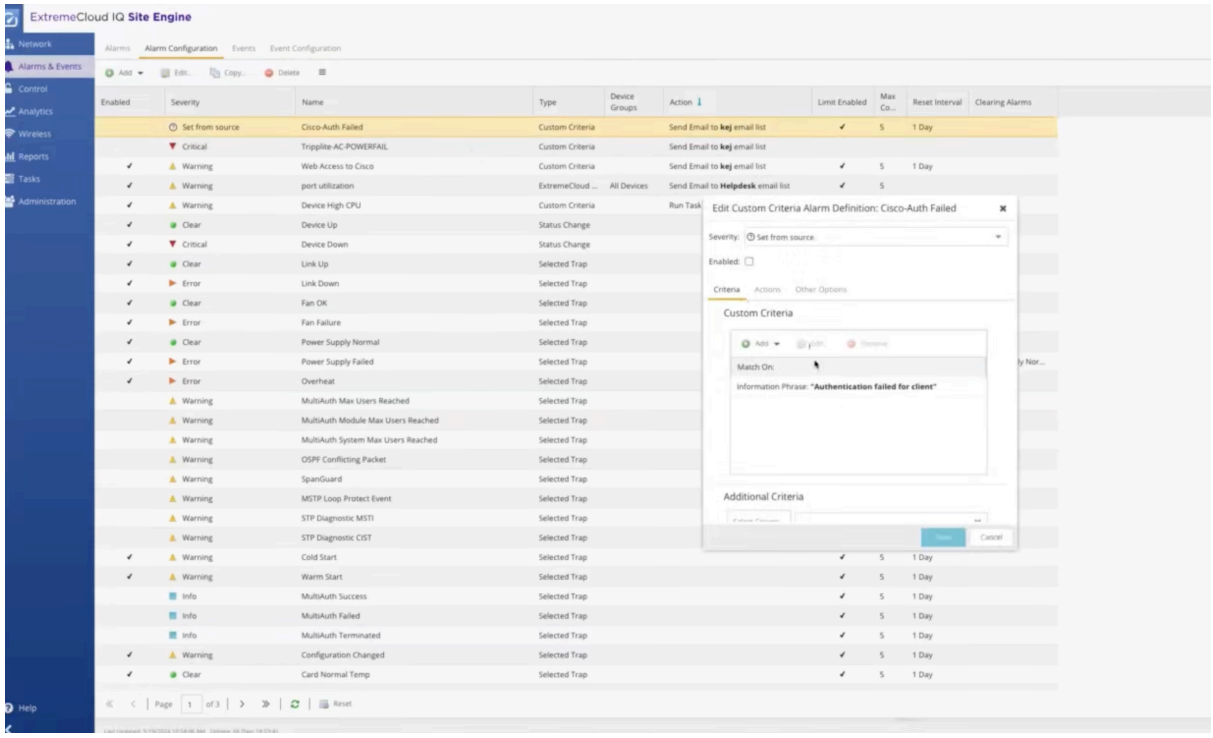
At the most basic level, Site Engine provides integrated access to terminal or web interfaces of any managed device without needing to leave the Site Engine console.

Site Engine provides scripting support to enable customers to automate any process on any device. These include CLI, TCL, and Python so customers can build tasks to accomplish device configuration tasks.

Extreme Networks provides pre-built scripts for many popular devices and maintains a GitHub site for these and other, community-contributed scripts for a wide range of devices. Those scripts can be found here: https://github.com/extremenetworks/ExtremeScripting/blob/master/XMC_XIQ-SE/README.md.

Site Engine takes this automation to the next level with workflows. Simply put,

ExtremeCloud IQ Site Engine Alarms & Events with Custom Alarm Configuration



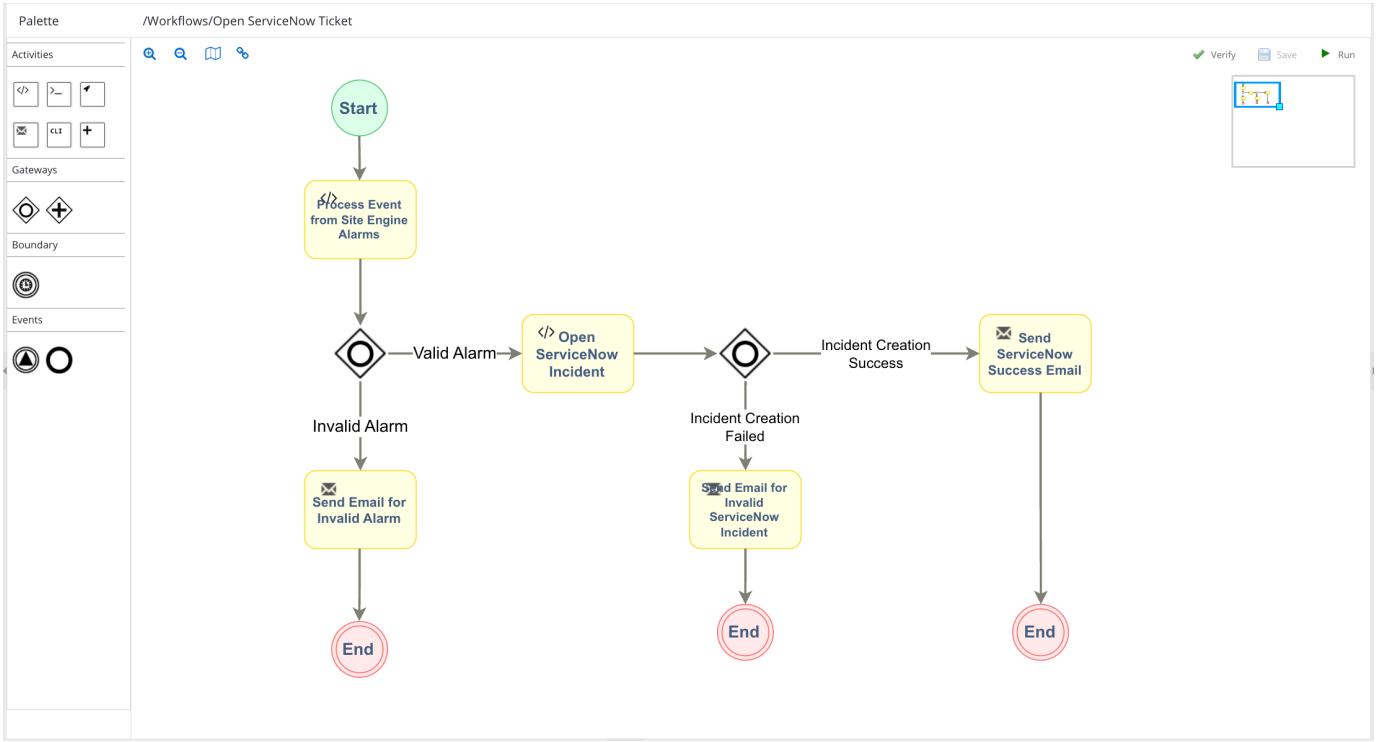
Source: Tolly, March 2024

Figure 3

workflows are individual tasks (scripts) that are linked with "If-then-else" logic.

They can be used for a variety of purposes including configuration and alarm response. Figure 4 illustrates the use of a workflow to respond to an alarm and automatically generate a "ServiceNow" trouble ticket.

ExtremeCloud IQ Site Engine Device Configuration - Workflow Example



Source: Tolly, March 2024

Figure 4

ExtremeCloud IQ Site Engine Management Interoperability with Aruba, Cisco Systems, Juniper Networks, & Third-Party Network Devices

Area	Feature	Notes
Device Discovery	SNMP Profile	Standard SNMP used to query device information. Uses customer-supplied device credentials
	Link Layer Discovery Protocol (LLDP) Interoperability	Standard LLDP used to gather link information from devices
	Topology Maps	Generated from information gathered via SNMP and LLDP
Device Archive	Create Backup	Scripting used to create backup via console interface
	Alarm on Config Mismatch	Scripting used to compare live configuration with configuration stored in Site Engine database
	Archive Restore	Scripting used to create restore via console interface
Firmware Upgrade	Firmware Upload to Site Engine	Scripting used to copy firmware from vendor site to Site Engine database
	Firmware Download to Device	Scripting used to drive console commands to download/install firmware on device
	Firmware Download Schedule	Site Engine scheduler used to set run time for firmware download/install
Device Monitoring	Syslog	Used to feed information from devices to Site Engine
	Traps	Used to feed information from devices to Site Engine for certain conditions
	Custom Alarms	Can use syslog/trap information to trigger custom alarms
Device Configuration	CLI Scripting	Use native device CLI to automate functions from Site Engine
	Workflows	Combine scripts with if-then-else logic to create workflows
	Web Access / Terminal Access	Integrated "right-click" access to ssh/telnet/web from Site Engine

Source: Tolly, March 2024

Table 2

Test Setup & Methodology

Because the test was a demonstration of capabilities, there was no formal methodology. Relevant technical details of the functions evaluated are included in the Test Results section of this report that begins on page 2.

About Tolly…

The Tolly Group companies have been delivering world-class IT services for more than 35 years. Tolly is a leading global provider of third-party validation services for vendors of IT products, components and services.
You can reach the company by email at sales@tolly.com, or by telephone at +1 561.391.5610.

Visit Tolly on the Internet at:
http://www.tolly.com

Terms of Usage

This document is provided, free-of-charge, to help you understand whether a given product, technology or service merits additional investigation for your particular needs. Any decision to purchase a product must be based on your own assessment of suitability based on your needs. The document should never be used as a substitute for advice from a qualified IT or business professional. This evaluation was focused on illustrating specific features and/or performance of the product(s) and was conducted under controlled, laboratory conditions. Certain tests may have been tailored to reflect performance under ideal conditions; performance may vary under real-world conditions. Users should run tests based on their own real-world scenarios to validate performance for their own networks.

Reasonable efforts were made to ensure the accuracy of the data contained herein but errors and/or oversights can occur. The test/audit documented herein may also rely on various test tools the accuracy of which is beyond our control. Furthermore, the document relies on certain representations by the sponsor that are beyond our control to verify. Among these is that the software/hardware tested is production or production track and is, or will be, available in equivalent or better form to commercial customers. Accordingly, this document is provided "as is", and Tolly Enterprises, LLC (Tolly) gives no warranty, representation or undertaking, whether express or implied, and accepts no legal responsibility, whether direct or indirect, for the accuracy, completeness, usefulness or suitability of any information contained herein. By reviewing this document, you agree that your use of any information contained herein is at your own risk, and you accept all risks and responsibility for losses, damages, costs and other consequences resulting directly or indirectly from any information or material available on it. Tolly is not responsible for, and you agree to hold Tolly and its related affiliates harmless from any loss, harm, injury or damage resulting from or arising out of your use of or reliance on any of the information provided herein.

Tolly makes no claim as to whether any product or company described herein is suitable for investment. You should obtain your own independent professional advice, whether legal, accounting or otherwise, before proceeding with any investment or project related to any information, products or companies described herein. When foreign translations exist, the English document is considered authoritative. To assure accuracy, only use documents downloaded directly from Tolly.com.

224125-fj-R—-wt-2024-07-11—VerJ