ExtremeCloud™ IQ - Site Engine Configuration and Requirements

10/2022
22.09.10
PN: 9037656-00

Table of Contents

ExtremeCloud™ IQ - Site Engine Configuration and Requirements 1

Table of Contents 2

Configuration and Requirements 3

- Security and Vulnerability Testing 3
- Installation Information 3
  - Important Installation Considerations 4
    - Custom FlexViews 4
    - Custom MIBs and Images 4
  - Important Upgrade Considerations 6
    - Access Control Version 8.0 and newer 6
- Firewall Considerations 6
- Supported MIBs 6

Ports List 7

- Ephemeral Ports 12

Configuration and Requirements

Security and Vulnerability Testing

Security is something that is taken seriously by Extreme Networks. Our commitment to achieving and maintaining a strong security stance for our products enables our customers to have confidence in networking, software, and management infrastructure provided by the company.

The Software Quality Assurance team at Extreme Networks scans every ExtremeCloud IQ - Site Engine release using the current versions of multiple anti-virus solutions, updated to include the latest virus signatures.

Additionally, all Extreme Networks products undergo rigorous security testing with best-of-breed industry standard scanners. Further, all product binary images are scanned with sophisticated anti-virus solutions for evidence of viruses and malware before the images are uploaded to customer-facing portals. Whenever issues are discovered by these scanners and anti-virus solutions, a well-defined triage process is engaged for remediation or mitigation of such findings. This enables Extreme Networks to engineer solutions that heighten the security of our products, and new releases are made available as necessary in order to address any discovered security vulnerabilities. This has several additional benefits in terms of helping customers maintain networks that are compliant under various regulatory or industry standards such as HIPAA, SoX, and PCI.

Extreme Networks also monitors industry security information data sources, such as CERT, the full-disclosure mailing list, and various authoritative CVE announcements for vulnerabilities that could potentially apply to our products. When such a vulnerability is found, we follow a process by which high severity vulnerabilities (such as the ShellShock bug in the bash shell from late 2014) are prioritized over lower severity vulnerabilities. The severity itself is derived from the Common Vulnerability Scoring System (CVSS) score which provides the most widely accepted measure for vulnerability severity. For applicable vulnerabilities, we provide feedback to CERT to keep them updated on the status of our findings.

Further, for many of our products that are based on a Linux engine image – ExtremeCloud IQ - Site Engine and ExtremeControl, for example – we harden the engines by ensuring that we do not start unnecessary services and we do not install unnecessary software. In addition, we apply security updates from the upstream Linux distribution.

Taken together, the security of Extreme Networks products is maintained and verified. For all inquiries about our security processes, contact Global Technical Assistance Center (GTAC).

Installation Information

For complete installation instructions, refer to ExtremeCloud IQ - Site Engine Suite Installation.

IMPORTANT: The Compliance tab is available and supported by Extreme on an ExtremeCloud IQ - Site Engine engine running the Linux operating system supplied by Extreme. Other Linux operating systems can support Compliance functionality, but python version 2.7 or higher must be installed. Additionally Compliance functionality requires the git, python2, python mysql module, python setup tools module, and python "pygtail" module packages be installed and related dependencies managed by the customer for their server's unique operating system and version.

Important Installation Considerations

Custom FlexViews

When reinstalling ExtremeCloud IQ - Site Engine Console, the installation program saves copies of any FlexViews you created or modified in the `<install directory>\.installer\backup\current\appdata\System\FlexViews` folder.

If you are deploying FlexViews via the ExtremeCloud IQ - Site Engine server, save them in the `appdata\VendorProfiles\Stage\MyVendorProfile\FlexViews\My FlexViews` folder.

Custom MIBs and Images

If you are deploying MIBs via the ExtremeCloud IQ - Site Engine server, they are saved in the `appdata\VendorProfiles\Stage\MyVendorProfile\MIBs\` folder.

If you are deploying device images (pictures) via the ExtremeCloud IQ - Site Engine server, they are saved in the `appdata\VendorProfiles\Stage\MyVendorProfile\Images\` folder.

ExtremeCloud IQ - Site Engine version 22.09.10 supports upgrades from Extreme Management Center versions 8.4.4, 8.5.7 or ExtremeCloud IQ - Site Engine.

NOTE: You can change deployment modes from air gap to connected or from connected to air gap after the upgrade.

The following table details which upgrades are needed for each NetSight, Extreme Management Center or ExtremeCloud IQ - Site Engine version prior to upgrading to ExtremeCloud IQ - Site Engine version 22.09.10.

Current Version				Upgrade to ExtremeCloud IQ - Site Engine version 22.9
	8.3.3	8.4.4	8.5.7	
ExtremeCloud IQ - Site Engine (all versions)				X

Current Version				Upgrade to ExtremeCloud IQ - Site Engine version 22.9
	8.3.3	8.4.4	8.5.7	
Extreme Management Center version 8.5.5, 8.5.6 , or 8.5.7				X
Extreme Management Center version 8.5.0-8.5.4			X*	X
Extreme Management Center version 8.4.4				X
*Extreme Management Center version 8.4.0-8.4.3		X*	X*	X
*Extreme Management Center version 8.2.x or 8.3.x		X*	X*	X
Extreme Management Center version 8.0.x or 8.1.x	X		X	X
NetSight version 7.1 or older	X		X	X

*These versions can be updated to either version 8.4.4 or 8.5.7 and then to ExtremeCloud IQ - Site Engine version 22.09.10.

IMPORTANT: A backup (**Administration** > Backup/Restore) of the database must be performed prior to the upgrade and saved to a safe location.

During the installation (if upgrading using the user interface installer), you have the option to backup additional user files by selecting a checkbox on the Previous Installation Detected screen. This option lets you backup user files such as Inventory Manager archive files not automatically backed up during the install because the backup could take several minutes.

Important Upgrade Considerations

- If your network is using ExtremeAnalytics or ExtremeControl engines, Fabric Manager, or another add-on feature, you must first perform the ExtremeCloud IQ - Site Engine upgrade to version 22.09.10 and then add the feature.
- The 4.xx version of the NAC Request Tool is not compatible with the 22.09.10 ExtremeCloud IQ - Site Engine server. If you are using the NAC Request Tool you need to upgrade the version of NAC Request Tool to version 22.09.10.
- To upgrade Traffic Sensor from version 21.x, a fresh installation is recommended. If the fresh installation cannot be used, then please check Knowledge Base for a special procedure.

Access Control Version 8.0 and newer

Beginning in version 8.0, ExtremeControl can fail to join Active Directory when accessing as a **Standard Domain User with Descendant Computer Objects ("Reset password" permissions only)** group member.

To enable this functionality, add the following permissions:

- **Reset Password**
- **Validated write to DNS host name**
- **Validated write to service principal**
- **Read and write account restrictions**
- **Read and write DNS host name attributes**
- **Write servicePrincipalName**

Firewall Considerations

To configure your firewall, see Ports List.

Supported MIBs

The following directory contains the IETF and Private Enterprise MIBs supported by ExtremeCloud IQ - Site Engine applications:

`<install directory>\appdata\System\mibs directory`

Navigate to the directory and open the .index file to view an index of the supported MIBs.

Additional MIB Support information is available at www.extremenetworks.com/support/policies.

Ports List

ExtremeCloud IQ - Site Engine Inbound Communication (Local Ports)

Type	Port	Description	Purpose
TCP	20	FTP Data	Device software and configuration upload/download
TCP	21	FTP Control	Device software and configuration upload/download
TCP	22	SSH	Shell access Device software and configuration upload/download
TCP	8080	HTTP	Web browser access to ExtremeCloud IQ - Site Engine user interface (redirects to port 8443) Communication with ExtremeControl and ExtremeAnalytics
TCP	8443	HTTPS	Web browser access to ExtremeCloud IQ - Site Engine user interface Northbound Interface (NBI) ExtremeControl, ExtremeAnalytics, and Fabric Manager communication
TCP	8444	HTTPS	ExtremeControl engine communication
TCP	8445	HTTPS	ExtremeControl Assessment communication
TCP	20504	ExtremeWireless Protocol	ExtremeWireless Controller communication
TCP	20505	ExtremeWireless Protocol	ExtremeWireless Controller communication
UDP	69	TFTP	Device software and configuration upload/download
UDP	123	NTP	
UDP	161	SNMP	SNMP agent (if enabled)
UDP	162	SNMP Traps	Reception of SNMP traps from all managed devices Reception of SNMP traps from ExtremeControl and ExtremeAnalytics engines, Guest & IoT Manager, Fabric Manager, ExtremeWireless Controller, and Virtual Sensors.
UDP	514	Syslog	Reception of syslog messages from monitored devices
UDP	2055	NetFlow	Default NetFlow collector
UDP	6343	SFlow	SFlow for ExtremeAnalytics / Application Telemetry

ExtremeCloud IQ - Site Engine Outbound Communication (Remote Ports)

Type	Port	Description	Purpose
TCP	22	SSH	CLI access to managed devices Shell access to ExtremeControl and ExtremeAnalytics engines, Guest & IoT Manager, Fabric Manager, and ExtremeWireless controllers
TCP	23	Telent	If used for CLI communication in lieu of SSH
TCP	25	SMTP	Communication with SMTP server (port is configurable, most common values: 25, 465, and 587)
TCP	49	TACACS+	Required when using TACACS+ for user authentication
TCP	80	HTTP	Internet for ExtremeControl Assessment Agent updates (extremenetworks.com) Virtual sensor communication
TCP	389	LDAP	Required when using LDAP for user authentication
TCP	443	HTTPS	Allows ExtremeCloud IQ - Site Engine to connect to ExtremeCloud IQ ExtremeAnalytics Fingerprint updates (services.enterasys.com)
TCP	443	Connect	Connect modules can be configured to communicate with third party solutions. The destination is defined in the Connect modules.
TCP	636	LDAPs	Required when using LDAP for user authentication
TCP	8080	HTTP	ExtremeControl and ExtremeAnalytics engine communication
TCP	8443	HTTPS	ExtremeControl, ExtremeAnalytics, Guest & IoT Manager, Fabric Manager, and Virtual Sensor communication
TCP	8444	HTTPS	ExtremeControl engine communication
TCP	20506	ExtremeWireless Protocol	ExtremeWireless Controller communication
UDP	53	DNS	Domain Name Server
UDP	123	NTP	Network Time Protocol
UDP	161	SNMP	SNMP Management of all managed devices SNMP Management of ExtremeControl and ExtremeAnalytics engines, Guest & IoT Manager, Fabric Manager, ExtremeWireless Controller, and Virtual Sensors.
UDP	162	SNMP Trap	Send SNMP traps to external trap receivers
UDP	514	Syslog	Send syslog messages to external syslog receivers
UDP	1812	RADIUS authentication	Required when using RADIUS for user authentication

Outbound Internet Connections From ExtremeCloud IQ - Site Engine (not mandatory in air gap deployment)

Type	Port	Description	Purpose
TCP	443	HTTPS	ExtremeAnalytics Fingerprint updates (services.enterasys.com)
TCP	443	HTTPS	Allows ExtremeCloud IQ - Site Engine to connect to ExtremeCloud IQ (`*.extremecloudiq.com` - Check the specifics for your RDC. Login to ExtremeCloud IQ > About ExtremeCloud IQ > Firewall Configuration Guide)
TCP	80	HTTP	ExtremeControl Assessment Agent download (`extremenetworks.com`)

ExtremeControl Inbound Communication (Local Ports)

Type	Port	Description	Purpose
TCP	22	SSH	Shell access Device software and configuration upload/download
TCP	80	HTTP	Captive Portal listening
TCP	443	HTTPS	Captive Portal listening
TCP	8080	HTTP	ExtremeControl web browser access (redirects to port 8443) ExtremeCloud IQ - Site Engine communication Communication between multiple ExtremeControl engines From every end-system subnet subject to ExtremeControl assessment agent in order to support agent mobility
TCP	8443	HTTPS	ExtremeControl web browser access ExtremeCloud IQ - Site Engine communication Communication between multiple ExtremeControl engines From every end-system subnet subject to ExtremeControl assessment agent in order to support agent mobility
TCP	8444	HTTPS	ExtremeControl web browser access (redirects to port 8443) ExtremeCloud IQ - Site Engine communication Communication between multiple ExtremeControl engines
TCP	8445	HTTPS	ExtremeControl Assessment communication
UDP	123	NTP	Network Time Protocol
UDP	161	SNMP	SNMP agent managed by ExtremeCloud IQ - Site Engine
UDP	1812	RADIUS authentication	ExtremeControl RADIUS server
UDP	1813	RADIUS accounting	ExtremeControl RADIUS server
		Connect	Distributed IPS module can be configured to receive information from third party solutions. Source (Protocol and Port and IP) is defined in the Distributed IPS module.

ExtremeControl Outbound Communication (Remote Ports)

Type	Port	Description	Purpose
TCP	22	SSH	Configuration of devices running VOSS/Fabric Engine (if ssh is configured in the CLI profile)
TCP	23	Telnet	Configuration of devices running VOSS/Fabric Engine (if telnet is configured in the CLI profile)
TCP	389	LDAP	User-based network authentication and directory services
TCP	80/443	HTTPS	CRL verification
TCP	445	DCERPC	Distributed Computing Environment/Remote Procedure Calls
TCP	636	LDAP	User-based network authentication and directory services
TCP	8080	HTTP	ExtremeCloud IQ - Site Engine communication Communication between multiple ExtremeControl engines
TCP	8443	HTTPS	ExtremeCloud IQ - Site Engine communication Communication between multiple ExtremeControl engines
TCP	8444	HTTPS	ExtremeCloud IQ - Site Engine communication Communication between multiple ExtremeControl engines
UDP/TCP	88	Kerberos	Kerberos Protocol
UDP	123	NTP	Network Time Protocol
UDP	161	SNMP	Communication to authenticators
UDP	162	SNMP Trap	SNMP traps sent to ExtremeCloud IQ - Site Engine
UDP	389	CLDAP	Winbind discovery
UDP	1700	RADIUS CoA	ExtremeControl RADIUS server to authenticators
UDP	1812	RADIUS authentication	Proxy authorization to remote RADIUS Server
UDP	1813	RADIUS accounting	Proxy accounting to remote RADIUS Server
UDP	3799	RADIUS CoA	ExtremeControl RADIUS server to authenticators

ExtremeAnalytics Inbound IP Protocols

Type	Protocol	Description	Purpose
IP	47	GRE	Mirror Traffic for CoreFlow, Virtual Sensor, Wireless Controller, and App Telemetry application identification.

ExtremeAnalytics Inbound Communication (Local Ports)

Type	Port	Description	Purpose
TCP	22	SSH	Shell access
TCP	8080	HTTP	ExtremeCloud IQ - Site Engine communication
TCP	8443	HTTPS	ExtremeCloud IQ - Site Engine communication
UDP	123	NTP	Network Time Protocol
UDP	161	SNMP	SNMP agent managed by ExtremeCloud IQ - Site Engine
UDP	2055	NetFlow	NetFlow Collector
UDP	2058	IPFIX	VMWare NSX IPFIX collector
UDP	2075	IPFIX	ExtremeXOS/Switch Engine IPFIX collector
UDP	2095	NetFlow	ExtremeWireless NetFlow collector
UDP	4739	IPFIX	VTAP IPFIX collector from Virtual Sensor
UDP	6343	SFlow	SFlow for ExtremeAnalytics Application Telemetry

ExtremeAnalytics Outbound Communication (Remote Ports)

Type	Port	Description	Purpose
TCP	80	HTTP	Virtual Sensor configuration
TCP	443	HTTPS	Virtual Sensor configuration
TCP	8080	HTTP	ExtremeCloud IQ - Site Engine communication
TCP	8443	HTTPS	ExtremeCloud IQ - Site Engine communication
UDP	123	NTP	
UDP	162	SNMP Trap	SNMP traps sent to ExtremeCloud IQ - Site Engine
UDP		IPFIX	Flow export. Destination and port is defined in the configuration of the Analytics Engine

Fabric Manager Outbound Communication (Remote Ports)

Type	Port	Description	Purpose
UDP	161	SNMP	Communicating with the devices
TCP	22	SSH	Communication between ExtremeCloud IQ - Site Engine and FM for SSH
TCP	8443	HTTP	Communication between ExtremeCloud IQ - Site Engine and FM for REST & ZTP+

Fabric Manager Inbound Communication (Local Ports)

Type	Port	Description	Purpose
TCP	22	SSH	Communication between ExtremeCloud IQ - Site Engine and FM for SSH

Ephemeral Ports

The port range 32768 to 61000 is reserved for dynamically allocated port numbers used by most TCP and UDP based protocols, such as TFTP and FTP.