Extreme Management Center®
Configuration and Requirements
Version 8.3

9/2019
9035981-02
Subject to Change Without Notice

Table of Contents

Extreme Management Center® Configuration and Requirements Version 8.3 1
Table of Contents 2
Extreme Management Center Configuration and Requirements 3
Security and Vulnerability Testing 3
Configuration Considerations 4
Firewall Considerations 4
Supported MIBs 6

Extreme Management Center 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 Extreme Management Center 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 – Extreme Management Center 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).

Configuration Considerations

Firewall Considerations

- Port 8080 (Default HTTP traffic) must be accessible through firewalls for users to install and launch Extreme Management Center client applications.
- Port 8443 (Default HTTPS traffic) must be accessible through firewalls for clients to access the Extreme Management Center Server Administration web pages, Extreme Management Center, and ExtremeControl Dashboard.
- Port 8444 (Default HTTPS traffic) must be accessible through firewalls for clients to access the ExtremeControl Engine Administration web pages.
- The following port must be accessible through firewalls for the Extreme Management Center Server and an ExtremeControl Assessment Server to communicate:
  TCP: 8445
- The following ports must be accessible through firewalls for the Extreme Management Center Server and an ExtremeControl engine to communicate:
  Required Ports (all bidirectionally)
  TCP: 4589, 8080, 8443, 8444
  UDP: 161, 162

- The following port must be accessible through firewalls for ExtremeControl engine to ExtremeControl engine communication:
  TCP: 8444
- The following ports must be accessible through firewalls for ExtremeControl engine-to-ExtremeControl engine communication in order for assessment agent mobility to function properly:
  TCP: 8080, 8443
- The following ports must be accessible through firewalls from every end-system subnet subject to the ExtremeControl assessment agent to every ExtremeControl engine in order to support agent mobility:
  TCP: 8080, 8443
- The following ports must be accessible through firewalls for the Extreme Management Center Server and Wireless Controllers to communicate:
  SSH: 22
  SNMP: 161, 162
  Langley: 20506
- The following port must be accessible through firewalls for Assessment Agent updates:
  TCP: 80 from Extreme Management Center to internet.
- The following ports must be accessible through firewalls for Extreme Management Center firmware updates:
  TCP: 443 from Extreme Management Center to internet
- The following ports must be accessible through firewalls for the Extreme Management Center Server and WAS to communicate:
  TCP: Port 8443 — Used by WAS to authenticate Extreme Management Center users. This port corresponds to Extreme Management Center's HTTPs Web Server port.
  TCP: Port 443 — Import data from Extreme Management Center into WAS.
  TCP: Port 8080 — Upgrade WAS from WAS UI.
- The following ports must be accessible (bidirectionally) through firewalls for the Extreme Management Center Server and an Extreme ExtremeAnalytics engine to communicate:
  TCP: Ports 4589, 8080, 8443
  UDP: Ports 161, 162
  To ExtremeAnalytics engine:
  UDP: Port 2055 (NetFlow)
  TCP: 22, 8443

For GRE Tunnels to the ExtremeAnalytics engine IP Protocol 47

- Port 2055 must be accessible through firewalls for the Extreme Management Center Server to receive NetFlow data.
- The following ports must be accessible through firewalls for Guest and IoT Manager and Extreme Management Center to communicate:
  TCP: 8443
  SNMP: 161, 162
  SSH: 22
- The following ports must be accessible through firewalls for Fabric Manager and Extreme Management Center to communicate:
  TCP: 8443
  SNMP: 161, 162
  SSH: 22
- The following ports must be accessible through firewalls for the ExtremeAnalytics engine and the Virtual Sensor to communicate:
  - UDP: 4739
  - IP type 47 (GRE)
- The following ports must be accessible through firewalls for Extreme Management Center and the Virtual Sensor to communicate:
  - TCP: 80, 443, 8443
  - UDP ports 161, 162

Supported MIBs

The following directory contains the IETF and Private Enterprise MIBs supported by Extreme Management Center 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.