



Extreme Management Center[®] Configuration and Requirements Version 8.5

7/2020
9036806-00 Rev. AA
Subject to Change Without Notice

Table of Contents

Extreme Management Center® Configuration and Requirements Version 8.5	1
Table of Contents	2
Extreme Management Center Configuration and Requirements	3
Security and Vulnerability Testing	3
Installation Information	4
Important Installation Considerations	4
Custom FlexViews	4
Custom MIBs and Images	5
Evaluation License	5
Upgrade Information	5
Custom FlexViews, Custom MIBs, and Images	5
Upgrade Considerations for ExtremeControl 8.5	6
General Upgrade Information	6
Access Control Version 8.0 and newer	6
Upgrade Considerations for ExtremeWireless8.5	7
Wireless Manager Upgrade Information	7
Configuration Considerations	7
Firewall Considerations	7
Supported MIBs	7
Extreme Management Center Port List	7



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 \(GTAC\)](#).

Installation Information

When you purchased Extreme Management Center, you received a Licensed Product Entitlement ID that allows you to generate a product license key. Prior to installing Extreme Management Center, redeem your Entitlement ID for a license key. Refer to the instructions included with the Entitlement ID sent to you.

For complete installation instructions, refer to the [installation documentation](#) located on the Documentation web page:

<https://www.extremenetworks.com/support/documentation/>.

IMPORTANT: The **Governance** tab is available and supported by Extreme on an Extreme Management Center engine running the Linux operating system supplied by Extreme. Other Linux operating systems can support Governance functionality, but python version 2.7 or higher must be installed. Additionally Governance functionality requires the git, python2, python mysql module, python setuptools 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 Extreme Management Center 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 Extreme Management Center server, save them in the `appdata\VendorProfiles\Stage\MyVendorProfile\FlexViews\My FlexViews` folder.

Custom MIBs and Images

If you are deploying MIBs via the Extreme Management Center server, they are saved in the `appdata\VendorProfiles\Stage\MyVendorProfile\MIBs\` folder.

If you are deploying device images (pictures) via the Extreme Management Center server, they are saved in the `appdata\VendorProfiles\Stage\MyVendorProfile\Images\` folder.

Evaluation License

If you have requested an Extreme Management Center evaluation license, you received an Entitlement ID. This Entitlement ID allows you to generate a product evaluation license key. Refer to the instructions included with the Entitlement ID to generate the license key. Use the key when you install the product.

Evaluation licenses are valid for 30 days. To upgrade from an evaluation license to a purchased copy, contact your Extreme Networks Representative to purchase the software. Refer to the Upgrading an Evaluation License section of the *Extreme Management Center Installation Guide* for instructions on upgrading your evaluation license.

Upgrade Information

Extreme Management Center 8.5 supports upgrades from Extreme Management Center version 8.2.x (except version 8.2.2) or 8.3.x. If you are upgrading from version 8.1 or earlier of NetSight/Extreme Management Center, you must perform an intermediate upgrade. For example, if you are upgrading from Extreme Management Center 7.1, you must first upgrade to the latest Extreme Management Center 8.1 release, then upgrade to the latest Extreme Management Center 8.2 or 8.3 release, then to 8.5.

IMPORTANT: When performing an upgrade, be sure to back up the database prior to performing the upgrade, and save it to a safe location. Use the **Administration > Backup/Restore** tab to perform the backup.

Custom FlexViews, Custom MIBs, and Images

See the Custom FlexViews and Custom MIBs and Images sections in the [Important Installation Considerations](#) for additional information.

Upgrade Considerations for ExtremeControl 8.5

General Upgrade Information

When upgrading to Extreme Management Center 8.5, you are required to upgrade your ExtremeControl engine version to 8.3 or 8.2. Additionally, both Extreme Management Center and the ExtremeControl engine must be at version 8.5 in order to take advantage of the new ExtremeControl 8.5 features.

NOTE: ExtremeControl 8.5 is not supported on the 2S Series and 7S Series ExtremeControl Controllers.

You can download the latest ExtremeControl engine version at the Extreme Portal: <https://extremeportal.force.com>. Be sure to read through the *Upgrading to ExtremeControl 8.5* document (available on the **Documentation** tab of the Portal) for important information.

In addition, if your ExtremeControl solution utilizes a Nessus assessment server, upgrade your assessment agent adapter to version 8.5 if you upgrade to the ExtremeControl engine 8.5. Version 8.5 of the assessment agent adapter requires an operating system with a 64-bit architecture.

Access Control Version 8.0 and newer

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

To allow 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**

Upgrade Considerations for ExtremeWireless8.5

Wireless Manager Upgrade Information

Following a Wireless Manager upgrade, clear the Java Cache before starting the Extreme Management Center client.

Configuration Considerations

Firewall Considerations

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.

Extreme Management Center Port List

Extreme Management Center 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 (redirects to port 8443) ExtremeControl and ExtremeAnalytics engine communication

Type	Port	Description	Purpose
			Web browser access to Extreme Management Center user interface
TCP	8443	HTTPS	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) Reception of SNMP traps from all managed devices
UDP	162	SNMP Traps	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

Extreme Management Center 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	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	Internet for ExtremeControl Assessment Agent updates (extremenetworks.com) Virtual sensor communication

Type	Port	Description	Purpose
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	20505	ExtremeWireless Protocol	ExtremeWireless Controller communication
UDP	53	DNS	
UDP	123	NTP	
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

ExtremeControl Local Ports

Type	Port	Description	Purpose
TCP	22	SSH	Shell access
TCP	80	HTTP	Device software and configuration upload/download
TCP	443	HTTPS	Captive Portal listening
TCP	8080	HTTP	Captive Portal listening ExtremeControl web browser access (redirects to port 8443) Extreme Management Center communication
TCP	8080	HTTP	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 Extreme Management Center communication
TCP	8443	HTTPS	Communication between multiple ExtremeControl engines From every end-system subnet subject to ExtremeControl assessment agent in order to support agent mobility

Type	Port	Description	Purpose
TCP	8444	HTTPS	ExtremeControl web browser access (redirects to port 8443) Extreme Management Center communication Communication between multiple ExtremeControl engines
TCP	8445	HTTPS	ExtremeControl Assessment communication
UDP	123	NTP	
UDP	161	SNMP	SNMP agent managed by Extreme Management Center
UDP	1812	RADIUS authentication	ExtremeControl RADIUS server
UDP	1813	RADIUS accounting	ExtremeControl RADIUS server

ExtremeControl Remote Ports

Type	Port	Description	Purpose
TCP	389	LDAP	User-based network authentication and directory services
TCP	443	LDAPs	User-based network authentication and directory services
TCP	8080	HTTP	Extreme Management Center communication Communication between multiple ExtremeControl engines
TCP	8443	HTTPS	Extreme Management Center communication Communication between multiple ExtremeControl engines
TCP	8444	HTTPS	Extreme Management Center communication Communication between multiple ExtremeControl engines
UDP	123	NTP	
UDP	162	SNMP Trap	SNMP traps sent to Extreme Management Center
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 IP Protocols

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

ExtremeAnalytics Local Ports

Type	Port	Description	Purpose
TCP	22	SSH	Shell access
TCP	8080	HTTP	Extreme Management Center communication
TCP	8443	HTTPS	Extreme Management Center communication
UDP	123	NTP	
UDP	161	SNMP	SNMP agent managed by Extreme Management Center
UDP	2055	NetFlow	NetFlow Collector
UDP	2058	IPFIX	VMWare NSX IPFIX collector
UDP	2075	IPFIX	ExtremeXOS 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 Remote Ports

Type	Port	Description	Purpose
TCP	80	HTTP	Virtual Sensor configuration
TCP	443	HTTPS	Virtual Sensor configuration
TCP	8080	HTTP	Extreme Management Center communication
TCP	8443	HTTPS	Extreme Management Center communication
UDP	123	NTP	
UDP	162	SNMP Trap	SNMP traps sent to Extreme Management Center

Ephemeral Ports

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