6480 Via Del Oro
San Jose, CA 95119

Extreme Networks®

Extreme Management Center Configuration and Requirements

Version 8.2

8/2018
P/N: 9035981
Subject to Change Without Notice

Table of Contents

Extreme™
Customer-Driven Networking

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 Extreme Access Control, 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).

System Requirements

IMPORTANT: Extreme Management Center version 8.2 only runs on a 64-bit engine image. Any Extreme Management Center or Extreme Access Control (ExtremeControl) engine currently running a 32-bit OS image must be upgraded to the newer 64-bit image prior to upgrading to 8.2. Please contact Global Technical Assistance Center (GTAC) with any questions.

Wireless event collection is disabled by default in version 8.2 due to the increase in disk space usage required. To enable event collection, select **Enable Event Collection** on the **Administration** > **Options** > **Event Analyzer** tab.

Extreme Management Center Server and Client OS Requirements

These are the operating system requirements for both the Extreme Management Center server and remote Extreme Management Center client machines.

IMPORTANT: Only 64-bit operating systems are officially supported on the Extreme Management Center server. Any Extreme Management Center server currently running a 32-bit OS must be upgraded to a 64-bit OS.

	Operating System
Windows (qualified on the English version of the operating systems)	Windows Server® 2012 and 2012 R2 Windows Server® 2016 Windows® 7
Linux	Red Hat Enterprise Linux WS and ES v6 and v7 Ubuntu 16.04
Mac OS X® (remote Extreme Management Center client only)	El Capitan Sierra
VMware® (Extreme Management Center Virtual Engine	VMware ESXi™ 6.0 server VMware ESXi™ 6.5 server VMware ESXi™ 6.7 server vSphere (client only)™
Hyper-V (Extreme Management Center Virtual Engine)	Hyper-V Server 2012 R2 Hyper-V Server 2016

Extreme Management Center Server and Client Hardware Requirements

These are the hardware requirements for the Extreme Management Center server and Extreme Management Center client machines.

NOTES: ExtremeControl and ExtremeAnalytics are not supported on Small Extreme Management Center servers.

Extreme Management Center Server

	Small	Medium	Enterprise	Large Enterprise
Total CPUs	1	2	2	2
Total CPU Cores	8	16	16	16
Memory	16 GB	32 GB	64 GB	64 GB
Memory allocated to Java:				
-Xms -Xmx	8 GB 12 GB	12 GB 18 GB	24 GB 36 GB	24 GB 36 GB
Disk Size	240 GB	480 GB	960 GB	1.92 TB
IOPS	200	200	10,000	10,000
Recommended scale based on server configuration:				
Maximum APs	250	2,500	25,000	25,000
Maximum Wireless MUs	2,500	25,000	100,000	100,000
Maximum Managed Devices	100	1,000	10,000	10,000
ExtremeControl End-Systems	N/A	50,000	200,000	200,000
Statistics Retention (Days)	90	180	180	360
ExtremeAnalytics	No	Yes	Yes	Yes
MU Events	No	Yes	Yes	Yes

Extreme Management Center Client

	Requirements
CPU Speed	3.0 GHz Dual Core Processor
Memory	8 GB (4 GB for 32-bit OS)
Disk Size	300 MB (User's home directory requires 50 MB for file storage)
Java Runtime Environment (JRE) (Oracle Java only)	Version 8
Browser* (Enable JavaScript and Cookies)	Microsoft Edge (version 41.16.199.10000.0 in compatibility mode) Internet Explorer (version 11 in compatibility mode) Mozilla Firefox (version 34 or later*) Google Chrome (version 33.0 or later)

*Browsers set to a zoom ratio of less than 100% may not display Extreme Management Center properly (e.g. missing borders around windows). Setting your browser to a zoom ratio of 100% corrects this issue.

**When accessing Extreme Management Center using Firefox version 59.0.1 on a non-touchscreen system on which a Windows operating system is installed, the vertical scroll arrows do not display.

Virtual Engine Requirements

The Extreme Management Center, Extreme Access Control, and Extreme Application Analytics virtual engines must be deployed on a VMWare or Hyper-V server with a disk format of VHDX.

- The VMWare Extreme Management Center virtual engines are packaged in the .OVA file format (defined by VMware).
- The Hyper-V Extreme Management Center virtual engines are packaged in the .ZIP file format.

IMPORTANT: For ESX and Hyper-V servers configured with AMD processors, the Extreme Application Analytics virtual engine requires AMD processors with at least Bulldozer based Opterons.

Extreme Management Center Virtual Engine Requirements

	Small	Medium	Large
Total CPU Cores	8	16	16
Memory	16 GB	32 GB	64 GB
Memory allocated to Java:			
-Xms	8 GB	12 GB	24 GB
-Xmx	12 GB	18 GB	36 GB
Disk Size	240 GB	480 GB	960 GB
IOPS	200	200	10,000
Recommended scale based on server configuration:			
Maximum APs	250	2,500	25,000
Maximum Wireless MUs	2,500	25,000	100,000
Maximum Managed Devices	100	1,000	10,000
Extreme Access Control End-Systems	N/A	50,000	200,000
Statistics Retention (Days)	90	180	180
Application Analytics	No	Yes	Yes

	Small	Medium	Large
MU Events	No	Yes	Yes

Extreme Access Control (ExtremeControl) Virtual Engine Requirements

	Small	Medium	Enterprise
Total CPU Cores	8	16	16
Memory	12 GB	16 GB	32 GB
Disk Size	40 GB	120 GB	120 GB
IOPS	200	200	200

Recommended scale based on server configuration:			
ExtremeControl End-Systems	3,000	6,000	9,000/12,000[1]
Authentication	Yes	Yes	Yes
Captive Portal	No	Yes	Yes/No[1]
Assessment	No	Yes	No

[1]The Enterprise Extreme Access Control engine configuration supports two different scale options:

- Up to 9,000 end-systems if your network uses Captive Portal functionality.
- Up to 12,000 end-systems if your network does not use Captive Portal functionality.

Extreme Application Analytics Virtual Engine Requirements

	Small	Medium	Enterprise
Total CPU Cores	8	16	16
Memory	12 GB	32 GB	64 GB
Disk Size	40 GB	480 GB	960 GB
IOPS	200	10,000	10,000

Recommended scale based on server configuration:			
Flows Per Minute	250,000	500,000	750,000

IMPORTANT: The ESXi free license supports a maximum of 8 CPU cores, while the medium and enterprise Extreme Application Analytics virtual engine installation require 16 CPU cores. This is only available by purchasing a permanent license. To use the Extreme Application Analytics virtual engine with an ESXi free license, adjust the number of CPU cores to 8.

Ensure at least 4 GB of swap space is available for flow storage on the Extreme Application Analytics virtual engine or impaired functionality may occur. Use the `free` command to verify the amount of available RAM on your Linux system.

Fabric Manager Requirements

	Requirements
Total CPU Cores	4
Memory	9 GB
Memory allocated to Java:	
-Xms	4 GB
-Xmx	6 GB
Disk Size	60 GB

ExtremeControl Agent OS Requirements

The table below outlines the supported operating systems for end-systems connecting to the network through an Extreme Networks ExtremeControl deployment that is implementing agent-based assessment. Additionally, the end-system must support the operating system disk space and memory requirements as provided by Microsoft® and Apple®.

	Operating System	Operating System Disk Space	Available/Real Memory
Windows*	Windows Vista Windows XP Windows 2008 Windows 2003 Windows 7 Windows 8 Windows 8.1 Windows 10	80 MB	40 MB (80 MB with Service Agent)
Mac OS X	Tiger Snow Leopard Lion Mountain Lion Mavericks Yosemite El Capitan Sierra	10 MB	120 MB

***NOTE:** Certain assessment tests require the Windows Action Center (previously known as Windows Security Center), which is supported on Windows XP SP2+, Windows Vista, and Windows 7, Windows 8, and Windows 8.1 operating systems.

Extreme Access Control Agent support for Antivirus/Firewall products includes, but is not limited to, the following families of products:

- McAfee
- Norton
- Kaspersky
- Trend Micro
- Sophos

Extreme Access Control Agent operating system support for the above products includes the latest Windows/Mac OS X versions currently available at the time of product release. Not all features of all products may be supported. For additional information on specific issues, see Known Issues and Limitations.

ExtremeControl Supported End-System Browsers

The following table outlines the supported desktop and mobile end-system browsers connecting to the network through the Mobile Captive Portal of Extreme Networks ExtremeControl.

	Browser	Version
Desktop	Microsoft Edge	41 and later
	Microsoft Internet Explorer	11 and later
	Mozilla Firefox	34 and later
	Google Chrome	33.0 and later
Mobile	Internet Explorer Mobile	11 and later (Windows Phone)
	Microsoft Edge	All versions
	Microsoft Windows 10 Touch Screen Native (Surface Tablet)	N/A
	iOS Native	9 and later
	Android Chrome	4.0 and later
	Android Native	4.4 and later
	Dolphin	All versions
	Opera	All versions

NOTES: A native browser indicates the default, system-installed browser. Although this may be Chrome (Android), this also includes the default, system-controlled browser used for a device's Captive Network Detection. Typically, this is a non-configurable option for Wi-Fi Captive Network Detection, but default Android, Microsoft of iOS devices are tested for compatibility with the Mobile Captive Portal.

A mobile device can access the standard (non-mobile) version of the Captive Portal using any desktop-supported browsers available on a mobile device.

For other browsers, the Mobile Captive Portal requires the browser on the mobile device be compatible with Webkit or Sencha Touch.

To confirm compatibility with Webkit or Sencha Touch, open `http://<Access Control Engine IP>/mobile_screen_preview` using your mobile web browser.

- If the browser is compatible, the page displays properly.
- If the browser is not compatible with the Mobile Captive Portal, the following error appears:

Extreme Access Control (ExtremeControl) Engine Version Requirements

For complete information on Access Control engine version requirements, see the Upgrade Information section of these Release Notes.

ExtremeControl VPN Integration Requirements

This section lists the VPN concentrators supported for use in Extreme Access Control VPN deployment scenarios.

Supported Functionality: Authentication and Authorization (policy enforcement)
Cisco ASA
Enterasys XSR

Supported Functionality: Authentication
Juniper SA (requires an S-Series Stand Alone (SSA) system in order to provide access control)

NOTE: For all Extreme Access Control VPN Deployment scenarios, an S-Series Stand Alone (SSA) system is required to change authorization levels beyond the initial authorization, for example, when using assessment.

ExtremeControl SMS Gateway Requirements

The following SMS Gateways have been tested for interoperability with ExtremeControl:

- Clickatell
- Mobile Pronto

Other SMS Gateways that support the SMTP API should be able to interoperate with ExtremeControl, but have not been officially tested.

ExtremeControl SMS Text Messaging Requirements

The following mobile service providers are supported by default for SMS text messaging in an ExtremeControl deployment. Additional service providers can be added:

AT&T	SunCom
Alltel	T-Mobile
Bell Mobility (Canada)	US Cellular
Cingular	Verizon
Metro PCS	Virgin Mobile (Canada)
Rogers (Canada)	Virgin Mobile
Sprint PCS	

ExtremeAnalytics Requirements

To use an ExtremeSwitching X440-G2 switch as an Application Telemetry source for ExtremeAnalytics, install firmware version `22.4.1.4-patch2-5` or higher.

Ekahau Maps Requirements

Extreme Management Center supports importing Ekahau version 8.x maps in .ZIP format.

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 NetSight Server service may not start after installing Extreme Management Center version 8.0 on a system on which a Windows Server operating system is installed. Restarting Windows corrects this issue.

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 re-installing 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, they are saved in the `appdata\VendorProfiles\Stage\MyVendorProfile\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 8.2 supports upgrades from Extreme Management Center version 8.1 only. If you are upgrading from a NetSight/Extreme

Management Center version prior to 8.1, you must perform an intermediate upgrade. For example, if you are upgrading from Extreme Management Center 7.1.3, you must first upgrade to Extreme Management Center 8.0, then to version 8.1, and then upgrade to Extreme Management Center 8.2.

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.

The NetSight Server service may not start after upgrading Extreme Management Center to version 8.0 on a system on which the Windows Server 2008 operating system is installed. Restarting Windows corrects this issue.

When upgrading the Application Analytics engines to version 8.2 after upgrading from version 6.1 to 7.1.3, the upgrade does not complete successfully. To successfully upgrade the engine to version 8.2 after upgrading from version 6.1 to 7.1.3, enter `dpkg --purge postgresql*` in the command line, then upgrade the Application Analytics engine to version 8.2.

Important Upgrade Considerations

- When upgrading the Extreme Management Center server, Application Analytics engine, or Extreme Access Control (ExtremeControl) engine to version 8.2, ensure the DNS server IP address is correctly configured.
- Upgrading to Extreme Management Center version 8.2 requires an internet connection and upgrades the Ubuntu version to 16.04. If no internet connection is available, see Migrating or Upgrading to a 64-bit Extreme Management Center Engine.

IMPORTANT: If a network proxy is required to access the internet, perform the following steps:

1. Enter one of the following commands, depending on your configuration:
   - `export http_proxy=http://`*`yourproxyaddress`*`:`*`proxyport`* if a username and password are not required.
   - `export http_proxy=http://`*`username`*`:`*`password`*`@`*`yourproxyaddress`*`:`*`proxyport`* if a username and password are required.
2. Run the binary upgrade for the engine.

- When upgrading to Extreme Management Center version 8.2, ensure the -Xms and -Xmx settings in the `nsserver.cfg` file are set to the values defined in the Requirements table and then restart the server:
  - On a server running a Linux operating system, enter `service nsserver restart` in the command line to restart the server.
  - On a server running a Windows operating system, right-click the NetSight Services Manager icon in the notification area of the task bar and select NetSight Server > Restart Server to restart the server.
- When upgrading a 64-bit Extreme Management Center server or when upgrading from a 32-bit to a 64-bit Extreme Management Center server, if the -Xmx setting is set below 1536m, it increases to 1536m.

NOTE: The `nsserver.cfg` file is located in the `<install directory>\NetSight\services` folder.

- If your network is using Extreme Application Analytics engines, you must first perform the Extreme Management Center upgrade to version 8.2 and then add the Extreme Application Analytics engines.
- If you are running Data Center Manager (DCM), a Mobile Device Management (MDM) integration, or other ExtremeConnect or Fusion integration with Extreme Management Center, or are accessing Web Services directly or through ExtremeConnect, you need to install an Extreme Management Center Advanced (NMS-ADV) license. Contact your Extreme Networks Representative for information on obtaining this license.

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 8.2

General Upgrade Information

When upgrading to Extreme Management Center 8.2, you are required to upgrade your Extreme Access Control (ExtremeControl) engine version to 8.0 or 8.2. Additionally, both Extreme Management Center and the Extreme Access Control engine must be at version 8.2 in order to take advantage of the new Extreme Access Control 8.2 features.

NOTE: Extreme Access Control 8.2 is not supported on the 2S Series and 7S Series Extreme Access Control Controllers.

You can download the latest Extreme Access Control engine version at the Extreme Portal: https://extremeportal.force.com. Be sure to read through the *Upgrading to Extreme Access Control 8.2* 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 8.2 if you upgrade to the Extreme Access Control engine 8.2. Version 8.2 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 ExtremeWireless 8.2

Wireless Manager Upgrade Information

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

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 Extreme Access Control Dashboard.
- Port 8444 (Default HTTPS traffic) must be accessible through firewalls for clients to access the Extreme Access Control (ExtremeControl) Engine Administration web pages.
- The following port must be accessible through firewalls for the Extreme Management Center Server and an Extreme Access Control Assessment Server to communicate:
  TCP: 8445
- The following ports must be accessible through firewalls for the Extreme Management Center Server and an Extreme Access Control engine to communicate:
  Required Ports (all bi-directionally)
  TCP: 4589, 8080, 8443, 8444
  UDP: 161, 162
- The following port must be accessible through firewalls for Extreme Access Control engine to Extreme Access Control engine communication:
  TCP: 8444
- The following ports must be accessible through firewalls for Extreme Access Control engine-to-Extreme Access Control 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 Extreme Access Control assessment agent to every Extreme Access Control 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 (bi-directionally) through firewalls for the Extreme Management Center Server and an Extreme Application Analytics engine to communicate:
  TCP: Ports 4589, 8080, 8443
  UDP: Ports 161, 162
  To Extreme Application Analytics engine:
  UDP: Port 2055 (NetFlow)
  TCP: 22, 8443

  For GRE Tunnels to the Extreme Application Analytics engine IP Protocol 47
- Port 2055 must be accessible through firewalls for the Extreme Management Center Server to receive NetFlow data.

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.

August, 2018
P/N: 9035981