Extreme Management Center® Configuration and Requirements Version 8.2

12/2018
9035981-01
Subject to Change Without Notice

Table of Contents

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).

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, 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 8.2 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 `/etc/init.d/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.