Extreme Management Center® Release Notes
Version 8.2

Table of Contents

Extreme Management Center Version 8.2 Release Notes

Extreme Management Center
8.2.1.57
November, 2018

Extreme Networks Extreme Management Center® provides a 360 degree view of your network, users, devices, and applications by providing integrated management, analytics, and policy. It allows you to view your network through a single pane of glass to manage your network from the wired and wireless edge to the data center. Extreme Management Center gives granular insights, visibility, and automated control across your networks.

With Extreme Management Center, you can distingush network from application performance and correlate with user and device activities to troubleshoot issues fast. Actionable insights from the network let you make real-time decisions on policies, devices, applications, and people. This way, the implementation of new technologies, such as IoT, can be automated and securely executed.

A better way to manage your complex network from the network edge to the data center

We integrated Extreme Management Center with our Smart OmniEdge solution and Automated Campus, so you can quickly deploy new digital technology, prevent cyber-attacks at every entry point, and do it all while delivering a consistent and personalized user experience.

High levels of virtualization, containerization and cloud environments, combined with enormous traffic, limit visibility in the modern data center. In addition, most data centers face challenges adapting to rapid business changes and virtual environments. Most customers have also grown tired of vendor lock-in and want an open flexible environment. Here Extreme Management Center, part of our Agile Data Center Networking solution, provides a pragmatic path to automation based on multi-vendor architectures. It gives you the granular visibility and real-time analytics, to make data-based business decisions. Our SLX switches and routers are managed by Extreme Management Center through a single pane of glass, which reduces data center administration and offers you the full view of the network.

The Extreme Management Center Release Notes provide information on the new features and enhancements included in version 8.2, as well as issues fixed and configuration changes for this release.

> **IMPORTANT:** For upgrade and installation requirements as well as configuration considerations, please see Extreme Management Center Configuration and Requirements.

The most recent version of these release notes as well as the most recent firmware compatibility matrix can be found on the Extreme Networks Documentation site: https://www.extremenetworks.com/support/release-notes. Follow this path to the document: Management and Orchestration > Extreme Management Center > Release 8.2.

For information regarding the features supported by specific devices, see the Firmware Support Matrix. Version 8.2 of Extreme Management Center supports the devices listed in the matrix as well as additional devices not yet included.

1. Enhancements in Version 8.2

New features and enhancements are added to the following areas in Extreme Management Center version 8.2:

- Extreme Management Center
- ExtremeControl
- ExtremeAnalytics
- Information Governance Engine

For additional information about each of the features listed in this guide, refer to the documentation posted online at ExtremeNetworks.com or the help system included with the software.

1.1 Extreme Management Center

- Introducing Fabric Manager
- Ability to Provision Fabric Topologies in Extreme Management Center
- Introducing the Multi Cloud Dashboard
- Ability to Export Rows You Select

- [Added Support for Additional Device Types](#)

- [Added Link Resolution Support for Additional Devices in Topology Maps](#)

Introducing Fabric Manager

Extreme Management Center version 8.2 provides support for Fabric Manager functionality in Extreme Management Center. Fabric Manager is deployed as a separate virtual machine in Extreme Management Center. Fabric Manager allows you to monitor the fabric topology on your network for the following device types:

- ERS35xx with firmware version 5.3.7 and later

- ERS36xx with firmware version 6.2.0 and later

- ERS48xx with firmware version 5.12.0 and later

- ERS49xx with firmware version 7.6.0 and later

- ERS59xx with firmware version 7.6.0 and later

- VSP7024 with firmware version 10.4.6 and later

- VSP4xxx with firmware version 6.1.3 and later

- VSP7xxx with firmware version 6.1.3 and later

- VSP8xxx with firmware version 6.1.3 and later

NOTE: For minimum requirements, see [Extreme Management Center Configuration and Requirements](#).

Extreme Management Center uses ZTP+ functionality to add Fabric Manager and is accessed via site to which you add it.

Extreme Management Center can also backup, restore, and upgrade the Fabric Manager virtual machine configuration within Extreme Management Center. To add Fabric Manager, upgrade Extreme Management Center to version 8.2.0 and follow the installation instructions.

Additionally, certificate management is updated and viewed in Extreme Management Center.

Ability to Provision Fabric Topologies in Extreme Management Center

Extreme Management Center now allows you to provision fabric topologies on your fabric-enabled devices. Via the **Site** tab, you can configure services, service applications, and service definitions. A service definition that includes a complete set of services is assigned to a site, which defines the fabric topologies for devices within a site.

Introducing the Multi Cloud Dashboard

The Multi Cloud dashboard provides an overview of all virtual machines on the network broken down into VM distribution. Additionally, the dashboard includes information about Amazon Web Service and Google Compute instances.

Ability to Export Rows You Select

Extreme Management Center now allows you to export only the rows you select in tables as a CSV file.

Added Support for Additional Device Types

Extreme Management Center now supports the MLX and VDX device types:

- Extreme Management Center supports inventory functionality via the **Workflows** tab

- Device Backup and Restore supported with firmware version 6.0.2 and later

- Device Firmware Upgrade support:

  - Upgrade from firmware version 6.0.2 (Logical Chassis mode) and 7.0 to 7.1.0

  - Upgrade from firmware version 7.1.0 to later versions

- Other device support supported with firmware version 7.1.0 and later

Added Link Resolution Support for Additional Devices in Topology Maps

Extreme Management Center topology maps now display links between additional device types, including:

- ERS35xx

- ERS36xx

- ERS45xx

- ERS48xx

- ERS49xx

- ERS59xx

- ERS55xx

- ERS56xx

- ERS86xx

- ERS88xx

- VSP9xx
- VSP7024

If one of these devices is at either end of a link, Extreme Management Center uses SONMP information to display the link in the map.

1.2 ExtremeControl

Ability to Join Multiple Active Directory Domains

ExtremeControl now allows you to join multiple Active Directory domains. This new capability facilitates authenticating users that may reside on Active Directories that do not have trust between them.

Fall-Through Authentication for AD/LLDP

Beginning in ExtremeControl version 8.2, you can configure multiple AAA authentication rules by which to authenticate an end-user. This functionality provides you with the ability to fall-through and authenticate against the next AAA authentication rule in the event the authentication configured as the first AAA authentication rule results in authentication failure or the Directory Service is unreachable.

SLX Endpoint Tracking

Beginning in ExtremeControl version 8.2, you can dynamically assign VLANs to VM applications connecting to SLX in the Data Center. ExtremeConnect now integrates with VMware vCenter to receive data about instantiating and motion of VMs to facilitate the dynamic assignments of VLANs.

ExtremeControl Policy Now Supports the ExtremeCloud Appliance

The policy roles you configure via the **Policy** tab in Extreme Management Center now support the ExtremeCloud Appliance. When accessing your wireless network via the ExtremeCloud Appliance, a wireless controller with integrated ExtremeControl functionality, users are automatically assigned a policy role that defines their level of access on the network.

Migration of NAC Manager Functionality into ExtremeControl

Beginning in ExtremeControl version 8.2.0, two of the remaining legacy java NAC Manager application tools are migrated to ExtremeControl:

- Configuration Evaluation Tool
- NAC Notification Engine

1.3 ExtremeAnalytics

- ExtremeAnalytics Locations Now Included in Sites
- Top Servers for Tracked Applications Report Now Available
- Ability to Collect Flow Information on VSP Devices
- Historical Application Flow Information Now Available
- Ability to View Packet Capture Data from Application Flows

ExtremeAnalytics Locations Now Included in Sites

End-system locations formerly configured in the **Analytics** tab are now part of the network sites. Unifying the sites with the end-system locations allows hierarchical organization and reporting of end systems, application usage, and user experience. Additionally, flows from or to external networks are tagged with the Country or cloud provider region (e.g. "France" or "AWS us-east-1").

> **IMPORTANT:** To map existing locations to sites, access the **Devices** tab and select a site. Select the **Endpoint Locations** tab in the right-panel. Locations that are not yet associated with a site contain a broken link icon ( ) icon. Right-click the location, select Assign to Site, and select a site from the drop-down menu.

Top Servers for Tracked Applications Report Now Available

ExtremeAnalytics now includes the Top Servers for Tracked Applications report, displaying the servers with highest number of clients, application bandwidth, or response time. Tracking these statistics for each server separately provides useful data for trouble-shooting user-experience issues.

Ability to Collect Flow Information on VSP Devices

Via Application Telemetry, ExtremeAnalytics now allows you to configure the following device types as flow sources:

- VSP86xx with firmware version 6.2 and later
- VSP4xxx, VSP72xx, VSP82xx, and VSP84xx with firmware version 7.1 and later

Historical Application Flow Information Now Available

Detailed flow information is stored for up to five days on the Application Analytics engine to allow for analysis of network usage by a client or server before, during, or after an incident.

Ability to View Packet Capture Data from Application Flows

You can initiate a packet capture for any device or end-system on the network. The resulting pcap files are stored on the Application Analytics engine and can be downloaded for inspection within Wireshark or other pcap utility.

1.4 ExtremeConnect

- VMware vShpere Enhancements
- Amazon Web Services Enhancements
- Google Compute Enhancements

VMware vSphere Enhancements

Extreme Management Center version 8.2 includes the following VMware vSphere enhancements:

- Import a Hypervisor as a device into Extreme Management Center for visibility.
- View virtual machine end-systems in ExtremeControl via end-system events without using RADIUS.
- Use virtual network architecture mapping on VXLAN port group formatting.

Amazon Web Services Enhancements

Extreme Management Center version 8.2 includes the following Amazon Web Services (AWS) enhancements:

- Create Extreme Management Center switches for AWS subnets.
- Create Extreme Management Center switch ports for instance interfaces connected to AWS subnets.
- View AWS instance reports in the Multi Cloud dashboard, now included on the **Network** > **Dashboard** tab.

Google Compute Engine Enhancements

Extreme Management Center version 8.2 includes the following Google Compute Engine enhancements:

- Create Extreme Management Center switches for Google subnets.
- Create Extreme Management Center switch ports for instance interfaces connected to Google subnets.
- View Google instance reports in the Multi Cloud dashboard, now included on the Network > Dashboard tab.

1.5 Information Governance Engine

Your version of IGE is automatically upgraded when installing Extreme Management Center 8.2. The new version provides you with support for ICX, MLX, SLX, and VDX, devices. Regimes and audit tests you create in version 8.1 are retained following the upgrade.

- Ability to Test ICX, MLX, SLX, and VDX Devices
- Ability to Schedule Email of Governance Results
- Usability Improvements

Ability to Test ICX, MLX, SLX, and VDX Devices
Extreme Management Center version 8.2.0 adds support for ICX, MLX, SLX, and VDX devices in IGE. You can now test your ICX, MLX, SLX, and VDX devices using audit tests in the PCI, HIPPA, and GDPR compliances, which evaluate your devices for firewall and management policy for security measures. These tests are designed to monitor the network for threats, penetrations, and intrusions.

Ability to Schedule Email of Governance Results
Beginning in Extreme Management Center 8.2.0, you can create a scheduled task that automatically emails the most recently run governance test as a PDF to an email address or list of addresses you configure.

Usability Improvements
The **Audit Tests** tab is improved in version 8.2.0 to provide better operating system filtering and improved usability.

2. Deprecated Features

There are no deprecated features in Extreme Management Center version 8.2.

3. Known Issues Addressed

3.1 Known Issues Addressed in 8.2.1.57

Extreme Management Center Issues Addressed	ID
Bookmarking a page in the Devices view and then accessing the bookmarked page was loading the **Dashboard** tab.	01412328
Attempting to upgrade the firmware on an ICX device is not completing successfully and displays a "Device did not reset- system uptime did not reset" error message. To upgrade the firmware, configure "com.extreme.scripting.commandTimeoutInMillis=5" in NSJBoss.properties file.	------
Attempting to upgrade the firmware on an ICX device using the ICX-TFTP script is not completing successfully when 'aaa authentication enable' is configured on the device. The upgrade the firmware, configure 'aaa authentication enable implicit-user' on the device.	------
ZTP+ devices added to Extreme Management Center before LLDP wait time expired was causing ports not to resolve from **ZTPPlusLLDPPending** role to the proper port **Configuration** on the **Site** > **Port Templates** tab.	------
The **Configuration** field on the **Site** > **Port Templates** tab was showing the internal port role **ZTPPlusLLDPPending** as a configurable option.	------
Clicking **Save** after editing a script that is saved as a task caused Extreme Management Center to become unresponsive.	01731269
Running a CLI script was slow to complete and generating timeout errors.	1730619
Clicking the **Save Task** button in the **Run Workflow** window and entering a **Task Name** window was causing Extreme Management Center to become unresponsive until you refresh.	------
Statistics Collection was occasionally not working properly for wireless controllers.	01740273
The Devices table on the Devices tab had two columns named **Status**.	------
ExtremeAnalytics Issues Addressed	**ID**

Using NetFlow to view flow information in ExtremeAnalytics was causing the following error to display: ERROR [FlowBaseSocket] Exception: null.	01735172

ExtremeControl Issues Addressed	**ID**
Clients attempting to connect to the network via guest registration were receiving an "Unknown error has occurred" error message.	------
Clicking **Edit** in the Authentication Rules table was causing the value in the **User/MAC/Host** field to be lost.	------
Attempting to enforce policy on X440G2 devices in a stacked configuration was occasionally not completing successfully because the device type was misidentified in Extreme Management Center.	1545397
Using the Captive Portal to perform HTTPS operations was resulting in poor performance.	------

3.2 Known issues addressed in 8.2.0.89:

Extreme Management Center Issues Addressed	**ID**
The status of an MLAG with a fiber link for control was incorrectly reported.	1218049
The Device Tree, when configured to display devices using the **System Name** format, was not using the system name for sort order.	1245000
Alarms that occurred on devices could not be cleared from the **Devices** tab, only from the **Alarms and Events** tab. Via the right-click menu, you can now clear alarms on the **Devices** tab.	------
The Extreme Management Center Webserver was not closing client connections effectively, which led to the server becoming unresponsive.	1392392
Users were unable to log into Extreme Management Center when using RADIUS authentication, if the RADIUS server was using a non-default port for authentication requests.	1549889
Filters applied to column data on the **Events** tab were not being applied when the page data automatically refreshed.	1726112

4. Upgrade, Installation, and Configuration Changes

4.1 Important Upgrade Considerations

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.

4.2 ExtremeWireless Upgrade Information

As of version 8.1.4, Extreme Management Center now supports the ExtremeCloud Appliance. This version now includes support for high-level ciphers, which allow Extreme Management Center to communicate with both the ExtremeCloud Appliance and ExtremeWireless version 10.41.

IMPORTANT: For ExtremeWireless controllers on which version 10.41.01 or later is installed to synchronize with Extreme Management Center version 8.1.4 or later, you need to disable the use of weak ciphers. Enter the following commands to support higher ciphers:

```
secureconnection
weak-ciphers disable
message-bus-ciphers AES128-SHA256 3
```

A warning displays stating the following:

```
Warning: [AES128-SHA256] contains no NetSight client
ciphers....
```

Ignore the warning and enter `apply` in the command line.

Verify the setting is configured properly by entering the following:

```
EWC.extremenetworks.com:secureconnection# show
```

If properly configured, the following message displays:

```
Weak Ciphers: disable
Message Cipher: AES128-SHA256 3
```

4.3 ExtremeAnalytics Upgrade Information

Enabling or disabling the disk flow export feature may cause enforce operations to time out. Enforcing again resolves the issue.

ZTP+ managed Summit G2 devices cannot be selected as an Application Telemetry source.

4.4 ExtremeControl Installation Information

Immediately after installing version 8.2 on the Access Control engine, the date and time does not properly synchronize and the following error message displays:

```
WARNING: Unable to synchronize to a NTP server. The time may
not be correctly set on this device.
```

Ignore the error message and the date and time automatically synchronize after a short delay.

4.5 VDX Device Configuration Information

To properly discover interfaces and links for VDX devices in Extreme Management Center, enable `three-tuple-if` on the device.

NOTE: To enable `three-tuple-if` on the device in Extreme Management Center:

1. Access the **Network** > .
2. Right-click on the device in the Devices table.
3. Select **Tasks** > **Config** > **VDX Config Basic Support**.

---

5. Getting Help

If you require assistance, contact Extreme Networks using one of the following methods.

- [Global Technical Assistance Center (GTAC) for Immediate Support](#)
  - **Phone:** 1-800-998-2408 (toll-free in U.S. and Canada) or 1-603-952-5000. For the Extreme Networks support phone number in your country, visit: www.extremenetworks.com/support/contact
  - **Email:** support@extremenetworks.com. To expedite your message, enter the product name or model number in the subject line.
- [GTAC Knowledge](#) — Get on-demand and tested resolutions from the GTAC Knowledgebase, or create a help case if you need more guidance.
- [The Hub](#) — A forum for Extreme customers to connect with one another, get questions answered, share ideas and feedback, and get problems solved. This community is monitored by Extreme Networks employees, but is not intended to replace specific guidance from GTAC.
- [Support Portal](#) — Manage cases, downloads, service contracts, product licensing, and training and certifications.

Before contacting Extreme Networks for technical support, have the following information ready:

- Your Extreme Networks service contract number and/or serial numbers for all involved Extreme Networks products
- A description of the failure
- A description of any action(s) already taken to resolve the problem
- A description of your network environment (such as layout, cable type, other relevant environmental information)
- Network load at the time of trouble (if known)
- The device history (for example, if you have returned the device before, or if this is a recurring problem)
- Any related Return Material Authorization (RMA) numbers