6480 Via Del Oro
San Jose, CA 95119

# Extreme Networks®

## *Extreme Management Center Release Notes*

## Version 8.2

9/2018
P/N: 9035219-04
Subject to Change Without Notice

# Table of Contents

# Extreme Management Center Version 8.2 Release Notes

Extreme Management Center
8.2.0.89
September, 2018

**IMPORTANT:** This version of Extreme Management Center is a beta release and is not intended for use in a production environment.

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.

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
- Added Support for Additional Device Types

**Introducing Fabric Manager**

Extreme Management Center version 8.2.0 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.

**NOTE:** Fabric configuration support in Extreme Management Center is expected in a future 8.2 release.

### 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

## 1.2 ExtremeControl



### 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



**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**

An ExtremeAnalytics user 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 Information Governance Engine

Your version of IGE is automatically upgraded when installing Extreme Management Center 8.2.0. The new version provides you with support for ICX, MLX, VDX, and MLXe 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**

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 you 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 8.2.0.89:

| 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. Installation, Upgrade, 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 ExtremeControl Installation Information

Immediately after installing version 8.2.0 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.

# 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