

DRAFT



Extreme Management Center[®] Release Notes Version 8.2

DRAFT

DRAFT

DRAFT

DRAFT

12/2018
9035977-03
Subject to Change Without Notice

Table of Contents

Extreme Management Center® Release Notes Version 8.2	1
Table of Contents	2
Extreme Management Center Version 8.2 Release Notes	5
1. Enhancements in Version 8.2	6
1.1 Engines	6
1.1 Extreme Management Center	7
1.2 ExtremeControl	10
1.3 ExtremeAnalytics	12
1.4 ExtremeConnect	13
1.5 Information Governance Engine	14
2. Deprecated Features	15
3. Known Issues Addressed	15
3.1 Known Issues Addressed in 8.2.3.67	15
3.2 Known Issues Addressed in 8.2.1.57	18
3.2 Known issues addressed in 8.2.0.89	19
3.3 Vulnerabilities Addressed	20
4. Upgrade, Installation, and Configuration Changes	21
4.1 Important Upgrade Considerations	21
4.1.1 License Renewal	21
4.1.2 Internet Connection	21
4.2 ExtremeAnalytics Upgrade Information	21
4.3 Fabric Manager Upgrade Information	22
4.4 ExtremeControl Installation Information	22

4.5 VDX Device Configuration Information	22
4.6 VSP Device Configuration Information	23
5. System Requirements	23
5.1 Extreme Management Center Server and Client OS Requirements	23
5.2 Extreme Management Center Server and Client Hardware Requirements	24
Extreme Management Center Server	24
Extreme Management Center Client	25
5.3 Virtual Engine Requirements	25
5.3.1 Extreme Management Center Virtual Engine Requirements	26
5.3.2 Extreme Access Control (ExtremeControl) Virtual Engine Requirements	26
5.3.3 Extreme Application Analytics Virtual Engine Requirements	27
5.3.4 Fabric Manager Requirements	27
5.4 ExtremeControl Agent OS Requirements	27
5.5 ExtremeControl Supported End-System Browsers	28
5.6 Extreme Access Control (ExtremeControl) Engine Version Requirements	30
5.7 ExtremeControl VPN Integration Requirements	30
5.8 ExtremeControl SMS Gateway Requirements	30
5.9 ExtremeControl SMS Text Messaging Requirements	31
5.10 ExtremeAnalytics Requirements	31
5.11 Ekahau Maps Requirements	31
5.12 Guest and IoT Manager Requirements	31
5.12.1 Guest & IoT Manager Server OS Requirements	31
5.12.2 Guest & IoT Manager Outlook Add-in Client Requirements	32

5.12.3 Guest and IoT Manager Virtual Engine Requirements	32
5.12.4 Guest and IoT Manager Supported Browsers	32
6. Getting Help	33

DRAFT

DRAFT

DRAFT

DRAFT

Extreme Management Center Version 8.2 Release Notes

Extreme Management Center
8.2.3.67
December, 2018

NOTE: This is a controlled availability release. Some of the features included in Extreme Management Center version 8.2.3 are still under active development. See the list of features that are not yet complete [here](#).

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 distinguish 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 Engines

- [Enhancement to SNMPv3 Configuration on Extreme Networks Engines](#)

Enhancement to SNMPv3 Configuration on Extreme Networks Engines

During initial engine deployment, you can now configure the SNMPv3 authentication (MD5 or SHA) and privacy (DES or AES) protocol that was previously hard-coded on the Extreme Management Center, Application Analytics, and Access Control engines.

1.1 Extreme Management Center

- [Introducing Workflows](#)
- [Ability to Hide Link Labels on Maps](#)
- [Ability to Configure Local Change Alarm on ZTP+ Devices](#)
- [NMS License Enhancements](#)
- [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 Workflows

Workflows allow you to automate complex tasks with a single click. Workflows are modeled as flow charts and can be configured to perform one set of actions that take place if an action occurs successfully and another set of actions that take place if the action does not occur successfully. System-defined workflows are available for all users. With an NMS-ADV license, you can create your own workflows that can be scheduled, or run ad hoc.

Ability to Hide Link Labels on Maps

The **Show Interswitch Connection** selection in the **View** menu of a map now includes a menu from which you can enable or disable map link labels.

Ability to Configure Local Change Alarm on ZTP+ Devices

Via the **Alarm on Local Change** option on the **Options > ZTP+** tab, you can now configure Extreme Management Center to generate an alarm when you make a change to a ZTP+-enabled device via the CLI to prevent Extreme Management Center from automatically overwriting the change the next time Extreme Management Center polls the device via ZTP+.

NMS License Enhancements

The NMS-xx license now provides support for 250 end-systems for ExtremeControl and 25 Guest and IoT Manager licenses. NMS-ADV-xx continues to support 500 end-systems and now includes 50 Guest and IoT Manager licenses.

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. A Fabric Topology and Service definition are created in a configuration template. Via the **Site** tab, you can assign a site a Fabric Topology

and Service Definition template. The Service definition template allows you to create L2 and L3 service mappings.

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
- General device support:
 - MLX – All firmware versions
 - VDX – Firmware version 7.1.0 and later
- Additional VDX-only support includes:
 - 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

- [Introducing Guest and IOT Manager](#)
- [Ability to Join Multiple Active Directory Domains](#)
- [Fall-Through Authentication for AD/LLDP](#)
- [ExtremeControl Policy Now Supports the ExtremeCloud Appliance](#)
- [Migration of NAC Manager Functionality into Extreme Management Center](#)

Introducing Guest and IOT Manager

Beginning in ExtremeControl version 8.2, a new set of User and Device provisioning is now available, called Guest and IoT Manager. The Guest & IoT Manager (GIM) is an application that integrates with ExtremeControl. Its purpose is to provide non-IT personnel with the ability to provision users and/or devices within constraints defined by the administrator. GIM communicates with an Access Control (ExtremeControl) engine(s) for provisioning of users and devices that later may access the network through standard process of authentication and authorization by ExtremeControl.

GIM allows the administrator to perform the following:

- Create and customize Onboarding Templates for users and devices
- Create Internal Provisioners
- Assign one or more Onboarding Templates to Internal Provisioners or External Provisioners (Provisioners on AD/LDAP)

- Enable and customize GIM REST APIs for integration with 3rd party applications
- Enable and customize GIM Outlook Plug-in

Furthermore, GIM allows the Provisioners to use the Onboarding Template(s) and provision users and/or devices based on their customized constrains.

Provisioners may be:

- External Provisioners — For example, Employees or Students that reside on an AD or LDAP server.
- Internal Provisioners — Provisioners created by the administrator and are, for example, Business Partners, Vendors, Suppliers, Contractors, Front Desk Security Guards etc.

The GIM administrator and the Provisioner use different login pages. When a Provisioner logs in, the Provisioner is authenticated by the ExtremeControl engine against AD/LDAP in the case of External Provisioner or against the Local Repository in the case of Internal Provisioner. Once the Provisioner logs in, then the Provisioner has access to the Onboarding Templates to which the administrator provides access and is able to provision users and/or devices.

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

- [ExtremeCloud Appliance Now Available as Flow Source](#)
- [Flows Sent to Cloud Providers Now Displayed on Application Flows Tab](#)
- [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 Initiate and View Packet Captures](#)

Extreme Cloud Appliance Now Available as Flow Source


The ExtremeCloud Appliance can now be added as a flow source to an Analytics engine.

Flows Sent to Cloud Providers Now Displayed on Application Flows Tab

ExtremeAnalytics now indicates flows that are sent to a cloud provider (for example, Amazon Web Services, Google Compute, and Microsoft Azure) via the **Server Site** column on the **Application Flows** tab.

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 (for example, "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

It is also possible to port-mirror SPB (Mac-in-Mac encapsulated) traffic to a PV-FC-180 for flow analysis. Firmware upgrade on PV-FC-180 may be required.

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 Initiate and View Packet Captures

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 vSphere 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.

- [Information Governance Engine Integration with Workflows](#)
- [Ability to Test ICX, MLX, SLX, and VDX Devices](#)
- [Ability to Schedule Email of Governance Results](#)
- [Usability Improvements](#)

Information Governance Engine Integration with Workflows

You can now integrate the Information Governance Engine with workflows functionality to automatically remediate devices that fail an audit test. By creating an alarm that is generated when a device fails an audit test, you can configure Extreme Management Center to automatically run a workflow when the alarm occurs. When configured, any time the Information Governance Engine performs an audit test for which a device fails, an alarm occurs that initiates a workflow designed to remediate the reason for the failure. To enable this functionality, configure the Information Governance Engine to send syslog messages by opening the `Installation Directory/GovernanceEngine/logger.conf` file and ensure `enableSyslog=true`.

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 8.2.3.67

Extreme Management Center Issues Addressed	ID
--	----

Firefox Browser users were incorrectly receiving the message: "Connection to server lost. Please try again later." when attempting to launch Java Client Applications.	01761267
The Extreme Management Center Server was not attempting to restart after it became unresponsive.	-----
Changing the number in the Retain Rows Count field in the Event Tables Row Limit section of the Alarm/Event Logs and Tables options was not changing the number of entries in the table.	01406736 1423143 01724568
Creating archives via ZTP+ was not completing successfully.	-----
Creating archives for VOSS devices were not completing successfully.	-----
Users were occasionally unable to log in to the legacy java applications.	1743521
The Interface Summary table on the Network tab was not displaying data.	1413817
The Protocol Address column in the VLAN Summary Device View was not updating for ZTP+-enabled devices.	-----
Backup configurations for ERS and VSP devices were taking over 10 minutes to complete.	-----
The Backup and Restore Configuration commands were not able to be modified via a script on devices on which the VOSS operating system is installed.	-----
Wireless clients were not being sorted correctly in the Wireless > Clients > Clients window.	1749184
The MAC OUI Vendor column on the Wireless Clients and Client Events tabs were incorrectly not displaying data.	01761266
Link Down alarms were missing a comma between the trap message and the port number in the Information field of the alarm.	1761694
ZTP+ was not upgrading ExtremeXOS devices if the firmware was marked for upgrade and there was no <code>cloud_connector.xmod</code> file. In the Alarms & Events > Discovered window, the following error was reported: Connector must be upgraded.	-----
Attempting to replace a device via ZTP+ functionality by selecting the Remove from Service checkbox and entering a value in the Replacement Serial Number field in the Configure Device window was not completing successfully if the device was upgraded while removing the device from service.	-----

The Extreme Management Center server was not restarting using the <code>service nserver restart</code> or <code>systemctl restart nserver</code> commands.	-----
Map links were not opening if the linked map was not visible (expanded) in the Sites tree.	01728714
Map links on the following device types sporadically disappeared until the device was rediscovered: <ul style="list-style-type: none"> • ERS-Series • VSP-7000 	-----
Opening the Vendor Profile tab in the Configure Device window was incorrectly forcing you to click the Enforce Preview button prior to modifying fields in the tab.	-----
Events on the Events tab were loading slowly.	-----
SNMP queries to devices with non-compliant SNMP agents occasionally stopped responding.	01760798
ExtremeAnalytics Issues Addressed	ID
Apache Tomcat formerly allowed TLSv1.0 connections, which was a less secure protocol to communicate with the Application Analytics engine.	-----
Enabling or disabling the disk flow export feature may cause enforce operations to time out. A subsequent enforce typically resolves this issue.	-----
Extreme Management Center was not generating an alarm when the Historical Application Flow table was empty because the disk space on a sensor was more than 80% full.	-----
ExtremeControl Issues Addressed	ID
To improve security when connecting to the Access Control engine, you can no longer use SSLv2Hello, TLSv1.0, and TLSv1.1 to access the engine. You can now only connect to the Access Control engine via TLSv1.2. The agent may still connect using TLSv1.0.	-----
Using quotation marks around an IP address to search for the exact match of an end-system located on the Access Control > End-Systems tab incorrectly returned non-matching results.	1321075
RADIUS Accounting STOP packets were not proxied for all session states.	01756188

Not all RADIUS attributes in the Access Control dictionaries correctly handle the <code>has_tag</code> attribute FLAG.	-----
Opening the Add/Edit RADIUS Server window on the Policy > Devices/Port Groups > Devices > RADIUS > Authentication Servers tab incorrectly displayed an error when the Server Shared Secret and Verify Shared Secret fields were blank.	1768295 1773636
Reauthenticating an end-system on a B5 or C5 device with an Authentication Type of MAC and 802.1X was causing the authentication to stop responding.	1743570
Attempting to edit or delete a rule included in an ExtremeControl configuration in Extreme Management Center was not completing successfully.	01776876

3.2 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 an operating system when using a network proxy behind a firewall did not complete successfully.	-----
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.	-----
Samba winbind processes were spawning unlimited child processes during periods of intermittent network connectivity with Active Directory controller.	1730745

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

3.3 Vulnerabilities Addressed

This section presents the Vulnerabilities addressed in Extreme Management Center 8.2:

- The following vulnerabilities were addressed in the Extreme Management Center, Extreme Access Control, and Extreme Application Analytics engine images:
 - CVE-2014-9620, CVE-2014-9621, CVE-2014-9653, CVE-2015-8865, CVE-2018-10360, CVE-2017-11108, CVE-2017-11541, CVE-2017-11542, CVE-2017-11543, CVE-2017-12893, CVE-2017-12894, CVE-2017-12895, CVE-2017-12896, CVE-2017-12897, CVE-2017-12898, CVE-2017-12899, CVE-2017-12900, CVE-2017-12901, CVE-2017-12902, CVE-2017-12985, CVE-2017-12986, CVE-2017-12987, CVE-2017-12988, CVE-2017-12989, CVE-2017-12990, CVE-2017-12991, CVE-2017-12992, CVE-2017-12993, CVE-2017-12994, CVE-2017-12995, CVE-2017-12996, CVE-2017-12997, CVE-2017-12998, CVE-2017-12999, CVE-2017-13000, CVE-2017-13001, CVE-2017-13002, CVE-2017-13003, CVE-2016-10254, CVE-2016-10255, CVE-2017-7607, CVE-2017-7608, CVE-2017-7609, CVE-2017-7610, CVE-2017-7611, CVE-2017-7612, CVE-2017-7613, CVE-2014-9092, CVE-2016-3616, CVE-2017-15232, CVE-2018-11212, CVE-2018-11213, CVE-2018-11214, CVE-2018-1152, CVE-2016-10087, CVE-2018-13785, CVE-2018-7182, CVE-2018-7183, CVE-2018-7184, CVE-2018-7185, CVE-2017-17833, CVE-2018-12938, CVE-2018-1000005, CVE-2018-1000007, CVE-2018-1122, CVE-2018-1123, CVE-2018-1124, CVE-2018-1125, CVE-2018-1126, CVE-2016-4429, CVE-2018-14622, CVE-2017-8779, CVE-2015-9262, CVE-2018-14598, CVE-2018-14599, CVE-2018-14600, CVE-2017-2619
- The following vulnerabilities were addressed in the Extreme Application Analytics engine images:

- CVE-2015-3218, CVE-2015-3255, CVE-2015-4625, CVE-2018-1116, CVE-2017-15422, dnsmasq, dns-root-data

4. Upgrade, Installation, and Configuration Changes

4.1 Important Upgrade Considerations

4.1.1 License Renewal

Upgrading to Extreme Management Center version 8.2 requires you to [renew your NMS license](#) if generated prior to November 30, 2018. Licenses generated prior to November 30, 2018 expire 90 days after upgrading to Extreme Management Center version 8.2.

4.1.2 Internet Connection

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 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 and stacked ExtremeSwitching X440-G2 devices cannot be selected as an Application Telemetry source.

4.3 Fabric Manager Upgrade Information

Fabric Manager may be unavailable via Extreme Management Center after upgrading if the certificate is missing in Extreme Management Center Trust store.

To ensure Fabric Manager is available, enter the Fabric Manager certificate in the Extreme Management Center Trust store using **Generate Certificate** option. This manually updates the Extreme Management Center trust store with Fabric Manager Certificate entry.

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**.
-

4.6 VSP Device Configuration Information

Topology links from VSP devices to other VSP or ERS devices may not display in a topology map (or may display inconsistently). To ensure topology map links display correctly, verify the VSP device is configured to publish its management IP address in the autotopology (SONMP) data.

Ensure the output of `show sys setting` command shows:

```
autotopology : on
ForceTopologyIpFlag : true
clipId-topology-ip : 0
```

If the output values displayed are different, configure the VSP device to publish management IP address in SONMP data by executing the following CLI commands:

```
(config)# autotopology
(config)# sys force-topology-ip-flag enable
(config)# default sys clipId-topology-ip
```

5. 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.

Internet Explorer is not supported in Extreme Management Center version 8.2.3.

5.1 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

5.2 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	8 GB	12 GB	24 GB	24 GB
-Xmx	12 GB	18 GB	36 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:

	Small	Medium	Enterprise	Large Enterprise
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) 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.

5.3 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 ExtremeApplication Analytics virtual engine requires AMD processors with at least Bulldozer based Opterons.

5.3.1 Extreme Management Center Virtual Engine Requirements

	Small	Medium	Large
Total CPU Cores	8	16	16
Memory	16 GB	32 GB	64 GB
<u>Memory allocated to Java:</u>			
-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
MU Events	No	Yes	Yes

5.3.2 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

¹The 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.

5.3.3 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 ExtremeApplication Analytics virtual engine installation require 16 CPU cores. This is only available by purchasing a permanent license. To use the ExtremeApplication 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.

5.3.4 Fabric Manager Requirements

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

5.4 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	80 MB	40 MB (80 MB with Service Agent)
	Windows XP		
	Windows 2008		
	Windows 2003		
	Windows 7		
	Windows 8		
	Windows 8.1		
	Windows 10		
Mac OS X	Tiger	10 MB	120 MB
	Snow Leopard		
	Lion		
	Mountain Lion		
	Mavericks		
	Yosemite		
	El Capitan		
	Sierra		

***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.

5.5 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 ControlEngine 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:



5.6 Extreme Access Control (ExtremeControl) Engine Version Requirements

For complete information on Access Control engine version requirements, see the [Extreme Management Center Version 8.2 Release Notes](#) section of these Release Notes.

5.7 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.

5.8 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.

5.9 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	

5.10 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.

5.11 Ekahau Maps Requirements

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

5.12 Guest and IoT Manager Requirements

5.12.1 Guest & IoT Manager Server OS Requirements

These are the operating system requirements for Guest & IoT Manager server:

	Operating System
VMware® (Extreme Management Center Virtual Engine)	VMware ESXi™ 5.5 server VMware ESXi™ 6.0 server VMware ESXi™ 6.5 server vSphere (client only)™

5.12.2 Guest & IoT Manager Outlook Add-in Client Requirements

These are the requirements for the Client Machines which need to run Guest & IoT Manager Outlook Add-in.

Operating System	
Windows*	Windows 7 Windows 10
Mac OS X	Sierra High Sierra Mojave

***NOTE:** Microsoft® Outlook® 2016 is needed on Windows/Mac clients for the add-in to operate.

5.12.3 Guest and IoT Manager Virtual Engine Requirements

The VMWare Guest & IoT Manager virtual engines are packaged in the .OVA file format (defined by VMware) and needs an x86, 64-bit capable environment

	Minimum	Recommended
Total CPU Cores	2	4
Memory	2 GB	4 GB
Disk Size	80 GB	80 GB
Interfaces	1 Physical NIC	3 Physical NICs

5.12.4 Guest and IoT Manager Supported Browsers

The following table outlines the supported desktop and mobile browsers that can be used to launch Guest & IoT Manager Admin and Provisioner Web Application:

	Browser	Version
Desktop	Microsoft Internet Explorer	11 and later
	Mozilla Firefox	63 and later
	Google Chrome	65 and later
Mobile*	iOS Native	9 and later
	Android Chrome	65 and later
	US Browser	11.5 and later
	Opera	40 and later
	Firefox	63 and later

*Mobile Browsers are supported only for the Guest Self-Service Provisioning flow.

Notes:

- A mobile device can access the Guest & IoT Manager Application by using any desktop-supported browsers available on a mobile device. Make sure to select the **Desktop site** option in the browser options before login.
- Browsers set to a zoom ratio of less than 100% may not display Guest & IoT Manager Application properly (for example, missing borders around windows). Setting your browser to a zoom ratio of 100% corrects this issue.
- Guest & IoT Manger Application is best viewed in 1920 x 1080 resolution or higher. Lower resolutions may result in improper layouts in some cases.

6. Getting Help

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

Extreme Portal

Search the GTAC (Global Technical Assistance Center) knowledge base, manage support cases and service contracts, download software, and obtain product licensing, training, and certifications.

The Hub

A forum for Extreme customers to connect with one another, answer questions, and share ideas and feedback. This community is monitored by Extreme Networks employees, but is not intended to replace specific guidance from GTAC.

Call GTAC

For immediate support: 1-800-998-2408 (toll-free in U.S. and Canada) or 1-603-952-5000.

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