Extreme Management Center® Release Notes
Version 8.2.6

5/2019
9035977-10 Rev. AB
Subject to Change Without Notice

Table of Contents

Extreme Management Center Version 8.2 Release Notes

Extreme Management Center
8.2.6.5
May, 2019

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 quickly. 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. 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 fixed issues 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:

- Engines
- 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

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.

1.2 Extreme Management Center

- New ExtremeXOS Device Type Supported
- 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

New ExtremeXOS Device Type Supported

Extreme Management Center now supports the ExtremeXOS X465 device type.

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 if an action is successful, and another set of actions if the action is not successful. 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 when necessary.

The following system-defined workflows are available in this release (a change in version number between releases indicates a change to the workflow):

- ICX-SLX Config Basic Support (version 116)
- MLX Config Basic Support (version 122)
- VDX Config Basic Support (version 91)
- MLAG with VOSS Cluster (version 131)
- VOSS Fabric NNI LAG (version 77)
- VOSS Virtual IST (version 137)
- Add Login Banner (version 76)
- Enable HTTPS (version 53)

- Enable SSH (version 52)
- ICX-MLX Backup Configuration (version 101)
- VDX Backup Configuration (version 33)
- ICX-SLX-MLX Restart Device (version 15)
- VDX Restart Device (version 21)
- ICX-MLX Restore Configuration (version 72)
- VDX Restore Configuration (version 64)
- ICX Upgrade Firmware (version 37)
- MLX Upgrade Firmware (version 47)
- VDX Upgrade Firmware (version 59)
- Collect Traffic Forensics (version 164)
- Create Trouble Ticket (version 191)
- Quarantine End System (version 154)
- Quarantine PCAP Flow (version 363)
- Revert Quarantine End System (version 175)

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 using the CLI. This prevents 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 (GIM) licenses. NMS-ADV-xx continues to support 500 end-systems and now includes 50 GIM 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 the site to which you add it.

Extreme Management Center can also back up, 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, you can also update and view the certificate in Extreme Management Center.

Ability to Provision Fabric Topologies in Extreme Management Center

With an NMS-ADV license, you can 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 Fabric Topology and Service Definition template to a site. The Service Definition template allows you to create VRF, VLAN, Layer 2, and Layer 3 service mappings. Extreme Management Center supports provisioning fabric topologies on the following device types:

- 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: VSP7024 and VSP86xx devices are not supported.

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 (AWS) 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 types 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.

1.3 ExtremeControl

- Additional Guest & IoT Manager Language Locales
- Introducing Guest & 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

Additional Guest & IoT Manager Language Locales

Beginning in version ExtremeControl version 8.2.5, Guest & IoT Manager supports 5 language locales for self-service and provisioners.

Introducing Guest & IoT Manager

Beginning in ExtremeControl version 8.2, a new set of user and device provisioning, called Guest & IoT Manager, is now available. 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 the 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 Add-in.

Furthermore, provisioners can use the GIM Onboarding Template(s) to provision users and/or devices based on their customized constraints.

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, ExtremeControl authenticates the user 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, he has access (provided by the administrator) to the Onboarding Templates 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, which is a wireless controller with integrated ExtremeControl functionality. When accessing your wireless network via the ExtremeCloud Appliance, the ExtremeCloud Appliance automatically assigns a policy role to users 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

1.4 ExtremeAnalytics

- Client Count Licenses Now Available
- Ability to Save ExtremeAnalytics Reports to Report Designer
- 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
- Flow Details Cached on ExtremeAnalytics Engine File System
- Ability to Initiate and View Packet Captures

Client Count Licenses Now Available

New ExtremeAnalytics licenses are based on the number of in-network end-systems rather than flow rate. With this version, ExtremeAnalytics enforces either legacy flow rate licenses or new end-system count licenses.

Ability to Save ExtremeAnalytics Reports to Report Designer

In Extreme Management Center version 8.2.5, you can now save ExtremeAnalytics reports that include user-defined values to the Report Designer so they can be used as report components in other areas of Extreme Management Center (for example, scheduled tasks).

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 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 ( ). Right-click the location, select **Assign to Site**, and select a site from the drop-down list.

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 troubleshooting 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. To use this functionality, EOS firmware version 8.63.04.0002 or later must be installed on a PV-FC-180.

Flow Details Cached on ExtremeAnalytics Engine File System

When running on a system with an SSD file system, the ExtremeAnalytics Engine can store flow details on disk for up to five days. This allows for detailed analysis of network usage by a client or server before, during, or after an incident.

IMPORTANT: Enabling this option on an engine with a spinning disk or on a virtual engine may cause severe performance problems resulting in lost data.

Ability to Initiate and View Packet Captures

You can initiate a packet capture (pcap) 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.

1.5 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 enhanced functionality:

- 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) enhanced functionality:

- 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 enhanced functionality:

- 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.

1.6 Information Governance Engine

Your version of the Information Governance Engine (IGE) is automatically upgraded when you install 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 IGE 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 IGE 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 IGE 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 and Vulnerabilities Addressed

3.1 Known Issues Addressed in 8.2.6.5

Extreme Management Center Issues Addressed	ID
Device Grid reference images and Impact Analysis for devices with reference images were sometimes not working for ERS switches.	------
The **Firmware Minimum Version** on the Administration > Vendor Profiles tab for the X465-24MU-24W device was incorrectly labeled **Firmware Maximum Version**, which prevented the newest firmware version from being downloaded.	------
Changing the selection of the left-panel drop-down list on the Network > Devices tab with a large number of devices caused a Could Not Load Report error.	------
Opening the Interface History report from the Port Tree on the Network > Devices tab caused an Invalid Target error.	------
Adding a device to a site with **Enable Collection** selected on the Site > Actions tab was not collecting port information on the device after it was discovered.	------
Links displayed on Maps were occasionally attached to the wrong port on a device.	01837871
The **Valid Values** field for an input with a **Display Type** of **ComboBox** in the Manage Inputs window (Tasks > Workflows > Inputs > Manage Inputs) was incorrectly not allowing special characters.	
Clicking **Register Trap Receiver** for a VSP device was not registering the VSP device as a trap receiver.	01842123
Extreme Management Center was continuously displaying a trap overflow error.	01790950

Restarting the Extreme Management Center server may not complete successfully. Additionally, attempting to access a site or perform actions to a site may not complete successfully.	
Upgrading the Extreme Management Center server, the Application Analytics engine, or the Access Control engine was occasionally adding or removing packages while updating the operating system.	------

ExtremeControl Issues Addressed	**ID**
Selecting **Auto-Detect** or selecting a domain in the Join AD Domain field on the Advanced AAA Configuration tab was not authenticating users from other trusted domains.	01841156
The **Name** field for a policy Role (Control > Policy > Roles/Services > Roles > Create Role) was incorrectly not allowing special characters.	01848955

3.2 Known Issues Addressed in 8.2.5.50

Extreme Management Center Issues Addressed	**ID**
After restarting the Extreme Management Center server, scheduled archives and firmware upgrades no longer started automatically.	01834762
After restarting an SLX device configured to receive traps in Extreme Management Center, the device was no longer receiving trap information.	------
Clicking **Unregister Trap Receiver** for an SLX device was not unregistering the SLX device as a trap receiver.	------
Extreme Management Center was incorrectly displaying "Trap Receiver Unregistered" for an SLX device following a device refresh.	------
Extreme Management Center was failing to update SNMP trap receiver configuration when changing between SNMPv1 and SNMPv2 profiles with the same community string.	------
Users were unable to access various areas on Extreme Management Center's **Network** tab if they did not have **Application Analytics > Read Access** capability.	1832985
After changing values in the Details right-panel of the **Archives** tab, the **Save** button remained disabled so the changes could not be saved.	1794934 01825611
The memory settings on the Extreme Management Center server was not automatically adjusted on systems with more than the recommended minimum amount of memory.	01411175 01830936

Extreme Management Center was not starting while McAfee antivirus software was running.	1708958
When attempting to set the Topology Definition to **None** to remove Fabric Connect configuration from a VSP device that has Fabric Attach enabled and learned L2VSN and Switched UNI services, the Topology Definition did not change to **None** due to an attempt to delete learned (non-deletable) services.	------
On the **VLAN Definitions** tab of the Enforce Preview window in Fabric Connect, the VLAN row displayed a mismatch after successfully enforcing a new VLAN with only the SNOOPING Multicast option selected.	------
The **Network > Devices > Sites** left-panel tree was not reordering the sites alphabetically when a site was renamed and the tree was refreshed.	1795286
Selecting the **Hide Location Probability** checkbox on the Administration > Diagnostics > System > Map Server Details tab was deleting configurations saved in the `NSJBOSS.properties` file.	01814374
Site endpoint definitions caused server log exceptions when using ExtremeConnect.	------
The **Remove Service** button in ExtremeConnect was allowing users to remove all services, including the default service configuration. Now, ExtremeConnect prevents the last entry from being removed in the configuration file.	1801959
The **BOSS Chassis Components** FlexView did not include the device serial number.	------
Managing IPv4 or IPv6 CLIP addresses caused unrelated Loopback Interface addresses to be modified or removed.	------
Managing IS-IS Source Addresses or the IPv4 or IPv6 CLIP addresses caused unrelated Loopback Interface addresses to be modified or removed.	------
Extreme Management Center was not prioritizing user-initiated requests to refresh device data when the user was waiting for the request to complete.	------
Multiple vulnerabilities were detected in the Oracle Java SE version. An upgrade to Oracle JDK/JRE 11 resolved the issues.	------

In some instances, after successfully enforcing Fabric Connect VLAN changes, the Summary status indicated VLAN Definition mismatches, even though the individual row statuses displayed as matching.	------
ERS-8600 Restart Request Statuses displayed as **FAILURE**, even though the operations were successful.	------
After a device was replaced by another device, Extreme Management Center displayed the previous device's serial number for the newly installed device in the Inventory Report on the **Reports > Reports > PDF Reports** tab.	1796037
Changes made in the **Configure Device** window for IPv6 CLIP Addresses caused Extreme Management Center to incorrectly identify mismatches, even after the changes were successfully enforced.	1783878
Clicking **Import to Site** on the **Network > Devices** tab was not importing VLANs currently on the device to the site.	1800707
The Interface History on the **DeviceView > Port** menu did not function for ports with empty Port Names.	1783878
The Devices with Reference Firmware chart on the **Network > Impact Analysis** Dashboard was not reflecting all the devices with reference firmware.	1782868
Extreme Management Center was unable to update captive portals with FQDN certificates if the portals were not configured for FQDN.	1820161
ERS 5500 Series devices were failing to register for Syslog messages.	------
Sites were being overwritten for ZTP+-enabled devices during the pre-register process.	------
On a VSP device with Fabric Connect configured and that had discovered L2 VSN and Switched UNI services, and attempts were made to merge those discovered services during enforce, the merge did not work and deletion of the discovered services was attempted.	------
Extreme Management Center was running slowly at regular intervals (typically every 12 hours), during which time the user interface was running slowly and occasionally memory problems were reported in the event log.	------
The Extreme Management Center Add and Edit Alarm Configuration functions were not functioning for NMS-U or NMS-BASE-xx licenses.	1818320 1817352 1819789

After applying Extreme Management Center 8.2.4, Extreme Management Center, ExtremeAnalytics, and ExtremeControl engines were losing IP connectivity. An upgrade to 8.2.5 resolved the issue.	1814819
Some ports on switches in a stacked configuration on which the ExtremeXOS operating system is installed were not displaying correctly when one device was powered down.	1269075
Creating a scheduled task to upgrade firmware on a device with **Restart Devices After Upgrade** selected was upgrading the firmware, but not restarting the device.	1336886
Firmware upgrades using FTP on ZTP+-enabled devices were not completing successfully.	------
Accessing the device list in the left-panel of the **Network** > **Devices** tab loaded slowly and automatic view updates could change the scroll position of the list.	------
Configuring a Custom Criteria Alarm such that the **Match On** for the alarm is **Host Name** was generating a NullPointerException event in the `server.log`.	01784227

ExtremeAnalytics Issues Addressed	**ID**
Generating an application report via the **Analytics > Browser** tab with a Display Format of **Chart over Time** was not displaying properly.	------
On the **Analytics > Browser** tab, **Chart Over Time** values were not displaying for target types with multiple components (for example, Application/Client or Application/Server).	------
In ExtremeAnalytics, the toggle function between the **Engines** and the **Fingerprints**, **Status**, and **Licenses** features on the Configuration tab was delayed and not functioning properly.	------
The Server Totals report on the **Analytics > Insights** Dashboard was displaying as a blank page.	------
On the **Analytics** tab, in browsers where the GMT offset was on a non-hour offset (for example, India Standard Time), no data displayed in the Top N Applications, Top N Clients, and Top N Server Reports.	------
The **Analytics > Packet Captures** tab was unavailable when one or more Analytics engines were down.	------
The Response Time Dashboard was incorrectly including unknown interfaces, which displayed as negative values.	01744900

ExtremeControl Issues Addressed	ID
IP Address policy rules were incorrectly written with a user-defined port value of 1 when enforced from Extreme Management Center.	1803365
When Extreme Management Center LDAP authentication was used for Guest and IoT Management (GIM) access, Extreme Management Center disconnected and the Could Not Acquire Lock error message was triggered when the GIM application was used.	1818862
End-System Identification in the Access Control Captive Portal was not functioning. The support for IP NAT and Firewall Friendly Captive Portal has been improved to resolve the issue.	1792959
Improper handling of links caused several URLs on the Access Control > Configuration tab to link to the Engines panel, rather than the panels to which they were linking.	1812644
During end-system IP Resolution, if the IP address was previously known, the existing IP address was displaying intermittently in the End-System table. Now, the IP address displays continuously in the table.	------
In ExtremeControl, the Read and Read/Write capabilities were not dependent on each other for the Guest and IoT Management (GIM), End-System REST API, NAC System Web Services APIs, and NAC Web Services API categories. Now, when the Read/Write capability is selected, the Read capability is automatically selected, and when the Read capability is deselected, the Read/Write capability is automatically deselected.	------
The driver for the BCM57xx interface was missing for the ExtremeControl NAC-A-20 engine.	1816400 1819129
The MAC OUI Vendor and Switch Nickname columns on the End-Systems tab could not be filtered or sorted.	------
SNMP contact issues to switches was causing the IP resolution task queue to fill, which resulted in the Access Control engine failing to process RADIUS authentication requests.	01777651 01797992 1783438 01818289 01819014 01804123 01833925
Weak default ciphers reduced security on ExtremeControl ports for agent-based assessments.	------

Groups included in the Group Editor on the Access Control tab could not be copied.	01781787
ExtremeControl Rules were occasionally incorrectly deleted from Extreme Management Center.	01778553

3.3 Known Issues Addressed in 8.2.4.55

Extreme Management Center Issues Addressed	**ID**
Attempting to enforce a change to Fabric Connect services from the enforce preview panel was not completing successfully if the device was configured with a Fabric Attach Management service which had been previously configured.	------
When running Extreme Management Center with multiple vCenter servers configured, Extreme Management Center was running slowly and eventually became unresponsive. Additionally, the server log indicated database connection errors.	------
Status Collection was using an unnecessary amount of CPU.	------
Installing the Extreme Management Center version 8.2.4 .OVA file without a license was generating the following exception in server.log during startup: Error while calling onServerReady.	------
Upgrading Extreme Management Center to version 8.2 was occasionally causing a loss of connectivity due to network interfaces being renamed.	01814819
Extreme Management Center was occasionally generating a low memory alarm when the percent of memory utilization was not above the memory alarm threshold.	------
After downloading firmware on an SLX9140, Extreme Management Center incorrectly displayed the status as Failed even if the download completed successfully.	------
Backing up or restoring a device configuration for an SLX device was not completing successfully.	------
Remaining idle for a short amount of time (a few minutes) was causing Extreme Management Center to disconnect if the server used an NMS-BASE license.	1815180 01821347 01823542
The driver for the BCM57xx interface was missing for the ExtremeControl NAC-A-20 engine.	01816400 01819129

Extreme Management Center was taking an excessive amount of time (over 30 minutes) to display SLX firmware versions after they were downloaded.	------
LAG links connected to SLX and older legacy Extreme devices were incorrectly labeled in topology maps.	------
The **Source** column on the Network > Devices > Site > Services tab was occasionally not accurate for VSP-series devices for which I-SIDs were manually configured.	------
PDF reports sent as the result of a running a scheduled task was failing because of an "Unauthorized" error.	------
Discovering a ZTP+-enabled device that was previously deleted from Extreme Management Center, but still exists in the database was creating a second entry for the same device in the database.	------
Firmware for SLX9140 devices was displaying a device type of **Unknown** on the **Firmware** tab, which caused the firmware upgrade to fail.	------
SLX firmware version 18.x was not associated with the SLX9030 device type in the firmware tree on the **Firmware** tab.	------
The **Ports** tab in the **Configure Device** window was incorrectly updating values when clicking **Reload**.	1772853
PortView > Interface Details was displaying the incorrect port speed.	01786614
Enforcing VLAN changes to a device with more than 1024 ports was incorrectly updating additional fields.	1792898
Removing ports from a VLAN on an ExtremeXOS device via a topology map was not functioning properly.	1224880
Executing a task for a script that no longer exists generated an Error Loading Report error.	1546390
ExtremeXOS scripts were experiencing connection failures without retrying with alternate VRs.	------
Configuration files for VSP 8400 series devices were occasionally failing to archive.	01794911
After running a TCL/Python script to restart an ExtremeXOS device, the confirmation returned in the CLI was missing a carriage return.	01762635

ExtremeAnalytics Issues Addressed	ID

ExtremeAnalytics engine status graphs were displaying very low **Percent Bandwidth Identified** values for ExtremeXOS devices.	------
The data in the Application/Client chart on the **End-System Applications Summary** tab was displaying inaccurate data.	01741582
Users were incorrectly unable to access the **Network** tab without the NetSight Application Analytics > Application Analytics Read Access capability.	------
Adding an ExtremeXOS device to ExtremeAnalytics as an Application Telemetry Source was not supported when the host IP was applied to an engine other than the VR-Default.	01746278 1757187
Adding a device as an Application Telemetry source on the ExtremeAnalytics **Advanced Configuration** tab was taking a considerable amount of time (occasionally over 20 minutes).	------
ExtremeControl Issues Addressed	**ID**
Accessing the Register New Guest User window in Guest & IoT Manager after creating a new SMS gateway and setting the new gateway as the default was causing the **Submit** button to be unavailable and caused a null error in the browser log.	01816503
Users were unable to scroll down to view the full Terms of Use on self-service pages provisioned by the Onboarding Template in Guest & IoT Manager.	01818349
Importing policy roles from another domain were incorrectly associating global services to the roles if the source domain contained local services of the same name.	1788278
The **Add VLAN** window in ExtremeControl's Policy Mapping Editor was losing focus or disappearing if the background or parent window was clicked.	01790982
Enforcing a policy role to an ExtremeCloud Appliance was failing if any rules contained a colon, semicolon, single quote, double quote, or ampersand.	01798248
LDAP user groups now use the LDAP configuration specified in the authenticating AAA authentication rule.	01790436
ExtremeControl was not correctly processing some SNMP errors, which was delaying all other SNMP tasks.	01745716
Clicking **Search for older events** was not functioning in the ExtremeControl End-Systems Events table.	1758370

3.4 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 `cloud_connector.xmod` 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 `service nsserver restart` or `systemctl restart nsserver` 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: • 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 `has_tag` 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

3.5 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

3.6 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

3.7 Vulnerabilities Addressed

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

- The following vulnerabilities were addressed in the Extreme Management Center, 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, CVE-2018-1000807, CVE-2018-1000808, CVE-2018-0495, CVE-2018-6594, USN-3715-1, CVE-2018-0494, CVE-2017-15422, CVE-2015-3218, CVE-2015-3255, CVE-2015-4625, CVE-2018-1116, CVE-2016-10713, CVE-2018-1000156, CVE-2018-6951, CVE-2018-1122, CVE-2018-1123, CVE-2018-1124, CVE-2018-1125, CVE-2018-1126, CVE-2018-18311, CVE-2018-18312, CVE-2018-18313, CVE-2018-18314, CVE-2016-2774, CVE-2017-3144, CVE-2018-5732, CVE-2018-5733, CVE-2016-10209, CVE-2016-10349, CVE-2016-10350, CVE-2017-14166, CVE-2017-14501, CVE-2017-14503, CVE-2017-7526, CVE-2018-6552, USN-3784-1, USN-3623-1, CVE-2018-16839, CVE-2018-16840, CVE-2018-16842, CVE-2018-11574, CVE-2017-13168, CVE-2018-15471, CVE-2018-16658, CVE-2018-9363, CVE-2018-18584 CVE-2018-18585, CVE-2018-3136, CVE-2018-3139, CVE-2018-3149, CVE-2018-3150, CVE-2018-3157, CVE-2018-3169, CVE-2018-3180, CVE-2018-3183, CVE-2018-3209, CVE-2018-3211, CVE-2018-3214, CVE-2018-13785, CVE-2018-14598, CVE-2018-14599, CVE-2018-14600, CVE-2015-9262, CVE-2018-18955, CVE-2018-6559, CVE-2018-18065, CVE-2018-15686, CVE-2018-15687, CVE-2018-6954, CVE-2018-18065, CVE-2018-0734, CVE-2018-0735, CVE-2018-5407, CVE-2018-17456, CVE-2016-10708, CVE-2018-15473, USN-3716-1

- 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 Information

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.

4.1.3 Upgrading Hardware

When attempting to upgrade the Extreme Management Center server, the Application Analytics engine, or the Access Control engine to version 8.2.5, the upgrade may occasionally not complete successfully. If the upgrade is not successful, begin the upgrade again.

Additionally, when restarting Extreme Management Center server (NMS-A-25 or NMS-A-305), the Application Analytics engine (PV-A-305), or the Access Control engine (IA-A-25 or IA-A-305) the following error message may display for each CPU in the engine console and in the engine log:

```
[Firmware Bug]: BIOS needs update for CPU frequency support
[Firmware Bug]: ACPI: Invalid BIOS _PSS frequency found for
processor 0: 0x0 MHz
[Firmware Bug]: ACPI: No valid BIOS _PSS frequency found for
processor 0
```

To correct the issue, access the engine console and perform the following:

1. Open the BIOS.
2. Access the **Setup Menu**.
3. Select **Advanced**.
4. Select **Power & Performance**.
5. Change the **Enable CPU HWPM** value from the default, **Disabled** to **HWPM NATIVE MODE**.
6. Press **F10** to save changes.
7. Enter **Y** to save and exit.

4.1.4 Free Space Consideration

When upgrading to Extreme Management Center version 8.2, a minimum of 15 GB of free disk space is required on the Extreme Management Center server.

To increase the amount of free disk space on the Extreme Management Center server, perform the following:

- Decrease the number of Extreme Management Center backups (by default, saved in the `<installation directory>/usr/local/Enterasys_Networks/NetSight/backup` directory).
- Decrease the Data Persistence settings (Administration > Options > Access Control > Data Persistance).
- Remove unnecessary archives (Network > Archives).
- Delete the files in the `<installation directory>/NetSight/.installer` directory.

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.

Deleting an ExtremeXOS device that is configured as a flow source via the Flow Sources table of the **Analytics** > **Configuration** > **Engines** > **Configuration** tab from the Devices list on the **Network** > **Devices** tab generates an error message in the `server.log`, but does not warn you that the device is in use as a flow source. Adding the device back in the Devices list on the **Network** > **Devices** tab or removing the device from the Flow Source table fixes the issue.

4.3 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.

Additionally, the following message may appear during the ExtremeControl upgrade to version 8.2:

No domain specified

To stop domain-specific `winbindd` process, run `/etc/init.d/winbindd stop` *`{example-domain.com}`*

4.4 Fabric Manager Upgrade Information

4.4.1 Certificate

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.

4.4.2 Authentication Key

When you provision authentication keys for Fabric Attach, the key cannot be read back for security reasons. When the key is read from the device it always shows "****". For this reason, it may appear that there is a configuration mismatch when one does not exist.

4.4.3 Service Configuration Change

If you change a configured service via the **Configure Device** window that references one of the following and then enforce those changes to the device, the configuration on the device may change unexpectedly:

- MLT
- SMLT
- port specific settings to a port belonging to an MLT or SMLT

To prevent this merge, changes from **Current** to **Desired** on rows where MLT or SMLT are in use in the **Enforce Preview** window.

To correct the issue after enforcement, modify the service on the device via the CLI.

4.4.4 CLIP Addresses

Via the CLIP Addresses table in the Configure Device window, you can enter addresses in both IPv4 and IPv6 format. However, Extreme Management Center version 8.2.5 only supports applying a single address (either IPv4 or IPv6) to a Loopback Interface. Only enter a single CLIP address to a Loopback Interface.

4.4.5 Gateway Address Configuration Change

In versions of Extreme Management Center prior to 8.2.5, the Default Gateway IP Address is configured as part of the VLAN. In 8.2.5, the Default Gateway IP Address is configured as part of the VRF.

When enforcing VRFs to a device after upgrading to version 8.2.5, merge any **Default Gateway IP Addresses** from the device into Extreme Management Center's configuration to prevent incorrect configuration of the device.

4.5 Device Configuration Information

4.5.1 VDX Device Configuration

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**.

4.5.2 VSP Device Configuration

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
```

4.5.3 ERS Device Configuration

ERS devices may automatically change VLAN configurations you define in Extreme Management Center. To disable this, change the `vlan configcontrol` setting for ERS devices you add to Extreme Management Center by entering the following in the device command line:

```
CLI commands
enable
config term
vlan configcontrol flexible
```

Additionally, configure all VLANs on an ERS device's port with the same tag status (tagged or untagged). If enforcing to an ERS device on which a port has at least one VLAN as tagged, Extreme Management Center adds all untagged VLANs to the tagged VLAN list and clears the untagged VLAN list.

4.5.4 SLX Device Configuration

The script configuring the SNMP profile does not work unless you use SNMPv3 profile with the highest security level (AuthPriv) for SLX devices.

Unregister Trap Receiver does not work properly on SLX devices.

After you register an SNMPv3 trap receiver for SLX (using the SNMPv3 trap), manually modify the `/usr/local/Extreme_Networks/NetSight/appdata/snmptrapd.conf` file to receive the SNMPv3 trap. Capture the SNMPv3 trap to find the engineID that SLX sends. Add a line in `snmptrapd.conf` file using the engineID and restart the snmptrapd process (`/etc/init.d/nssnmptrapd restart`). For example, enter `add createUser -e <engineID> snmpuser MD5 snmpauthcred DES snmpprivcred`.

4.6 Firmware Upgrade Configuration Information

Extreme Management Center supports firmware downloads/uploads to devices using the TFTP, FTP, SCP, and SFTP protocols. However, before firmware images can be downloaded/uploaded from the server, Extreme Management Center needs to know the root path/directory for each of the protocols. The following shows the default root paths for each of the protocols and are configurable from the **Administration** > **Options** > **Inventory Manager** tab:

Protocol Root Path:

- TFTP: /tftpboot/firmware/images/
- FTP: /tftpboot/firmware/images/
- SCP: /root/firmware/images/
- SFTP: /root/firmware/images/

To upload firmware images 2 GB or less to the server, use the Extreme Management Center **Network** > **Firmware** tab. For files larger than 2 GB, use a third-party client (for example, SCP, WinSCP, FTP).

For example, enter the following to use SCP to upload a firmware image to the SCP root path on the server:

- `scp` *`<LOCAL_FIRMWARE_PATH>`* `root@`*`<Extreme Management Center_SERVER_IP>`*`:/root/firmware/images`

- Where:
  - *<Extreme Management Center_SERVER_IP>*= IP Address to Extreme Management Center Server
  - *<LOCAL_FIRMWARE_PATH>*= fully qualified path to a firmware image on the client machine

5. System Requirements

IMPORTANT: Extreme Management Center version 8.2 only runs on a 64-bit engine image. Any Extreme Management Center or 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

	Operating System
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 -Xmx	8 GB 12 GB	12 GB 18 GB	24 GB 36 GB	24 GB 36 GB
Disk Size	240 GB	480 GB	960 GB	1.92 TB
IOPS	200	200	10,000	10,000
Recommended scale based on server configuration:				
Maximum APs	250	2,500	25,000	25,000
Maximum Wireless MUs	2,500	25,000	100,000	100,000
Maximum Managed Devices	100	1,000	10,000	10,000
ExtremeControl End-Systems	N/A	50,000	200,000	200,000
Statistics Retention (Days)	90	180	180	360
ExtremeAnalytics	No	Yes	Yes	Yes
MU Events	No	Yes	Yes	Yes

Extreme Management Center Client

	Requirements
CPU Speed	3.0 GHz Dual Core Processor
Memory	8 GB (4 GB for 32-bit OS)
Disk Size	300 MB (User's home directory requires 50 MB for file storage)
Java Runtime Environment (JRE) (Oracle Java only)	Version 8
Browser* (Enable JavaScript and Cookies)	Microsoft Edge (version 41.16.199.10000.0 in compatibility mode) 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, Access Control, and Extreme Application Analytics virtual engines must be deployed on a VMWare or Hyper-V server with a disk format of VHDX.

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

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

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
Memory allocated to Java:			
-Xms -Xmx	8 GB 12 GB	12 GB 18 GB	24 GB 36 GB

	Small	Medium	Large
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
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 Access Control (ExtremeControl) Virtual Engine Requirements

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

Recommended scale based on server configuration:

ExtremeControl End-Systems	3,000	6,000	9,000/12,000[1]
Authentication	Yes	Yes	Yes
Captive Portal	No	Yes	Yes/No[1]
Assessment	No	Yes	No

[1] The Enterprise 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 Extreme Application Analytics virtual engine installation require 16 CPU cores. This is only available by purchasing a permanent license. To use the Extreme Application Analytics virtual engine with an ESXi free license, adjust the number of CPU cores to 8.

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

5.3.4 Fabric Manager Requirements

	Requirements
Total CPU Cores	4
Memory	9 GB
Memory allocated to Java: -Xms -Xmx	 4 GB 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 ExtremeControl deployment that is implementing agent-based assessment. Additionally, the end-system must support the operating system disk space and memory requirements as provided by Microsoft® and Apple®.

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

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

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

- McAfee
- Norton
- Kaspersky
- Trend Micro
- Sophos

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

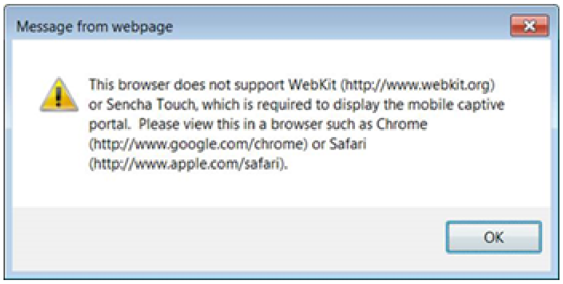
NOTES: A native browser indicates the default, system-installed browser. Although this may be Chrome (Android), this also includes the default, system-controlled browser used for a device's Captive Network Detection. Typically, this is a non-configurable option for Wi-Fi Captive Network Detection, but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

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

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

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

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



This browser does not support WebKit (http://www.webkit.org) or Sencha Touch, which is required to display the mobile captive portal. Please view this in a browser such as Chrome (http://www.google.com/chrome) or Safari (http://www.apple.com/safari).

5.6 Access Control 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 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 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
Alltel
Bell Mobility (Canada)
Cingular
Metro PCS
Rogers (Canada)
Sprint PCS
SunCom
T-Mobile
US Cellular
Verizon
Virgin Mobile (Canada)
Virgin Mobile

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 Mozilla Firefox Google Chrome Microsoft Edge Safari	11 and later 63 and later 65 and later 42 and later 12 and later
Mobile*	iOS Native Android Chrome US Browser Opera Firefox	9 and later 65 and later 11.5 and later 40 and later 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.
- If you are using self-signed certificates, they must be added in the Trusted Root Certificate store on the client machine or you may observe issues in the “print” use cases. This is only applicable for Microsoft Edge and Microsoft Internet Explorer browsers.

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