Extreme Management Center Release Notes Version 8.5.7

02/2022
9036781-10 Rev AA

Table of Contents

Version 8.5.7 Release Notes

The Extreme Management Center Release Notes provide information on the new features and enhancements included in version 8.5.7.6, as well as issues that have been resolved 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.

IMPORTANT: Upgrading to Extreme Management Center version 8.5.7 requires you to renew your NMS license if generated prior to July 31, 2020. Licenses generated prior to July 31, 2020 expire 90 days after upgrading to Extreme Management Center version 8.5.7.

You can view the status of your license by accessing **Administration > Diagnostics > Server > Server Licenses**.

For the most recent version of these release notes, see Extreme Management Center Release Notes.

For information regarding the features supported by specific devices, see the Firmware Support Matrix. Version 8.5.7 of Extreme Management Center supports the same devices listed in the matrix for version 8.5.5, with the addition of Extreme Campus Controller 5.36 and 5.46.

NOTE: NIS packages are not installed with the Extreme Management Center, ExtremeAnalytics, or ExtremeControl Engines.

Refer to the Sectionf **Engines** of this Release Notes document for more information.

NOTICE: Extreme Management Center's Transition to ExtremeCloud IQ

Extreme Management Center has transitioned to Extreme Networks' cloud-based environment, ExtremeCloud IQ.

Contact your representative to have your Extreme Management Center license migrated to an ExtremeCloud IQ - Site Engine licensing model. The ExtremeCloud IQ - Site Engine license also includes licensing for ExtremeAnalytics.

Customer Defects and Security Enhancements

This is the list of customer found defects found in the software releases of 8.5.

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.

Customer Found Defects Addressed in 8.5.7

Extreme Management Center CFDs Addressed	ID
The Interface Details PortView values for TX, RX, and Total Utilization percent were incorrect.	02350211
A Port Template that was previously deleted and then was added back with a new template was not properly added.	02358680 02406713 02434566
Occasionally, devices were not being polled by ExtremeCloud IQ - Site Engine in environments where SNMPv3 is heavily used.	02389786
Predefined port templates are no longer allowed to be removed.	02446435
NBI pre-reg useDiscoveredIP has been added back in. If set, ZTP+ will use the discovered IP and management interface for configuration.	02455391

ExtremeAnalytics CFDs Addressed	ID
Duplicate end point locations were no longer populating the site configuration.	02217766 02330868 02452213
10GB Adapters were not recognized on PV-A-300 Hardware.	02402772

Customer Found Defects Addressed in 8.5.6

Extreme Management Center CFDs Addressed	ID
Portview Usage Percentages Corrected PortView was displaying low usage percentages for 10G full duplex ports. This issue has been corrected.	02350211
Customer Feedback Program Time Out Corrected Extreme Management Center's Customer Feedback Program usage check was timing out too soon for customers with 300-500+ devices, which was preventing updated subscription and wireless endpoint licenses from downloading. The issue has been corrected.	02363551 02355548
Issues with Base License and Wireless Tab and Reports Corrected The Wireless tab was not opening and the error message, "Could not Load Report" displayed when it was the initial view and the license used was NMS. This issue has been resolved.	02385940 02335769 02406887
Notify Engine Timers Set to Null Now Are Canceled Setting Notify Engine Timers to null was causing timer threads to accumulate because the timers were not actually canceled. The accumulation was leading to potential Out of Memory errors and the inability to create new threads. The issue was fixed and null threads are now always canceled.	2307751

ExtremeAnalytics CFDs Addressed	ID
Issues Caused by Duplicate End-point Locations Corrected Duplicate end-point locations were causing issues in the ExtremeAnalyticsengine. The issue has been resolved.	02330868
Unrelated End-points No Longer Included in Defined Sites or Locations Unrelated end-points were improperly being included in defined sites and end-point locations. The issue has been corrected.	02217766 02330868
Correct Drivers for 10G Uplink for PV-A-300 Added Extreme Management Center version 8.5.5 did not include the correct driver files for the 10G uplink for the PV-A-300 upgrade. The drivers have been updated and the correct driver file is now included.	02402772

ExtremeControl CFDs Addressed	ID

Usernames in MAC Format Now Included in End-Systems End-system authentication of 802.1x devices was clearing usernames that were configured with MAC addresses. This is no longer occurring.	02332925
LDAP Authentication Failures for Unformatted MAC Addresses Improved Unformatted MAC addresses used for LDAP authentication were incorrectly being formatted with delimiters, which caused the authentication to fail. The issue has been corrected.	02344542

Guest and IoT Manager (GIM) CFDs Addressed	ID
In the Guest and IoT Manager (GIM), REST API was not using the same regex for email checks as the GIM UI . The issue has been fixed and now both GIM and and Rest API use the same regex for email checks.	02331153

Customer Found Defects Addressed in 8.5.5

Extreme Management Center CFDs Addressed	ID
Policy Enforce to ExtremeXOS Patch Failure Corrected Extreme Management Center version 8.5.2.6 Policy Enforce to ExtremeXOS version 30.7.1.1patch1-54 fails for Roles with names starting with "802.1x". The issue has been corrected	2306872
Popups Now Able to be Prevented There was no ability to globally prevent window popups on various pages in Extreme Management Center. The issue has been corrected.	01993579
Add Device to Policy Domain Functionality Improved Manually adding a device to Extreme Management Center with the "Add Device to Policy Domain" action selected in the Site Actions was failing to add the device. In some cases, future attempts to add a device would also fail, requiring the user to restart the Extreme Management Center server.	02334861
RMA Process Completing Properly The RMA process was not completing when the **Configuration Updates** field was set to **Never** in the World site.	02259784
PV-A-300 Hardware w/ 10GB Adapter Not Recognized In Extreme Management Center The PV-A-300 Hardware w/ 10GB Adapter was not being recognized in Extreme Management Center versions 8.1.7.27, 8.3.0.111, and 8.5.	02265680

Extreme Management Center CFDs Addressed	ID
Cold and Warm Start Traps Labeled Correctly As Warning Alarms Cold and Warm Start traps were improperly labeled as information alarms. Now, Cold Start and Warm Start Alarms are warning level alarms instead of information level alarms by default.	02307127
Device Menu Actions Launch Function Improved Device menu actions were not launching properly from the **Alarms and Events > Alarms** tab.	02290186
Process to Delete VLANs Clarified Customers wanted to delete VLANs, but did not realize that VLANs cannot be deleted from sites when defined within the parent site. The delete process has been clarified that VLANs should be added only to the specific sites for which they are intended, and not to parent sites of intended sites.	02222569
Delete Extreme Management Center Data Function Working Properly When a device's firmware was not known, the device data was not deleting when the **Delete Extreme Management Center Data** function was selected. This issue has been corrected.	02312388
NBI PortData.portSpeed Value No Longer Being Used The NBI PortData.portSpeed value was no longer being used and had been replaced by portConfigSpeed (when auto is disabled) and portConfigSpeedList (when auto is enabled). PortData.portSpeed has been removed from the NBI.	02319113
Documentation on ClientID for NBI Clarified Clarified in documentation that in order to access the following information through the Northbound API, the Client ID must also be assigned to an Authorization Group: • Workflow Queries (only the NetSight Administrator Authorization Group can access System Workflows) • Workflow Mutations • Task Mutations • Device Mutations	02314907
Menu Actions Launch Successfully from Alarms View All menu actions now successfully launch from the Alarms view in Extreme Management Center.	02290186
Alarm Trap Action Now Sends SNMPv2 and SNMPv3 Traps Not Informs The Alarm Trap action was sending informs if configured to SNMPv2 or SNMPv3 for action. Now, Alarm Trap action supports the ability to send SNMPv2 and SNMPv3 traps instead of informs.	02253512

Extreme Management Center CFDs Addressed	ID
Connection Issues between Extreme Management Center and Extreme Wireless Connectors (EWCs) Improved When an EWC was down and not reachable from Extreme Management Center, multiple contact requests created for that specific controller caused slowness in Extreme Management Center. This issue has been corrected.	189978 1915223

ExtremeAnalytics CFDs Addressed	ID
The Appid Process Performance Improved The Appid Process was occasionally crashing. The issues have been addressed.	02289778
3rd Party Sflow Collector No Longer Being Overwritten 3rd party sflow collectors for VSP devices were being overwritten by Extreme Management Center when the device was removed. A second collector ID is now used if the first collector ID is in use.	1926465

ExtremeControl CFDs Addressed	ID
Changes to ExtremeControl RADIUS Server Certificates Now Display Changes to ExtremeControl RADIUS Server certificates were not shown in the WebView certificates diagnostics page after enforce until the engine was restarted. This issue has been corrected.	02315158
Import Function for User Groups Improved Import of User Group entries was causing the enforce to fail. This issue has been corrected.	2270556
SMS Texts Now Sent During Guest Registration if One Service Provider is Configured for Sending Authorization Codes. SMS texts were not sent during captive portal guest registration if there is only one service provider configured to choose for sending authorization codes. The issue has been corrected and texts can now be sent if only one service provider option is available for sending authorization codes.	02311032

Customer Found Defects Addressed in 8.5.4

Extreme Management Center CFDs Addressed	ID
Slow Page Loads and Error Messages for Servers with Large Scale Configurations Corrected Extreme Management Center was running slow with page load errors on Extreme Management Center servers with large scale configurations.	02309089

Extreme Management Center CFDs Addressed	ID
Warning Added for Flexview Listings Exported to .CSV Reports Delays were occurring when Flexview / Physical Entity Listings were exported to .csv reports because of the large volume of data being exported, and the reports were failing to execute. A new warning message has been added that indicates that more than 2,000 records are being exported and the report will take some time to generate, and the timeout has now been increased from 30 seconds to five minutes.	02268103
Support for MyVendorProfiles Now Included in Backup/Restore Operations MyVendorProfiles were not included in the backup/restore operations.	02141955
Newly Added Archives Display in Detailed View Archives that contain a group were not displaying newly added devices in the Detailed View. Now, If devices are added to the group, they will be archived the next time the scheduled archive is executed.	1801552
Scheduled Tasks During Daylight Savings Time Execute Scheduling tasks for Sundays that transition from Daylight Savings Time to Standard Time displayed an "Add failed" error dialog. Scheduled Tasks can now be started on Sundays which transition from Daylight Savings Time to Standard Time (or vice-versa).	02267383
TCL Scripts No Longer Requiring Script to be Saved Execution of TCL scripts that use "scope = device" were requiring the script to be saved, even when there were no changes to save.	02283123
Enforce Time of Policy Domain Lag Time Improved Enforce of a policy domain was experiencing extremely long completion time.	02156722
Duplicate VLANS No Longer Imported When .PMD Files Imported When policy .pmd files were imported into the policy domain, duplicate VLANs were being imported. Duplicate VLANs are no longer being imported.	02005844
Netlogins Preserved During Enforce to ExtremeXOS After Change to ACL Policy Role Mode When changes were made to the ACL / policy role mode, the netlogin was being disabled during enforce to ExtremeXOS. This issue has been corrected and netlogins are preserved during enforce.	02248336
IP/UDP/TCP Rules Properly Enforced to Extreme Campus Controller Some rule types were failing to be set because the IP/UDP/TCP rules were not being enforced correctly to the Extreme Campus Controller.	02303839
ACL Policy Role Data Correctly Transferred During Upgrade When upgrading from Extreme Management Center version 8.5.2 to version 8.5.3, incorrect NAS-Filter-Rule ACL policy role data was being transferred. As a result, HP and Cisco devices were not working properly.	2304517

Extreme Management Center CFDs Addressed	ID
Login and Password Error Message Removed An error message was generating when a password or login was copied and pasted into the field during login attempts. The message is no longer generated.	02274240
Script Documentation No Longer Includes Custom Scopes Extreme Management Center Documentation topic on "Creating Scripts" incorrectly included references to a "Custom" scope. Only global and device scopes should be described.	02276871

ExtremeAnalytics CFDs Addressed	ID
Imported and Exported Locations Execution Improved; Error Message No Longer Generated When attempting to import or export locations in ExtremeAnalytics, an error message was being generated and the imports and exports were not always executing successfully.	02260320

ExtremeControl CFDs Addressed	ID
Enforce to Extreme Campus Controller Failing to Create Rate Limits Enforcing policy to Extreme Campus Controller was failing to create new rate limits.	02307178
In-Use Check Verifies Mappings Not Set as Default Before Deleting Policy mappings could be deleted if they were set as default policy mappings in ExtremeControl options. Now, the in-use check verifies the mappings are not set as default before allowing delete.	02307796
Incorrect Successful Policy Enforce Corrected Policy Enforce to Extreme Campus Controller was reporting success after failing to enforce the configuration to the device. The REST set failure events were reported in the event log.	02307184
Captive Portal No Longer Setting OS from the Browser The captive portal was sometimes incorrectly setting the OS from the browser in an end-system session, resulting in unexpected device type rule processing.	01951730
IP Subnet Config No Longer Preventing Proper Subnet Mapping Setting IP subnet configuration location value to None was preventing proper subnet mapping by VLAN ID or VLAN Name on the ExtremeComplianceengine.	02161385
Renaming Access Control Profiles No Longer Corrupting Database Renaming Access Control profiles was sometimes corrupting the database and leading to "Cannot load reports" errors when trying to view configuration rules.	02280562

ExtremeControl CFDs Addressed	ID
Case Insensitive UserNames No Longer Preventing ExtremeControlEngine From Joining Domain ExtremeControlengine was not successfully joining the domain when case insensitive usernames, hostnames, and other lookup fields were entered. Now, ExtremeControl joins the domain when new LDAP configurations and authentications using new LDAP configurations with mixed-case user and host name data are entered.	02265831

Customer Found Defects Addressed in 8.5.3

Extreme Management Center CFDs Addressed	ID
Remove From Service Option Clarified When Remove from Service was selected on the Configure Device window for a device, it was unclear that Extreme Management Center continues to monitor that device. Additional directions have been added to Help documentation that, once a replacement device is ready, the RMA process is continued by adding the replacement device's serial number, shutting down the device to be removed, and starting the replacement device. In order to stop monitoring the device, you also need to change the Poll Type to Not Polled.	02249867
VSP Series Family Type Expanded to Include Multiple Vendors The VSP Series option could not be selected as Family type on the Site > Actions > Custom Configuration tab for more than one vendor, even if multiple vendors supported the VSP Series as a Family type. Now, multiple vendors can have the VSP Series as a Family type.	02230122
EMail List Function Improved for Workflow Mail Activity Once selected, there was no way to unselect Email lists for a Task or Scheduled Tasks Workflow's Mail Activity.	02258069
Default SFTP/SCP User Name and Directory Now Set in Inventory Manager Default SFTP/SCP user names and directories are now set in **Administration > Options > Inventory Manager**.	02288993
Extreme Management Center Upgrades Completing Properly Upgrading to Extreme Management Center version 8.5.1 was sometimes exiting halfway and not completing because files were not found during the upgrade process. Additional checks have been added to ensure all files are in place during upgrade and that upgrade completes successfully.	02265429

ExtremeAnalytics CFDs Addressed	ID
Introducing the Application Sensor and Analytics Engine Extreme Networks is introducing the new Extreme Application Sensor and Analytics Engine. This new Analytics engine combines the sensor and engine into one package, eliminating the need for additional hardware requirements.	-----
New DHCP Fingerprint for Apple Mobile Devices A new DHCP fingerprint for Apple mobile devices that run iOS 14 has been added.	02250934
Extreme Management Center and ExtremeAnalytics Start-up Improved After upgrading to Extreme Management Center version 8.5.0, Extreme Management Center and, in turn, the ExtremeAnalyticsengine, were not starting up completely. This issue has been corrected and start up for both now completes properly.	02236775 02250432

ExtremeConnect CFDs Addressed	ID
The ExtremeConnect Services API online documentation was missing after Extreme Management Center version 8.3.3 update. Those pages have been added back to the online Help documentation with Extreme Management Center version 8.5.3.	02253977

ExtremeControl CFDs Addressed	ID
MAC Lock Additions and Deletions No Longer Require Enforce MAC Lock additions and deletions were requiring an enforce. The issue has been fixed so that no enforce is needed to make additions or deletions.	-----
Multiple RADIUS Certificates Now Supported ExtremeControl version 8.5.3 now supports installing multiple RADIUS Certificates on an ExtremeControlengine. During 802.1X authentication, the installed RADIUS Certificate will be used and exchanged based on incoming RADIUS packet data, such as User-Name, NAS-IP-Address (Switch IP) or Calling-station-id (MAC Address). This is called 'Attribute to EAP Group Mapping' in ExtremeControl. With this feature, ExtremeControl now includes the capability to specify an EAP Group to store RADIUS server certificate(s), from which you can designate RADIUS certificate(s) for each tenant in your network instead of using the default RADIUS certificate for all tenants.	01946914
Port Authentication Function Improved The "Disable Authentication on all Ports" function on the **Control > Policy** tab was displaying a list of ports that included ports that do not support authentication. This issue has been corrected.	02236922

ExtremeControl CFDs Addressed	ID
New Extreme Management Center NMS or NMS Advanced Licenses Can Now Be Applied to ExtremeControlengines New Extreme Management Center NMS or NMS Advanced licenses can now be applied to ExtremeControlengines if the engine license is within the grace period number of days before expiration.	02264108
ADV190023 - Microsoft Guidance for Enabling LDAP Channel Binding and LDAP Signing Security Advisory ADV190023, published August 2019, suggested changing default security settings within Active Directory. Changes to some of these settings could impact the interoperability of ExtremeControl within Active Directory environments. The impacts to the ExtremeControlengine would be: • All current releases of ExtremeControl are impacted if LDAP-based (cleartext) AAA configurations are used and LDAP Signing is enabled. • Enabling LDAP Signing for LDAP-based configurations will prevent ExtremeControl from performing LDAP queries to Active Directory. • Use of LDAPS (Secure LDAP) transport is recommended to work around this security requirement. • In environments where LDAPS is not available, disabling the LDAP Signing security setting on Active Directory is required. • There is no impact to any current release of ExtremeControl if LDAPS-based (secure LDAP) AAA configurations are used. • There is no impact to changes for LDAP Channel Binding as noted in the advisory. Please refer to GTAC KB article https://gtacknowledge.extremenetworks.com/articles/Q_A/000044961 for more information and optionally visit Microsoft's site for updated information about this proposed change: https://msrc.microsoft.com/update-guide/en-us/vulnerability/ADV190023.	01970727 01975814

Customer Found Defects Addressed in 8.5.2

Extreme Management Center CFDs Addressed	ID
Map Scale Issues Corrected Setting the scale on a map (away from the default setting) was causing the map to corrupt. The scale workflow issue has been corrected and maps no longer corrupt if the scale is adjusted. In addition, sometimes when a map was created or edited, the Map Scale was dramatically increased or decreased, and the drawings on the map were duplicated. These issues have also been corrected.	02242633

Extreme Management Center CFDs Addressed	ID
Extreme Management Center Log-In Delays Improved Log-in delays seen in Extreme Management Center, caused by third-party devices with poor SNMP response time, have been addressed. In addition, the License Diagnostics page now includes the time it takes to retrieve license counts and to refresh the data.	02247375

Customer Found Defects Addressed in 8.5.1

Extreme Management Center CFDs Addressed	ID
DvR Functionality Supported in Extreme Management Center Extreme Management Center now supports DvR functionality to provide routing redundancy in a fabric-connect network. **NOTE:** VOSS devices support a new "dvr-one-ip" feature in the 8.2 release that allows you to share an IP address between a VLAN and its DvR interface. Extreme Management Centercurrently does not support the "dvr-one-ip" feature and cannot read or enforce configurations of this type. Configure VOSS device IP addresses on VLANs and their DvR interfaces through the **VLAN Definition** tab.	-----
New Warning For NMS-EVAL License Expiry No warning was issued when an NMS-EVAL license was about to expire. New notifications have been added to alert users prior to NMS-EVAL license expiry.	-----
Extreme Management Center Now Supports Unified Series 5520 Devices **NOTE:** Changing unified series devices from ExtremeXOS to VOSS or vice versa is not supported in Extreme Management Center. We recommend the following steps when changing a unified series to a different operating system. 1. Delete the device from Extreme Management Center (make sure the check box is checked to delete from database). 2. Manually change the device to the different operation system ("ExtremeXOS to VOSS" or "VOSS to ExtremeXOS" or use ExtremeCloud IQ to perform this action). 3. Add the device back into Extreme Management Center.	-----
Remove From Device Group Available When Multiple Devices Selected The **Remove From Device Group** menu action was available only when a single device listed under a User Device Group was selected. It is now available when one or more devices listed within the Devices table are selected.	01709827 01971882
Overview Tab Functionality for Imported Scripts Corrected Overview tab functionality has been corrected so that scripts that are imported or edited via the Overview tab are no longer corrupted.	02216199
Support for RADIUS ERS-CoA-Reauthenticate Attribute Added Support for RADIUS ERS-CoA-Reauthenticate attribute has been added for Extreme ethernet routing switches.	02200420

Extreme Management Center CFDs Addressed	ID
RADIUS Servers Now Configurable on Several Tabs Extreme Management Center is now able to configure RADIUS servers in Administration, Users, Manage SSH Configuration tabs.	02219510
MIB Not Supported Error Not Improperly Reported 3rd party devices were reporting a "MIB Not Supported" error even though they had a valid script associated to them for archives. This error is no longer being reported in these cases.	01932839 02190132
Schedule Options Properly Displayed The **Device Reset** screen was displaying the schedule option when devices in the group did not support scheduled operations (for example, VOSS and EWC devices). Now the schedule box does not display if at least one of the devices in the group does not support the scheduled reset.	01917452
New Capability to Rediscover Added The capability for executing a "Rediscover" of a device has been moved from the **NetSight OneView>Access OneView Administration** capability and is now included with the **NetSight Suite > Devices > Add, Discover, Import** capability.	02177860
New Capability to Launch WebView Added The capability for executing a "WebView" of a device has been moved from the **NetSight OneView > Access OneView Administration** capability to a new capability: **NetSight Suite > Devices > Launch WebView**. NOTE: If you are upgrading to Extreme Management Center Version 8.5.1(and future versions), the "Launch WebView" capability is enabled by default for new Authorization Groups. For Extreme Management Center Versions 8.5.0 or earlier, the "Launch WebView" capability is DISABLED by default. After upgrading to version 8.5.1, you must review and modify your Administrative Groups and configure them for “Launch WebView” individually.	02177860
Message Added to Warn of Impact to Tasks When Deleting User Profile A new message warns that, when deleting a user profile, the scheduled firmware and archived tasks created by the user being deleted are impacted.	01930813 01931694
Standby Units Identified for Archiving ExtremeXOS Devices ExtremeXOS stacks with backups but no standby units were failing to archive the configuration. Standby units have been identified to successfully archive ExtremeXOS devices.	02230235 02229333
Password Updates and Prompts Improved Changes have been made to properly update passwords and ensure password change prompts occur.	01918709 01977127
Loading Icon Introduced to DeviceView A loading icon has been introduced for the DeviceView that remains visible until all the grids of the tab are loaded to prevent an empty view from displaying if there is a delay in the rendering of one grid.	1987849
ZTP+ Onboarding for VOSS Devices Added VOSS devices can now be configured using the ZTP+ onboarding process.	-----
Message to Use System Workflow Added A new message to use a System Workflow instead of using Legacy Inventory scripts when attempting to upgrade VDX devices has been added.	1869524

Extreme Management Center CFDs Addressed	ID
Alarm Refresh Interval Updated An additional Refresh interval of 5 seconds has been added to Alarms in Extreme Management Center.	01992245
Warning Message for Port Settings Added A warning message has been added that alerts you if an HTTP/HTTPS port was set to a value less than 1024, and Extreme Management Center was installed as non-root user, the setting is ignored and not saved.	01910126
Ability to Access Scheduled Tasks Improved If the (legacy) Access OneView Administration option was disabled, the **Access Scheduled Tasks** option was also being improperly disabled. Now, if the Access OneView Administration option is disabled, the Access Scheduled Tasks option is no longer disabled.	01883066 01988991 02208186
Export to CSV Button Added to Ports Tabs A new **Export to CSV** button has been added to Extreme Management Center's **Device View > Ports** and **More Views > Port Tree** tabs that provides the ability to export port details to a .csv file.	1926242
Ability to View Configuration Options for Archived Devices Added Two new options to View Configuration have been added to the **Device** and **DeviceView** tabs: • DeviceView > Archives > Select a Config file > View Configuration • Right-click a Device > Archives > View Last Configuration In addition, you can now select View Configuration File from the **Archives** tab to view archive information for ERS8600 series devices.	02234207
Ability to Add Tagged and Untagged VLANs for LAG / MLAG Added You can now add Tagged & Untagged VLANs for LAG/ MLAG on the Configuration > Ports tab.	-----
Maximize Feature Added to Tasks Windows The Maximize feature has added to several **Tasks > Scripts and Tasks > Workflows** windows.	1889058

ExtremeAnalytics CFDs Addressed	ID
New Titles and Data Added to ExtremeAnalytics Reports Additional data has been added for several ExtremeAnalytics reports, which are accessible on the **Analytics > Reports and Reports > Reports > Application Analytics** tabs. The enhanced reports (with new titles) are: • Analytics Events • Bandwidth for a Client Over Time • Most Popular Applications • Most Used Applications for a Client • Most Used Applications for a User Name • Network Activity by Cloud Region and Site • Network Activity by Site • Network Activity for a Client • Network Activity for an Application • Sites Using the Most Bandwidth • Slowest Applications by Site	1783081
Insights Dashboard Drill Down Displays Correct Data The **ExtremeAnalytics > Insights Dashboard Response Time** ring chart often displayed error data (in red); however, if you select the error data to drill down for details, no errors displayed on the Tracked Applications Dashboard. Now the Tracked Applications Dashboard displays the appropriate error data.	01854859
Dashboard Response Time Results Now Consistent The ExtremeAnalytics Dashboards were displaying inconsistent Response Time results. The **Insights, Network Service,** and **Tracked Application Dashboards** now all display consistent Response Time results.	01846024
Disable and Enable Options for Web Applications Fingerprints Functioning Properly The Disable function for fingerprints was improperly continuing to display data. The Disable and Enable options are now functioning properly for Web Application fingerprints.	01978971
False Data From Exports No Longer Seen ExtremeAnalytics was showing incorrect data when processing records exported from FortiGate firewalls. The issue has been corrected and false data is no longer seen.	02000756
Flow Collection Process Corrected to Discontinue Continual Issuing of SNMP Requests The ExtremeAnalytics engine was constantly issuing SNMP requests for switch port data. The flow collection process has been corrected to prevent performing any unneeded SNMP on the engine and should significantly reduce the load on the engine.	2161359

ExtremeControl CFDs Addressed	ID
New ExtremeControl Engine Property Added A new ExtremeControl engine property, "AAA_STRIP_USERNAME_USE_LDAP_CONFIG" allows AAA auth requests using LDAP configuration to strip or preserve the domain name in usernames for auth request from the LDAP configuration being used.	01937405
Option to Skip EAP-Message Check Added ExtremeControl engine settings now allow you to skip the EAP-Message check when determining if a request is administrative.	01414443
Web View Rendering Process Improved Large configurations and rules in ExtremeControl were causing the web view to lag and load slowly. Pagination has been introduced for the Rules table and for the Groups tab, and page size has been set to 100, to speed the rendering process for the web view.	01938001
Ability to Override RADIUS Shared Secret Via NBI ExtremeControl northbound interface (NBI) now allows you to override a RADIUS shared secret when creating or updating a switch on an Access Control engine group.	-----
SNMP Profile Changes Cause Enforce Flag Changing switch SNMP profile in either the ExtremeControl configuration or the **Network > Devices** view now causes an enforce flag.	02168972
WebView and Terminal Features Added to End System Table WebView and Terminal features were included on the **ExtremeControl > Access Control > End System** table. Webview and Terminal options have been added to the End System table menu.	1926229
GIM Sponsor Retrieval Advanced Configuration Feature Added A new feature in Extreme Management Center and GIM (Guest and IoT Manager) enables you to choose how you configure the method of retrieving sponsors in the GIM Domain.	01978498 01898456 01816454

Customer Found Defects Addressed in 8.5.0

Extreme Management Center CFDs Addressed	ID
Port Template Enhancement In addition to User-configured Port Templates, Extreme Management Center now supports Vendor-configured Automated Port Templates. After Extreme Management Center discovers devices via ZTP+ and asks for configuration, the automated port templates are automatically assigned to the ports on the device.	-----
Policy ACL Rule Management Support Extreme Management Center version 8.5.1allows you to manage ACL rules on ExtremeXOS devices on which version 30.5 or later is installed. By using ACLs, the access control entries (ACEs) can be ordered by the administrator, allowing for more flexibility in the configuration and better utilization of hardware resources on the device. ExtremeXOS uses the IETF YANG data model for ACLs (ietf-access-control-list) defined in RFC- 8519.	-----
New FlexView for BOSS Power Supply Information Serial Numbers and Power Supply information were not included in the BOSS Chassis Components FlexView for ERS devices on which BOSS 7.8.x or later was installed. The information is now in a new FlexView called BOSS Power Supply Information.	1943390

Extreme Management Center CFDs Addressed	ID
Enhancement to Alarms in Extreme Management Center Beginning in Extreme Management Center version 8.5.0, you can open the map to which a device belongs from the **Alarms** tab.	1709802
VRRP Provisioning Support Added for VSP Devices Extreme Management Center now supports VRRP (Virtual Router Redundancy Protocol) provisioning. Using the **Configure Device > VLAN Definitions** tab, you can configure your VSP devices to form a virtual router interface to act as a redundant forwarding element for the network.	-----
ExtremeCloud Appliance Versions 4.56.02 and 5.06 Now Supported Extreme Management Center 8.5.0 now supports ExtremeCloud Appliance versions 4.56.02 and 5.06.	-----

ExtremeControl CFDs Addressed	ID
Functions Added to LDAP Mappings The Add, Edit, and Delete functions, as well as Import and Export functions, for LDAP Mappings have been added to the **Configuration > AAA** tab and **Configuration > Access Control > Profiles** tab.	01912554 01979187
Filter Enhancements to Rules Tab Added Columns on the ExtremeControl **Configuration > Rules** tab now can be filtered by criteria you define.	01889129

Engines

NIS Packages Not Installed with Engines

NIS packages are not installed with the Extreme Management Center, ExtremeAnalytics, or ExtremeControl Engines.

During installation, if you select yes at the “Do you want to use NIS? (y/n)” prompt, you must install the NIS package for it to function.

To do this, run:

```
apt update
apt install nis
```

The NIS package install will ask you if you want to keep `/etc/yp.conf`. Choose ‘N’ (the default) to keep your existing `yp.conf` file. NIS should then work.

To test it, use a command such as “`ypcat passwd`”.

Upgrades Accessible to Engines without Internet Connectivity

Upgrades for the Extreme Management Center server, the ExtremeAnalytics engine, and the ExtremeControl engine are now accessible without internet connectivity.

Operating Systems Upgrade to Ubuntu 18.04

The Extreme Management Center, ExtremeAnalytics, and ExtremeControl engine operating systems have been upgraded to Ubuntu 18.04.

Fabric Manager VM OS Upgrade to Ubuntu 18.04

Beginning with Extreme Management Center 8.5.5, the Fabric Manager VM operating systems have been upgraded to Ubuntu 18.04.

For customers that have Internet connectivity in the lab systems:

- Initiate engine upgrade as per the recommended procedure.
- Perform an online OS upgrade, using the following CLI commands:
  - `#>apt update`
  - `#>apt upgrade`
  - `#>apt autoremove`
  - `#>do-release-upgrade` (Follow the instructions and retain any `.conf` files that might have been updated during the original configuration of the Fabric Manager.)
- Once the upgrade is completed, confirm the status of the OS version:

```
#>lsb_release-a
No LSB modules are available.
Distributor ID: Ubuntu
Description: Ubuntu 18.05.5 LTS
Release: 18.04
Codename: bionic
```

For customers that do not have Internet connectivity in the lab systems:

- Save and back up any data on the Fabric Manager as per the recommended procedure.
- Delete the Fabric Manager from the device inventory in Extreme Management Center. (Check the Remove from the database option.)
- Shut down the Fabric Manager VM.
- Deploy a fresh VM from the latest release with the updated Ubuntu.

Extreme Management Center

- Support for Extreme Campus Controller 5.46 Added
- Support for Extreme Campus Controller 5.36 Added
- VOSS rcnaAuthenticationFailure trap Now Supported
- Polling Expanded to Include snmpEngineTime

- Fabric Attach and Switched UNI Enhancement
- Enhancements to VPEX
- Improvements to Server Certificates
- 11ax Radio for AP5xx Models Supported
- Enhancements to Network Status Summary
- New Wireless FloorPlans Summary Added
- Enhancements to ExtremeConnect

Support for Extreme Campus Controller 5.46 Added
Extreme Management Center now supports Extreme Campus Controller version 5.46.

Support for Extreme Campus Controller 5.36 Added
Extreme Management Center now supports Extreme Campus Controller version 5.36.

VOSS rcnaAuthenticatonFailure Trap Now Supported
Extreme Management Center now supports VOSS rcnaAuthenticationFailure traps.

Polling Expanded to Include snmpEngineTime
Extreme Management Center now polls for snmpEngineTime (if present on the device) for determining sysUpTime.

Improvements Made to Import Tab in Workflows
The Import tab of a Workflow script activity has been enhanced.

Filters Added to Port Templates Tables
Column filters have been added to the Port Templates table in the **Network > Devices > Sites** tab, as well as a button to quickly filter the table to show all templates or only the Local templates. Also, a filter was added to the Port Template field on the **Device Configuration View > Ports** tab that you can type to filter the list, which makes the port template selection process easier.

MIB Tools and Flexview Editor Launched as Standalone App
The MIB Tools browser has been combined with the FlexView Editor diagnostic tool, which can now be launched as a standalone application. To launch, navigate to your Extreme Management Center server IP (`https://<your XMC Server IP>:8443/Clients/MIB_Tools.jnlp`) or access it from the **Administration > Diagnostics** tab.

NOTE: Access to the MIB Tools and FlexView Editor diagnostic tool via the Console Java application will be removed in a future release.

Policy Domain Evaluation Tool Launched as Standalone App
The **Generate Wireshark Filters** menu dialog has been repackaged into the Policy Domain Evaluation Tool, which can now be launched as a standalone application. To launch, navigate to your Extreme Management Center server IP (`hhtps://<your XMC Server IP>:8443/Clients/PMDEval.jnlp`) or access it from the **Administration > Diagnostics > Server Utilities** tab.

Customer Experience Option Added

A new Customer Experience option has been added to the **Administration > Options** tab, which allows customers to opt out of providing feedback.

Unified Switching Devices Now Supported by Extreme Management Center and Fabric Manager

Extreme Management Center Compliance and Fabric Manager now support Unified Switching 5420 devices.

Workflow Charts Renamed

Charts in the Workflow Dashboard have been re-labeled from "Completed" to "Successful" and from "Failed" to "Unsuccessful" to minimize confusion.

SHA256 Checksums Now Used

Extreme Management Center files are now published with SHA256 checksums, instead of MD5 checksums.

VSP VLAN/ ISID Pruning Function Added

CVLAN UNI L2 Services that are associated with VLANs that are pruned are now also pruned themselves.

NOTE: VLAN pruning occurs when the VLAN does not have any ports associated with it, and pruning has been enabled.

DvR Redistribution Allowed

Extreme Management Center now allows you to redistribute static and locally configured routes via DvR.

Capabilities for Map and Sites Access Enhanced

The Authorization Group > NetSight OneView capabilities for Maps and Sites have been reorganized as "Maps Write Access," "Maps/ Sites Read Access," and "Sites Write Access."

NOTE: After upgrading from a previous version of Extreme Management Center, Authorization Groups should be reviewed to ensure the intended access with these refined capabilities.

New Threaded Blocking Queue

A new dedicated threaded Blocking Queue (JCiaQueue) has been introduced which is responsible to read/ write Langley messages. The JCiaQueue is introduced to address the intermittent loss of connection with ExtremeWireless controllers, which Extreme Management Center and ExtremeWireless Manager were experiencing that generated out-of-sync errors.

NOTE: The queuing functionality is configurable from NSJBoss.properties with the following key: LangleyMessageBus.useMessageQueue. If the key is set to true, then Extreme Management Center will use JCiaQueue. If the key is set to false, then Extreme Management Center will not use JCiaQueue. The Extreme Management Center server must be restarted in case any modifications to NSJBoss.properties file have been made.

New Limit on Backup/ Restore Log Files

A new feature has been added that removes backup or restored log files when the backup/ restore log file count exceeds 30. This new feature is enabled by default but may be overridden by adding the 'extreme.database.backup.loghistory.maxFiles' entry in the NSJBoss.properties file.

Statistics Collection Updated

The interval for collecting statistics on devices and ports has been moved from the **Administration > Options** tab to the Configure Device view. The Monitor Mode for statistic collection has been renamed Threshold Alarms Mode, and terminology in the Inventory Dashboard and **Administration > Options** has been changed accordingly. The statistics collection interval cannot be changed for devices that are being polled with ZTP+.

DeviceView Enhanced with Asset Tag, User Data, Notes

The DeviceView is enhanced to display the Asset Tag, User Data and Notes on a device in the Extreme Management Center server, if these attributes are configured on the device in Extreme Management Center.

Access Terminal Capability Added

The Access Terminal capability, in the NetSight OneView list of capabilities, controls your access to opening a terminal session from the device menu.

NOTE: If you are upgrading to Extreme Management Center Version 8.5.3 (and future versions), the Access Terminal capability is enabled by default for new Authorization Groups, but is DISABLED by default for existing Authorization Groups. After upgrading to version 8.5.3, you must review and modify your Administrative Groups and configure them for Access Terminal individually.

Search Result Field Added to Search Maps Function

A new Search Result field has been added that displays all the maps that include the client or device you searched, if that client or device is included in multiple maps. If the client or device you searched is included in only one map, that map opens as a result of the search.

Ability to Choose How to Access Device Web Session

From the Device > Configure Device tab, you can choose how to access your device's Web Session by modifying the device WebView URL. You can select either the default WebView URL, provided by Extreme Management Center, or enter another WebView URL.

NOTE: The ability to edit the device WebView URL is available only after the device is successfully onboarded to Extreme Management Center.

Ability to Export Filtered Events Added

The ability to export filtered events to a .csv file has been added to Extreme Management Center.

New Alarms Added In Extreme Management Center

The following alarms are available in Extreme Management Center version 8.5.1:

- Port RX %Utilization Threshold Alarm
- Port TX %Utilization Threshold Alarm

WebAccess Added to Authorization Group Capabilities

WebAccess has been added to the **Administration > Users > Group Authorization > Capabilities** tab.

Ping Device Feature Added

You can now send a Ping (ICMP or TCP Echo Request) to determine if a device is reachable. The timeout value for the request is configured in **Administration > Options > Status Polling > Ping > Length of Ping**

Timeout, and the result of the request is displayed in a pop-up dialog. Extreme Management Center installations that are configured to run as root issue ICMP Requests, while installations that are configured to run as users other than root will use a TCP Echo Request. In addition, the Ping Device feature, accessible via the **Alarms & Events > Search Maps > More Actions**, displays the results of a Ping Device.

NOTE: Firewalls and server configurations can block ICMP and/or TCP requests, which can result in an Unsuccessful Ping, even though SNMP, SSH, Telnet and other protocols are successful.

Devices Now Supported by Extreme Management Center

The following devices are now supported by Extreme Management Center version 8.5:

- AP310i-FCC
- AP310i-CAN
- AP310i-IL
- AP310e-FCC
- AP310e-WR
- AP310e-CAN
- Ap310e-IL
- AP360i-WR
- AP360i-CAN
- AP310i-FCC
- AP310i-CAN
- AP310i-IL
- AP310e-FCC
- AP310e-WR
- AP310e-CAN
- AP310e-IL
- AP360i-WR
- AP360i-CAN
- AP360i-IL
- AP360e-FCC
- AP360e-WR
- AP360e-CAN
- AP360e-IL

Discover Now Allowed for Sites Based on Add Device Capability

Discover is now allowed for valid sites based on Add Device capability. The capability for "Sites Read/Write Access" is not necessary for Site Discover, but it is necessary for adding or editing sites.

Clarification of Port Type Column in Device View > Port Tab

The Port Type column on the Device View > Port tab has been renamed Neighbor Capabilities and shows all advertised capabilities of the neighbor, instead of displaying “Interswitch” or “Access.”

Enhancement to Extreme Management Center Backups

A new checkbox on the Administration > **Backup/Restore** tab allows you to select whether alarm, end-system event, and reporting are included in Extreme Management Center backups.

Failed to Join Domain Alarm Added

A “Failed to Join Domain” alarm is now automatically generated in Extreme Management Center when an engine is unable to join a domain and an event is generated.

REST API Added to GIM

REST API has been added to GIM to increase the .CSV import level for devices from 200 to 5000, and to improve the time to provision these devices.

Fabric Authentication Type Enhancement

Fabric Enable in NNI mode now supports the SHA-256 Fabric Auth Type.

Fabric Attach and Switched UNI Enhancement

Extreme Management Center now supports Fabric Attach (FA) and Switched User Network Interface (S-UNI) on the same port at the same time.

This feature is supported by VSP firmware version 8.1.1 and later, and on all platforms currently supported by Extreme Management Center with two exceptions: XA1400 and VSP-8600.

Enhancements to VPEX

Extreme Management Center now supports the following Virtual Port Extender (VPEX) configurations:

- VPEX Ring Topologies – When two VPEX cascades are linked together, they form a VPEX ring. This type of ring provides a redundant connection from any bridge port extender (BPE) in the ring to the controlling bridge (CB).
  Extreme Management Center requires the controlling bridge to have ExtremeXOS 30.6 or later.
- One-Armed MLAGs – In this dual control configuration, the first tier BPEs are only connected to one of the two controlling bridges, which leaves more trusted ports available. In some applications, BPEs are limited to only two links for forming the ring, and the use of one-armed MLAGs is required.

Improvements to Server Certificates

The following improvements to server certificates are included in Extreme Management Center version 8.5:

- PKCS#12/ PFX keystores without a keystore password can be imported
- Unencrypted RSA private keys containing a "BEGIN RSA PRIVATE KEY" header can be imported
- Error messages are more descriptive

11ax Radio for AP5xx Models Supported

Extreme Management Center now supports 11ax Radio for AP5xx models.

Enhancements to Network Status Summary Report

The Network Status Summary PDF report has been updated to include the following enhancements:

- Reports display Top 10 instead of Top 5 statistics.
- New “Top 10 WLANs by Clients” and “Top 10 Clients by Bandwidth” reports have been added.
- Enhanced color and graphic resolution for all reports.
- Ability to select a site and generate a Network Status Summary based on the activity for that site.
- Scheduling capability to generate the Network Status Summary on an hourly, daily, weekly, or monthly basis.

The Network Status Summary reports are now also available in the **Reports Catalog** under the **Network** option in the left-panel tree.

New Wireless FloorPlans Summary Added

A new **FloorPlans Summary** report, which displays AP, WLAN and Client data based on selected floorplans, has been added to Extreme Management Center's **Reports Catalog** under the **Wireless** option in the left-panel tree. You can also schedule the FloorPlan Summary to generate hourly, daily, weekly or monthly reports.

Enhancements to ExtremeConnect

- New custom end-system data fields and additional operating system data fields have been added to ExtremeConnect.
- Extreme Management Center backups now include ExtremeConnect configurations.
- Beginning with Extreme Management Center version 8.5.7, the following ExtremeConnect modules are hidden by default:

  Several enhancements have been made to ExtremeConnect, including:

  - FiberlinkMaaS360
  - FntCommand
  - Intune
  - McAfee Dxl
  - McAfee EPO
  - MobileIron
  - MSLync SDN
  - OpenStack
  - Sophos Mdm
  - Xen Desktop
  - Xen Server
  - Xen Mobile
  - Domain Portal (cross-XMC search – has no UI anymore)
  - Eset Security
  - Nutanix
  - VWClever RDC

If you have enabled one or more of these modules, it should not be hidden in your network; however, ExtremeConnect may hide the module if it is disabled at any time. Hidden modules are still fully functional, but cannot be configured automatically by ExtremeConnect. To enable a hidden module, modify the configuration file manually.

ExtremeAnalytics

Streaming Flow Data from ExtremeAnalytics into Splunk

ExtremeAnalytics supports the ability to stream flow data from an ExtremeAnalytics engine into Splunk. This support includes instructions on how to configure IPFIX to work with Splunk and files that you can copy to the Splunk server to facilitate integration.

Improvements to Response Time Dashboard

The ExtremeAnalytics Response Time dashboard, when grouping by interface, displays only the device IP address for received Application Telemetry flow data when it is lacking sampled packet information.

Additional Devices Support Application Telemetry

Application Telemetry is supported on the following device types:

- EXOS Summit Series X440-G2
- EXOS5520
- ERS4900
- ERS5900

- VOSS5520
- SLX9740
- ERS devices running firmware versions later than 7.7.0
- BOSS devices running firmware versions later than 7.7.0

ExtremeCompliance

ExtremeCompliance now supports the following device types (as of Extreme Management Center Version 8.5):

- VSP4900-12MXU12XE
- VSP4900-24S
- VSP4900-24XE
- SLX9740-40C
- SLX9740-80C
- AP310i/e
- AP310i/e
- AP360i/e

Regimes and audit tests created in versions 8.1, 8.2, and 8.3 are retained following the upgrade.

ExtremeControl

- SIEM Notifications Functions Added to Access Control Tab
- Ping End-Systems Option Added to Tools Menu
- Message Strings Manager Feature Now in ExtremeControl
- Local Repositories Option Easier to Locate
- Manage Assessment Servers Upgrade Ability Now in ExtremeControl
- New Ciphers Added to ExtremeControl Engine Web Server Ports
- Filtering Function in Access Control Rule Table Enhanced
- Support for Extreme-Policy-ACL Added
- Rule Usage and Rule Hit Counts Tabs Added
- UDP & TCP Range Rules for Edit Traffic Description Supported
- Enhancements to DHCP Fingerprint Functionality
- Ability to Configure RADSec and TCP on Proxy RADIUS Servers
- Export of End-System Table Data Now Supports HTML Format
- New Option to Remove End-Systems via the End-Systems Tab
- Advanced Location-Based Registration and Web Access Configuration Available
- Ability to Create Helpdesk Provisioners in Guest & IoT Manager
- Preview with RADIUS Attributes Added
- Enhancement to Variables in RADIUS Attribute Configurations
- Enhanced Enforce Preview Functionality for ExtremeControl

SIEM Notifications Functions Added to Access Control Tab

A configuration menu button has been added to the **Access Control > Configurations > Notifications tab** that can be used to create default SIEM Notifications or change the default SIEM server.

Ping End-Systems Option Added to Tools Menu

The Ping End-Systems option has been added to Tools drop-down list on the **Access Control > End-Systems** table.

Message Strings Manager Feature Now in ExtremeControl

The Message Strings Manager feature has been added to ExtremeControl. It is accessible from the **Access Control > Configurations > Captive Portals > Website Configuration > Look & Feel** tab.

Local Repositories Option Easier to Locate

The Local Repositories option on the **Access Control > Configuration > AAA** tab is now located in the left-panel tree, making it more visible than where it was previously located.

Manage Assessment Servers Upgrade Ability Now in ExtremeControl

The Manage Assessment Servers check for updates and upgrade features on the **Access Control > Configuration > Profiles > Assessments** tab are now available in ExtremeControl.

New Ciphers Added to ExtremeControl Engine Web Server Ports

New ciphers have been added to ExtremeControl Engine web server ports, allowing browsers to be able to block CBC-based ciphers and still connect with engine web pages.

Filtering Function in Access Control Rule Table Enhanced

Column filtering in the Access Control Rule table now requires rule matches for all filters, not any single filter.

Support for Extreme-Policy-ACL Added

Support for ExtremeControl RADIUS attribute Extreme-Policy-ACL, which is used for dynamic ACLs on ExtremeControl devices, has been added.

Rule Usage and Rule Hit Counts Tabs Added

New **Rule Usage** and **Rule Hit Counts** tabs have been added to the **Policy > Devices/ Port Groups** tab. The **Rule Usage** table displays a raw usage report of the Content-Aware Processors (CAP) on devices. The **Rule Hit Counts** tab displays the number of packets that matched each ACE by the traffic description configured on the device you select on the **Policy > Devices / Port Groups > Devices** tab.

UDP & TCP Port Range Rules for Edit Traffic Description Supported

For ExtremeXOS devices running version 30.5.x or later, new functionality for range rules requires only a single rule on the device. Previous implementation broke port ranges into multiple rules to support them on the device. The new range rule support also allows a source or destination IP to be combined with UDP or TCP ranges. The "Optional Value" field is now enabled to allow an optional IP address when a UDP or TCP "Range" traffic classification type is selected. Devices that do not support this optional IP address combined with a UDP or TCP port range will show the rule as unsupported in the Enforce Preview window.

Enhancements to DHCP Fingerprint Functionality

Several enhancements to the **Detection and Profiling** table on the **Administration > Device Types** tab have been made to improve DHCP fingerprint functionality.

- Add or edit DHCP device type profiles directly to the table. If a system fingerprint is edited, a custom fingerprint is created that overrides the system fingerprint.

- Delete custom fingerprints directly from the table. If the custom fingerprint was overriding a system fingerprint, the system fingerprint becomes active once again.
- Import a custom DHCP fingerprint xml definitions file to Extreme Management Center.
- The Detection and Profiling table now supports additional operations, including the Group by this Field option, which groups the data in the table by the selected column heading, and the Show in Groups option, which displays the fingerprints grouped by the field you selected.

NOTE: Fingerprints are now applied to all ExtremeControl engines and are no longer engine-specific.

Ability to Configure RADSec and TCP on Proxy RADIUS Servers

You can now select TCP and RADSec setting options when configuring RADIUS Server authentication and accounting ports. RADSec adds TLS (Transport Layer Security) over TCP. For versions prior to Extreme Management Center version 8.5.7, TCP/ TLS settings are not supported and cannot be enforced to ExtremeControl engines.

Export of End-System Table Data Now Supports HTML Format

Export of ExtremeControl end-systems and end-system events from the respective tables now supports HTML format.

New Option to Remove End-Systems via the End-Systems Tab

A new Cleanup Data option has been added to the Tools menu in the End-Systems Table on the **Access Control > End-Systems tab**, which enables you to easily remove end-systems from the tables and charts on the End-Systems tab.

Advanced Location-Based Registration and Web Access Configuration Available

Advanced location-based registration and web access enables you to configure different access features for end users based on the location of a connecting end-system. Using the **Rules** tab, you can define a location-based access configuration, which specifies the access method and portal used by the end user to register or log in, and the access levels assigned to the end user following registration or login.

Ability to Create Helpdesk Provisioners in Guest & IoT Manager

You can now create a Helpdesk Provisioner user in Guest & IoT Manager with the ability to view and edit all the Guest user and Device records of the Onboarding Templates to which they are assigned. Helpdesk Provisioners can add records of assigned Onboarding Templates; edit, delete and extend user expiration; and perform resend password, resend details, renew password, and print operations on accessible records.

Preview with RADIUS Attributes Added

A new **Preview with RADIUS Attributes** option, which allows you to preview your policy with a given RADIUS Attribute configuration, has been added to **Access Control > Policy Mappings**.

Enhancement to Variables in RADIUS Attribute Configurations

Custom substitution variables can now contain other variables and are resolved up to three times in RADIUS Attribute configurations.

Enhanced Enforce Preview Functionality for ExtremeControl

The Enforce Preview functionality is enhanced for the ExtremeControl engine configuration, displaying additional details about the enforce.

Deprecated Features

In Extreme Management Center 8.5.5, NBI deviceData.portSpeed has been deprecated. Instead, use deviceData.portConfigSpeed when auto-negotiation is disablednd deviceData.portConfigSpeedList when auto-negotiation is enabled.

In Extreme Management Center version 8.5.7, the following legacy Java applications (Console, MIB Tools, NAC Manager, and Policy Manager) are disabled by default. To use the legacy Java applications in version 8.5.7, follow the instructions in the GTAC knowledgebase article.

Beginning in Extreme Management Center version 8.5, the Extreme Management Center server no longer supports native installation for the Windows operating system.

Known Issues and Vulnerabilities Addressed

Known Issues Addressed in 8.5.7

Extreme Management Center Issues Addressed
Enforcing a device will no longer disable port collection.
Adding and deleting devices occasionally caused the server to become unresponsive. This caused unintended behavior in Extreme Management Center and required a server reset to resolve the problem.

Known Issues Addressed in 8.5.6

Extreme Management Center Issues Addressed	ID
On the **Tasks** tab, the "emc_cli.send" was not waiting the maximum number of seconds defined by the timeout, and, as a result, the emc_cli.setSessionTimeout(60) was not changing the timeout to 60 seconds.	-----
SYSLOG alarm messages were not displaying in Events table when Netsight was configured as the owner of the Extreme Management Center server.	-----

ExtremeControl Issues Addressed	ID
The Guest and IoT Manager (GIM) Provisioner login was failing after upgrading to Extreme Management Center version 8.5.6.14.	-----

Known Issues Addressed in 8.5.5

Extreme Management Center Issues Addressed	ID
Fabric Manager was displaying only the Dynamic FA VLAN ISID Mappings for EXOS device running on versions prior to EXOS OS version 30.1 For EXOS OS versions above 30.1, Fabric Manager will display both Static and Dynamic FA VLAN ISID mapping. **NOTE:** There is limitation that when a particular VLAN is mapped to both static and dynamic NSI / ISID bindings. In such scenarios, Fabric Manager will display either Static or Dynamic, since the response from the EXOS device has only one FA VLAN ISID Mapping information	-----
Devices were improperly being added to maps other than those specified in the **Add Device Action** tab. The issue has been corrected. Now, selecting a Map from the **Network > Devices** tree and selecting "Add Device" adds the device to the map and to the map's parent site. From the **Network > Discovered** tab, specifying a map when adding the device will add the device to the specified map, as well as to the map specified in the site's **Add Action** tab.	-----

Known Issues Addressed in 8.5.4

Extreme Management Center Issues Addressed	ID
An Unable to Load Pages or Data state sometimes occurred if several buttons or tabs are selected before pages were allowed to fully or properly load.	-----
Slow SNMP response time, while a significant number of device status changes were processing, was generating “Out-of-Memory” errors.	02292280
The System Workflow task “Config VOSS Virtual IST” did not support the LACP SMLT System ID. Now, the LACP SMLT System ID field is optional in System Workflows.	-----
Selecting "Generate PDF" from the Devices > Interface History tab was resulting in a 404 File Not Found Page.	-----
The Wireless > Network > Topologies tab was displaying a number of topologies that did not belong to EWCs.	-----

ExtremeAnalytics Issues Addressed	ID
Port-based fingerprint match errors were sometimes appearing in the ExtremeAnalytics server log.	-----

Known Issues Addressed in 8.5.3

Extreme Management Center Issues Addressed	ID
Importing multiple scripts using the Tasks > Scripts > Import function occasionally changed the original indexing and lead to incorrect script matching or deletion.	01852604
Scheduled archives of more than 10 devices that use SCP or SFTP were randomly failing.	02187412
The Progress bar, as shown in the Results of an Execute CLI Commands execution, was incorrect; the completion percentage value was not shown. The Progress bar is completion percentage value is now correctly displayed.	02276741
Logging statements were included for debugging the Device Menus options. Since CLI scripts do not support Menus, debug statements have been modified to not append in the log files.	02249872
REST device calls use SSL if the WebView URL protocol is HTTPS. The URL must also include the correct TCP port (e.g. https://%IP:443).	02265917
Deploying Extreme Management Center version 8.5.0 was executing differently than if Extreme Management Center was upgraded from version 8.4.x to version 8.5.0. The issues have been addressed and now deployment of and upgrade to Extreme Management Center version 8.5.0 execute properly.	02242528
Extreme Management Center was treating EAPS domain names as case-sensitive while computing domain membership, which resulted in devices in the same domain with different domain names. Now, EAPS domain names are treated as case-insensitively while computing domain membership across devices.	01933011
Selecting the 'Refresh Port Status' button on the Devices > Summary > Ports tab for VSP / VOSS devices was not updating the devices' port status. In addition, alarms may not have been created based on port status for VOSS platforms.	02246282
In the Workflows > Scheduled Tasks table, the "Last Run" field was not displaying the last time a task executed after a first run or only run of the task.	02269563
Extreme Management Center was querying an MIB table for topology information for all VSP devices that is not supported by VSP9000 devices. Now, the correct MIB table is queried for topology information for VSP9000 series devices.	02263113
On the Archives tab, deleted devices were still displaying in the Archives table when the Stamp New Version option was used.	02247177
Clearing an alarm was resulting in the Alarm Name and Information fields appearing blank in the Alarm History table.	02251627
The wrong device was occasionally displaying in the DeviceView > Device Logs > Syslog and/or Traps table.	02221460
The connection for ICX backup workflows was closing before the workflow was fully executed and generating an improper 'Failed' message.	02168685
Selecting the Archive > Inventory Settings device option generated a "Could not load report" error message and the Inventory Settings panel would not display.	2264072

Extreme Management Center Issues Addressed	ID
for ExtremeXOS devices in Extreme Management Center, if the source IP address was not added, traps and syslogs appeared with the wrong IP address. Also, email notifications and events did not appear in alarms if the IP addresses did not match the managed IP address. Now, registering for traps and syslog sets the trap and syslog message source IP address for ExtremeXOS devices to the IP address that Extreme Management Center uses to manage the device.	02005429
Certain trap messages generated by the third-party CheckPoint for end-point devices were truncated after parsing the snmptrapd log file(s).	01943997
When adding a new device type fingerprint, the Vendor Name was not displaying if the “Is Partial” box was selected.	2258176
The FlexViews EXPR column on FlexViews reports was displaying ‘-‘ when values were non-numeric; for example, the Active Wireless Access Points and Wireless Access Points views.	2221529
After upgrading to Extreme Management Center version 8.5.0, log-on delays were occurring that were caused by third party devices with poor SNMP response times.	02247375
User defined Port Templates for a Site were unable to be deleted.	02251367
After upgrading to Extreme Management Center 8.5.2, FlexReport PDFs did not contain data.	02276233
A limit of 100 Access Points per map was being applied for wireless controllers and Extreme Campus Controller. This limit has been removed.	02267218
Deleting firmware images from Extreme Management Center for MLX, ICX, VDX and SLX devices was not deleting all images and directories.	02198267
Extreme Management Center did not use the slot:port format for ExtremeXOS devices that support it. A new emc_vars format has been introduced to the script engine i.e emc_vars[slot:port] that provides both slots and ports information.	01953506
Extreme Management Center was processing RADIUS accounting requests for devices with MAC address of zero. The issue has been corrected so if a MAC address of zero occurs, the RadiusAuthInfo is returned as null and doesn't proceed further.	01243712
Authorization Group capabilities and functions, specifically the options related to Device control, were still available for use after the devices were disabled. This issue has been corrected. Also, while the ability to run scripts using the right-click menu was not available, the ability to execute scripts against the disabled devices via the **Tasks** tab was still available. This issue is corrected by unselecting the NetSight > OneView>Access Scheduled Tasks, and Workflows/ Scripts > View > Edit, Workflows, Scripts, and Saved Tasks functions in Extreme Management Center.	1786436
The Reports tab auto-refresh was not working for custom reports created with the Reports Designer. The reports had to be manually refreshed to be updated.	02256858
In Extreme Management Center version 8.5.1, read-only users were improperly able to access the Configure window and make device changes.	2260874
For Extreme Management Center workflow scripts, imported scripts with unicode characters are no longer truncated.	1825871

Extreme Management Center Issues Addressed	ID
The firewall state was being incorrectly reported on recent Mac OSX versions. The agent will now detect firewall states of "0" as OFF and anything greater than "0" (1=ON, 2 = OFF + Essential Services) as ON. NOTE: Firewall states are retrieved from the globalstate variable in com.apple.alf.plist.	-----
The auto-refresh function was not working properly for custom reports created using the Report Designer.	02256858
The wrong device was occasionally displayed in the DeviceView > Device Logs > Syslog and Traps table.	02221460
Extreme Management Center was not accepting a password longer than eight characters if Extreme Management Center was installed or run as the user "netsight".	-----
Read-only users incorrectly had access to the 'configure' function, which allowed them the ability to enforce changes to the devices.	2260874

ExtremeAnalytics Issues Addressed	ID
ExtremeAnalytics Flow Grid filters were timing out when attempting to display filtered flow results.	-----
On the Analytics tab, a "Could not load report" error message was improperly being generated when IP subnets were added to end-point locations.	02211025 1955045
Importing end-point locations in ExtremeAnalytics was improperly generating error messages.	02260320
When a VSP device, for which collectors are configured to forward sflow to a third-party server, was later added as a flow source to the ExtremeAnalyticsengine, the sflow configuration was improperly deleted when the device was removed from the ExtremeAnalytics engine.	1926465
The Analytics License Violation message would improperly display when either no engines were configured or a non-Analytics view was being accessed.	1906404

ExtremeControl Issues Addressed	ID
It was not possible to enter a Virtual Router Name when adding a new switch with NBI.	02263955
Policy enforce failed and an "Unexpected error" message displayed when using an IP Socket Automated Service with a Network Resource that contained a masked IP address.	02229897
Admin users, using the Admin Role in the Captive Portal administrative setting and when the “Limit the Sponsor’s View to Own Users” option was enabled, were able to view pending sponsored users who used different email addresses than the Admin Users through sponsor page.	01883106
The maximum limits set for backup scripts for ExtremeControl and Workflow folders were not being considered.	01887642
No error message was generated when configuring a switch with NBI with same ExtremeControl gateway used as both the primary and secondary gateway.	02262810
On the **Control > Policy** tab, changes made to a Class of Service applied to a Global Service Rule were not being saved when the domain was saved.	01989463

ExtremeControl Issues Addressed	ID
On the **Control > Policy** tab, attempts to delete a Class of Service applied to a Global Service Rule using the Delete & Clear Actions button were not deleting the CoS when the domain was saved.	01996239
The Ports table (or Port Tree) in the DeviceView window was not populating with data for some VSP-4900 devices.	02219711
After adding a device to a policy domain in ExtremeControl, the data was not displaying immediately in the Policy Domain column of the Devices table.	1992716
An error was caused when the read operation was attempted on the 802.1x MIB "dot1xAuthTxPeriod," which is deprecated and obsolete. The Get and Set Operation on Authentication txPeriod has been removed from Port Authentication in Policy Manager.	02155440
If an end-system record was deleted from the End-System group in Extreme Management Center, it was removed but remained as a visible entry in Guest and IoT Manager (GIM). Because it is recommended that GIM entries are managed in GIM, a warning message is displayed and the deletion of the GIM entry is prevented in ExtremeControl.	02007116
The mobile captive portal improperly displayed the selector and provider field with only a single entry listed. Now, the mobile captive portal displays the providers list only if the number of providers is greater than one.	01909449
The option to print more than one user record at once was not available in the Guest and IoT Manager (GIM). Now, the option to print multiple user records at once is available.	02214309
When adding or editing a User Group on the **Control > LDAP User Group Entry Editor** window, commas are generally used to separate the attribute/value pairs in an entry to ensure they are evaluated separately. However, adding a comma was sometimes impacting how wildcards (*) are handled. To force the entry to be treated as a single value, do not use a comma before a second '='. For Example: `ou=NacDev, DC=com` is evaluated as two separate entries; `ou=ou=NacDev, DC=com` is evaluated as a single entry.	01772140
NBI was allowing the ability to access and modify control switches and add secondary Gateway switches, but was not allowing the ability to unset secondary Gateway switches.	02262704
Device services, including SNMP services, were being configured on multiple interfaces for the ExtremeControlengine. However, SNMP is only supported on one interface, and users were not informed appropriately. A warning has been added to alert that, when configuring device services on more than one interface, SNMP will only work over one interface.	-----
The end-systems table was displaying incorrect status. The addition of a live update feature has corrected this issue.	215582
The ExtremeControl captive portal was not working if both IPv4 and IPv6 addresses are configured on the registration and remediation interface. This issue has been corrected.	01911557
An individual certificate could not be deleted if the Trusted Authority certificate list contained duplicate entries with the same certname/ SHA-type as the certificate. All certificates with the same certname/ SHA-type had to be deleted and then the desired certificate had to be re-added.	01952004
ExtremeControl was using pooled LDAP connections, which are left open indefinitely and may be eventually torn down by the LDAP server, resulting in the entire pool being "dead" on the LDAP server side. Now, the pooled connection timeout is set to 5 minutes (300000 milliseconds).	01957077

ExtremeControl Issues Addressed	ID
By default, if a wireless controller sent Siemens-BSS-MAC attribute, ExtremeControl overwrote the called-station-id with the value to be used to identify the location of end-system. ExtremControl now supports an engine property to disable the default behavior of Siemens-BSS-MAC RADIUS attribute sent by Extreme wireless controllers that overwrites the Called-Station-Id attribute value. The new property is REPLACE_CALLED_STATION_ID_WITH_SIEMENS_BSS_MAC and setting this to false disables the default behavior.	-----

Known Issues Addressed in 8.5.1

Extreme Management Center Issues Addressed	ID
The **Add Device to Access Control Engine Group** option on the **Site > Actions** panel and the **Add/ Configure Device > Actions** panel was not completing for ExtremeControl engines during ZTP+ process.	2183833
Moving maps within the left-panel navigation tree on the **Sites** tab did not always move the devices properly and, sometimes, associated submaps did not move with the maps.	2172986
A tooltip message was improperly displaying for the Neighboring Capabilities field on the DeviceView > Ports and Port Tree views. The message no longer displays.	02211816
The ICX-MLX Backup Configuration System Workflow was assigning different directories for a single archive configuration, which was causing an unusable backup organization for the archive.	2184831
Selecting **Stamp New Version** on the **Network** > **Archives** tab did not complete successfully if the user's name contained an "at sign" character (@).	01807646
XML fields with greater than 2048 characters were causing the LDAP Configuration to stop responding.	1222245
Attempting to create a manual link for devices in a map was unsuccessful.	2241955
The Archived Devices ring chart on the Impact Analysis dashboard could not be configured to display the number of archives created for devices over a duration of more or less than 30 days. Users can now configure the duration from which the total number of device archives is calculated and displayed on the Impact Analysis dashboard via the **Administration** > **Options** > **Impact Analysis** tab. Additionally, when an archive was not created successfully, alarms did not clearly explain the issue. Events that indicate a device archive failure are now prepended with Failed to more clearly indicate the issue.	1940347
Administrator-selected options were sometimes being ignored when the list of Archived devices was updated.	-----
An improperly implemented base collector class support was creating a memory leak in the Trap Receiver.	-----
Enforce/Verify failures were occasionally occurring after changing the VLAN or NSI mapping of Policy Roles or Rules and enforcing to a Wireless Controller.	**-----**

ExtremeAnalytics Issues Addressed	ID
IPFIX parsing was potentially ignoring flow set data, resulting in some flow sets not being processed. Now, flows in every flow set in an IPFIX packet are processed.	-----
The appid process was crashing when it encountered certain ERSPAN packets.	02192534

ExtremeControl Issues Addressed	ID
On the Access Control tab, column settings were not persisting in the End Systems table when navigating away from the page and back again, and when the Refresh button was selected.	2178542
When adding a secondary device modeled with non-default SNMPv3 credentials to the ExtremeControl engine, the device would lose or alter the `/etc/snmpd.conf` file and fail to be modeled thereafter. This is no longer happening.	01880374
The AUP for Guest Registration was improperly preventing guests from being able to register. The issue has been addressed and is no longer interfering with guest registration.	01889261
On the Access Control tab, end-systems were displaying in the wrong ExtremeControl engine End-System table. Now, end-systems display in the appropriate end-system table	02190793
Policy enforcement failure with "ArrayIndexOutOfBounds" exceptions in the server.log were occasionally occuring when enforcing to an X435 on which ExtremeXOS version 30.5 or later was installed.	-----

Known Issues Addressed in 8.5.0

Extreme Management Center Issues Addressed	ID
The `watchdog.log` and `appmonitor.log` files could not be configured to remove the oldest files. Now the cleanLogs script is included with Extreme Management Center so that only the latest 10 files are saved.	01981039
Devices with a **Poll Type** of **Maintenance** no longer periodically issue SNMP requests in order to check for component changes.	-----
SNMP timeouts were occurring when Extreme Management Center was communicating with third-party devices.	-----
Extreme Management Centeroptions for displaying MAC addresses with an OUI prefix were not available.	-----
Discover was not being allowed for valid Sites based on the "Add Device" capability. The capability for "Sites Read/Write Access" is not necessary for Site Discover, but it is necessary for adding or editing sites.	-----
QoS and EAPs fields were required fields to create VLAN scripts for ExtremeXOS in Extreme Management Center. Now, the Create_VLAN scripts for ExtremeXOS have been updated to treat QoS and EAPs as optional fields.	1813187
The default TransferProtocol setting for the Cisco Vendor Profile database was previously set incorrectly.	01985239
The Archive Restore function was not displaying a warning if the archive was from a different model type.	-----
The Scheduled Task Name, Description, and Subject values were reverting back to default values after being changed during editing.	1782136

Extreme Management Center Issues Addressed	ID
NMS-BASE license now allows you to enable, disable and add a port to a group via the right-click Port drop-down list in the Devices > Device view.	01837802
The Interface History PDF was unclear because it was missing titles on three area charts and multi-line charts were using the same colors for each line.	01709514
The Generate Show Support feature was not showing the current status when navigating away and back.	-----
The MLAG Summary report was displaying information from more than one MLAG pair when devices had identical MLAG configurations.	1946635
Attempting to set an ExtremeXOS device's restart time to a date more than a month ahead would fail, indicating that the proposed reboot time was in the past.	1784366
Extreme Management Center was indicating that devices had exceeded device memory usage on ExtremeXOS and was generating alarms, although the devices appeared to have plenty of memory available.	1958668
The Mgmt [4095] VLAN for ExtremeXOS devices was incorrectly able to be added to the Tagged list for a port in Extreme Management Center. Now, the Mgmt [4095] VLAN is no longer selectable in the Tagged list for a port.	-----
Archives were being sorted incorrectly because they were being sorted alphabetically, which doesn't respect numerical date formats properly.	01946495
The temperature graph for certain VOSS devices was not displaying on the Device View > Historical Performance tab.	01994534
The maximum SNMP Compass search time has been expanded from 2 minutes to 10 minutes to support larger deployments.	-----
Workflow paths with a conditional expression were not working for device specific variables, causing Workflows to fail.	-----
Firmware upgrades were not allowed for devices set to Maintenance / Remove from Service.	1944261
netSNMP log messages were being merged with the device trap message in the Extreme Management Center > Event view.	1942303
Archive menu options were hidden when permission for firmware upgrade was removed from user permissions.	01940887
ExtremeXOS 8 Stacks were sometimes timing out before completing archive backup.	01973463
The ICX-7450 stacks with 2 units were mapping as one single system in Extreme Management Center.	01877301
In the Devices table, the Firmware column was displaying the Boot ROM version for Aruba 2930F.	1968881
Workflows triggered by an alarm/event were only working for devices that existed in the Extreme Management Center database, but not for missing or unknown devices.	-----
The Manage SSH Configuration > Create/Edit/Delete functionality was not working properly on the **Administration > Users** tab.	01982920 01992095 01984146
Logical ports on third-party devices were counting against the license limit.	1974488
The MLAG Summary report, generated from the **Network** > **Devices** tab, was displaying unnecessary MLAG information.	1946635

Extreme Management Center Issues Addressed	ID
End-system groups that were deleted or renamed in Extreme Management Center were being deleted from GIM Onboarding Templates. Now, when end system groups are deleted in Extreme Management Center, a warning message is shown in GIM when the Onboarding Template is opened for editing.	01934063
The **Diagnostics > Server> Server License > Add License** window did not include IA-GIM.	01991124
The **Devices > Device > Ports** view was not displaying Cisco Fabric Extender ports correctly.	01981119
A message was displaying that a VLAN name could not be modified when it was assigned to a port. That message no longer displays because names of VLANs that are assigned to ports can be changed.	1155260 1718693
The Syslog and Trap "Ignore IP List" filter was not being applied to new trap or syslog messages.	-----
The Archive Compare File Swap feature was not swapping the displayed files.	1404408
Deleting an Extreme wireless controller that shares a WLAN or VNS with another Extreme wireless controller was displaying a ConstraintViolationException error in the System log.	01964545

ExtremeAnalytics Issues Addressed	ID
In ExtremeAnalytics, the Application Server compound collector was not respecting the limit of top 100 apps and top 100 servers per app.	01851795
The ExtremeAnalytics > Engine License Rates chart was incorrectly displaying significantly less unique end-system counts than were observed.	01992118 02161641

ExtremeControl Issues Addressed	ID
In the **Control> Dashboard> Overview** Report page, Authentication Type wasn't launching the filtered end-systems table correctly, and in the **Control> Dashboard> Health** Report pane, Risk Level wasn't launching the filtered end-systems table correctly.	-----
End systems were displaying as "MAC" authenticated on the **Control > End System** tab when an X session was active on the switch.	01801463 01827905 01932037
The value of sysObjectID was being incorrectly set for ExtremeControl engines.	01983768
Resetting End-System diagnostics by MAC or IP address was not completely disabling diagnostics.	01522146 01982359
The AAA Rule Configuration> Supported RADIUS Type incorrectly included PAP and EAP-TTLS with tunneled PAP as options for NTLM authentication. Those options have been removed to clarify this field.	-----
End-System table live updates were not being filtered by zone when viewed with view access limited to specified zones.	01955995
Sorting some **Access Control > Policy Mapping** table columns was throwing exceptions if any values were empty.	01956869

ExtremeControl Issues Addressed	ID
In ExtremeControl, the live end-system count was increasing in the End-system table when end-systems were updating and not newly added. Now, only newly added end-systems are counted, and updated end-systems are not counted again.	-----
The Access Control evaluate tool was not launching from the Configurations table.	-----
The **Access Control > End Systems > End System** table was not displaying port alias information.	01981206
ExtremeControl engine was incorrectly running the snmpconfig script to change SNMP.	01983768
The ExtremeControl > Guest Web Access > Customize Fields > Edit window was lagging in the "Loading" state.	01916225
The "Start Packet Capture" option is no longer available in any ExtremeControl end-system tables.	-----

ExtremeConnect Issues Addressed	ID
Using ExtremeConnect with a large number of end-systems connected (for example, 50,000) was causing significant performance issues for the Extreme server.	01937179

Vulnerabilities Addressed

This section presents the vulnerabilities addressed in Extreme Management Center versions 8.5.0 - 8.5.7.

Addressed in 8.5.7

Extreme Management Center images:

CVE-2021-3800,CVE-2021-3612,CVE-2021-3653,CVE-2021-3656,CVE-2021-34693,CVE-2021-38160,CVE-2021-3679,CVE-2021-3732,CVE-2021-22543,CVE-2021-37576,CVE-2021-38204,CVE-2021-38205,CVE-2021-43527,CVE-2021-3711,CVE-2021-3712,CVE-2020-16592,CVE-2021-3487,CVE-2020-36311,CVE-2021-3612,CVE-2021-4104,CVE-2021-21703,CVE-2017-6363,CVE-2021-38115,CVE-2021-40145,CVE-2021-3770,CVE-2021-3778,CVE-2021-3796,CVE-2021-40330,CVE-2017-17087,CVE-2019-20807,CVE-2021-3872,CVE-2021-3903,CVE-2021-3927,CVE-2021-3928,CVE-2020-21913,CVE-2021-3564,CVE-2021-3573,CVE-2020-3702,CVE-2021-38198,CVE-2021-40490,CVE-2019-19449,CVE-2020-36322,CVE-2020-36385,CVE-2021-3655,CVE-2021-3743,CVE-2021-3753,CVE-2021-3759,CVE-2021-38199,CVE-2021-3744,CVE-2021-3764,CVE-2021-37159,CVE-2021-32027,CVE-2021-32028,CVE-2021-32029,CVE-2021-25219,CVE-2021-28831,CVE-2021-42374,CVE-2021-42378,CVE-2021-42379,CVE-2021-42380,CVE-2021-42381,CVE-2021-42382,CVE-2021-42384,CVE-2021-42385,CVE-2021-42386,CVE-2021-23214,CVE-2021-23222,CVE-2021-3709,CVE-2021-3710,CVE-2021-38185,CVE-2021-33560,CVE-2021-40528,CVE-2021-3677,CVE-2021-40153,CVE-2021-22945,CVE-2021-22946,CVE-2021-

22947,CVE-2021-3428,CVE-2021-3739,CVE-2021-34556,CVE-2021-35477,CVE-2020-27781,CVE-2021-3509,CVE-2021-3524,CVE-2021-3531,CVE-2021-3712,CVE-2021-3733,CVE-2021-3737,CVE-2020-15778,CVE-2021-41072,CVE-2021-42008, CVE-2021-35577, CVE-2021-35646, CVE-2021-35638, CVE-2021-35597, CVE-2021-35602,CVE-2021-35596, CVE-2021-35631, CVE-2021-35642, CVE-2021-35612, CVE-2021-35626,CVE-2021-35625, CVE-2021-2478, CVE-2021-35613, CVE-2021-35591, CVE-2021-35647,CVE-2021-35608, CVE-2021-35644, CVE-2021-35641, CVE-2021-35632, CVE-2021-35640,CVE-2021-35637, CVE-2021-35645, CVE-2021-35648, CVE-2021-35546, CVE-2021-35639,CVE-2021-35627, CVE-2021-2481, CVE-2021-35628, CVE-2021-35623, CVE-2021-2479,CVE-2021-35635, CVE-2021-35633, CVE-2021-35622, CVE-2021-35610, CVE-2021-35604,CVE-2021-35607, CVE-2021-35636, CVE-2021-35575, CVE-2021-35584, CVE-2021-35624,CVE-2021-35643, CVE-2021-35630, CVE-2021-35634, CVE-2021-42252, CVE-2021-3587

ExtremeControl images

CVE-2021-3800,CVE-2021-3612,CVE-2021-3653,CVE-2021-3656,CVE-2021-34693,CVE-2021-38160,CVE-2021-3679,CVE-2021-3732,CVE-2021-22543,CVE-2021-37576,CVE-2021-38204,CVE-2021-38205,CVE-2021-43527,CVE-2021-3711,CVE-2021-3712,,CVE-2020-16592,CVE-2021-3487,CVE-2020-36311,CVE-2021-3612,CVE-2021-3653,CVE-2021-3656,CVE-2021-4104,CVE-2021-21703,CVE-2017-6363,CVE-2021-38115,CVE-2021-40145,CVE-2021-3770,CVE-2021-3778,CVE-2021-3796,CVE-2021-40330,CVE-2017-17087,CVE-2019-20807,CVE-2021-3872,CVE-2021-3903,CVE-2021-3927,CVE-2021-3928,CVE-2020-21913,CVE-2021-3564,CVE-2021-3573,CVE-2020-3702,CVE-2021-38198,CVE-2021-40490,CVE-2019-19449,CVE-2020-36322,CVE-2020-36385,CVE-2021-3655,CVE-2021-3743,CVE-2021-3753,CVE-2021-3759,CVE-2021-38199,CVE-2021-3744,CVE-2021-3764,CVE-2021-37159,CVE-2021-32027,CVE-2021-32028,CVE-2021-32029,CVE-2021-25219,CVE-2021-28831,CVE-2021-42374,CVE-2021-42378,CVE-2021-42379,CVE-2021-42380,CVE-2021-42381,CVE-2021-42382,CVE-2021-42384,CVE-2021-42385,CVE-2021-42386,CVE-2021-23214,CVE-2021-23222,CVE-2021-3709,CVE-2021-3710,CVE-2021-38185,CVE-2021-33560,CVE-2021-40528,,CVE-2021-3449,CVE-2021-3677,CVE-2021-40153,CVE-2021-41072,CVE-2021-22945,CVE-2021-22946,CVE-2021-22947,CVE-2021-38198,CVE-2021-40490,CVE-2019-19449,CVE-2021-3428,CVE-2021-3739,CVE-2021-3743,CVE-2021-3753 ,CVE-2021-34556,CVE-2021-35477,CVE-2021-3744,CVE-2021-37159,CVE-2020-27781,CVE-2021-3509,CVE-2021-3524,CVE-2021-3531,CVE-2021-20288,CVE-2021-3712,CVE-2021-3733,CVE-2021-3737, CVE-2021-33624, CVE-2020-15778, CVE-2019-7303, CVE-2020-11933, CVE-2020-11934, CVE-2020-27352, CVE-2021-42008, CVE-2021-42252, CVE-2021-3587

ExtremeAnalytics images

CVE-2021-3800,CVE-2021-3612,CVE-2021-3653,CVE-2021-3656,CVE-2021-34693,CVE-2021-38160,CVE-2021-3679,CVE-2021-3732,CVE-2021-22543,CVE-2021-37576,CVE-2021-38204,CVE-2021-38205,CVE-2021-43527,CVE-2021-3711,CVE-2021-3712,CVE-2020-16592,CVE-2021-3487,CVE-2020-36311,CVE-2021-3612,CVE-2021-4104,CVE-2019-7303,CVE-2020-11933,CVE-2020-11934,CVE-2017-6363,CVE-2021-38115,CVE-2021-40145,CVE-2021-3770,CVE-2021-3778,CVE-2021-3796,CVE-2021-40330,CVE-2017-17087,CVE-2019-20807,CVE-2021-3872,CVE-2021-3903,CVE-2021-3927,CVE-2021-3928,CVE-2020-21913,CVE-2021-3564,CVE-2021-3573,CVE-2020-3702,CVE-2021-38198,CVE-2021-40490,CVE-2019-19449,CVE-2020-36322,CVE-2020-36385,CVE-2021-3655,CVE-2021-3743,CVE-2021-3753,CVE-2021-3759,CVE-2021-38199,CVE-2021-3744,CVE-2021-3764,CVE-2021-37159,CVE-2021-25219,CVE-2021-28831,CVE-2021-42374,CVE-2021-42378,CVE-2021-42379,CVE-2021-42380,CVE-2021-42381,CVE-2021-42382,CVE-2021-42384,CVE-2021-42385,CVE-2021-42386,CVE-2021-3709,CVE-2021-3710,CVE-2021-33560,CVE-2021-40528,CVE-2021-40153,CVE-2021-41072,CVE-2021-22945,CVE-2021-22946,CVE-2021-22947,CVE-2021-3428,CVE-2021-3739,CVE-2021-34556,CVE-2021-35477,CVE-2020-27781,CVE-2021-3509,CVE-2021-3524,CVE-2021-3531,CVE-2021-20288,CVE-2021-3712,CVE-2021-3733,CVE-2021-3737,CVE-2021-33624,CVE-2020-15788,CVE-2020-27352,CVE-2021-38185,CVE-2021-42008,CVE-2021-42252, CVE-2021-3587

Fabric Manager images

CVE-2019-2894,CVE-2019-2933,CVE-2019-2945,CVE-2019-2949,CVE-2019-2958,CVE-2019-2962,CVE-2019-2964,CVE-2019-2973,CVE-2019-2975,CVE-2019-2977,CVE-2019-2978,CVE-2019-2981,CVE-2019-2983,CVE-2019-2987,CVE-2019-2988,CVE-2019-2989,CVE-2019-2992,CVE-2019-2996,CVE-2019-2999,CVE-2019-11068,CVE-2021-3517,CVE-2021-3522,CVE-2021-35550,CVE-2021-35556,CVE-2021-35559,CVE-2021-35560,CVE-2021-35561,CVE-2021-35564,CVE-2021-35565,CVE-2021-35567,CVE-2021-35578,CVE-2021-35586,CVE-2021-35588,CVE-2021-35603,,CVE-2020-25694,CVE-2020-25695,CVE-2020-25696,CVE-2020-12695,CVE-2021-0326,CVE-2021-3612,CVE-2021-3653,CVE-2021-3656,CVE-2021-34693,CVE-2021-38160,CVE-2021-3679,CVE-2021-3732,CVE-2021-22543,CVE-2021-37576,CVE-2021-38204,CVE-2021-38205,CVE-2021-43527,CVE-2021-3711,CVE-2021-3712,CVE-2020-16592,CVE-2021-3487,CVE-2020-36311,CVE-2021-4104,CVE-2019-13117,CVE-2019-13118,CVE-2019-16168,CVE-2020-2583,CVE-2020-2585,CVE-2020-2590,CVE-2020-2593,CVE-2020-2601,CVE-2020-2604,CVE-2020-2654,CVE-2020-2655,CVE-2020-2659,CVE-2019-18197,CVE-2020-2754,CVE-2020-2755,CVE-2020-2756,CVE-2020-2757,CVE-2020-2764,CVE-2020-2767,CVE-2020-2773,CVE-2020-2778,CVE-2020-2781,CVE-2020-2800,CVE-2020-2803,CVE-2020-2805,CVE-2020-2816,CVE-2020-2830,CVE-2020-14556,CVE-2020-14562,CVE-2020-14573,CVE-2020-

14577,CVE-2020-14578,CVE-2020-14579,CVE-2020-14581,CVE-2020-14583,CVE-2020-14593,CVE-2020-14621,CVE-2020-14664,CVE-2020-14779,CVE-2020-14781,CVE-2020-14782,CVE-2020-14792,CVE-2020-14796,CVE-2020-14797,CVE-2020-14798,CVE-2020-14803,CVE-2020-14803,CVE-2021-2161,CVE-2021-2163,CVE-2021-27803,CVE-2017-6363,CVE-2021-38115,CVE-2021-40145,CVE-2021-3770,CVE-2021-3778,CVE-2021-3796,CVE-2021-40330,CVE-2017-17087,CVE-2019-20807,CVE-2021-3872,CVE-2021-3903,CVE-2021-3927,CVE-2021-3928,CVE-2020-21913,CVE-2021-3564,CVE-2021-3573,CVE-2020-3702,CVE-2021-38198,CVE-2021-40490,CVE-2019-19449,CVE-2020-36322,CVE-2020-36385,CVE-2021-3655,CVE-2021-3743,CVE-2021-3753,CVE-2021-3759,CVE-2021-38199,CVE-2021-3744,CVE-2021-3764,CVE-2021-37159,CVE-2021-32027,CVE-2021-32028,CVE-2021-32029,CVE-2021-25219,CVE-2021-28831,CVE-2021-42374,CVE-2021-42378,CVE-2021-42379,CVE-2021-42380,CVE-2021-42381,CVE-2021-42382,CVE-2021-42384,CVE-2021-42385,CVE-2021-42386,CVE-2021-2478,CVE-2021-2479,CVE-2021-2481,CVE-2021-35546,CVE-2021-35575,CVE-2021-35577,CVE-2021-35584,CVE-2021-35591,CVE-2021-35596,CVE-2021-35597,CVE-2021-35602,CVE-2021-35604,CVE-2021-35607,CVE-2021-35608,CVE-2021-35610,CVE-2021-35612,CVE-2021-35613,CVE-2021-35622,CVE-2021-35623,CVE-2021-35624,CVE-2021-35625,CVE-2021-35626,CVE-2021-35627,CVE-2021-35628,CVE-2021-35630,CVE-2021-35631,CVE-2021-35632,CVE-2021-35633,CVE-2021-35634,CVE-2021-35635,CVE-2021-35636,CVE-2021-35637,CVE-2021-35638,CVE-2021-35639,CVE-2021-35640,CVE-2021-35641,CVE-2021-35642,CVE-2021-35643,CVE-2021-35644,CVE-2021-35645,CVE-2021-35646,CVE-2021-35647,CVE-2021-35648,CVE-2021-23214,CVE-2021-23222,CVE-2021-3709,CVE-2021-3710,CVE-2021-38185,CVE-2021-33560,CVE-2021-40528,CVE-2021-3449,CVE-2021-3677,CVE-2021-40153,CVE-2021-41072,CVE-2021-22945,CVE-2021-22946,CVE-2021-22947,CVE-2020-CVE-2021-3732,CVE-2021-38198,CVE-2021-38205,CVE-2019-19449,CVE-2021-3428,CVE-2021-3739,CVE-2021-34556,CVE-2021-35477,CVE-2020-27781,CVE-2021-3509,CVE-2021-3524,CVE-2021-3531,CVE-2021-20288,CVE-2021-3712,CVE-2021-3733,CVE-2021-3737, CVE-2021-3800, CVE-2020-15778 CVE-2021-42008, CVE-2021-42252, CVE-2021-3587

Addressed in the 8.5.0 - 8.5.6 images

Extreme Management Center, ExtremeControl, and ExtremeAnalytics images

- CVE-2018-0500, CVE-2018-8740, CVE-2019-19603, CVE-2019-19645, CVE-2020-11655, CVE-2020-13434, CVE-2020-13435, CVE-2020-13630, CVE-2020-13631, CVE-2020-13632, CVE-2020-13790, CVE-2020-0543, CVE-2020-0548, CVE-2020-0549, CVE-2019-1547, CVE-2019-1549, CVE-2019-1551, CVE-2019-1563, CVE-2017-11109, CVE-2017-5953, CVE-2017-6349, CVE-2017-6350, CVE-2018-20786, CVE-2019-20079, CVE-2019-12387, CVE-2019-12855, CVE-2019-

9512, CVE-2019-9514, CVE-2019-9515, CVE-2020-10108, CVE-2020-10109, CVE-2020-10531, CVE-2020-1700, CVE-2019-13734, CVE-2019-13750, CVE-2019-13751, CVE-2019-13752, CVE-2019-13753, CVE-2019-19880, CVE-2019-19923, CVE-2019-19924, CVE-2019-19925, CVE-2019-19926, CVE-2019-19959, CVE-2019-20218, CVE-2020-9327, CVE-2020-8130, CVE-2019-19221, CVE-2020-9308, CVE-2016-9840, CVE-2016-9841, CVE-2016-9842, CVE-2016-9843, CVE-2020-8597, CVE-2019-19956, CVE-2020-7595, CVE-2018-16888, CVE-2019-20386, CVE-2019-3843, CVE-2019-3844, CVE-2020-1712, CVE-2019-19906, CVE-2017-16808, CVE-2018-10103, CVE-2018-10105, CVE-2018-14461, CVE-2018-14462, CVE-2018-14463, CVE-2018-14464, CVE-2018-14465, CVE-2018-14466, CVE-2018-14467, CVE-2018-14468, CVE-2018-14469, CVE-2018-14470, CVE-2018-14879, CVE-2018-14880, CVE-2018-14881, CVE-2018-14882, CVE-2018-16227, CVE-2018-16228, CVE-2018-16229, CVE-2018-16230, CVE-2018-16300, CVE-2018-16451, CVE-2018-16452, CVE-2018-19519, CVE-2019-1010220, CVE-2019-15166, CVE-2019-15167, CVE-2019-5188, CVE-2019-15795, CVE-2019-15796, CVE-2019-20367, CVE-2019-13627, CVE-2019-15165, CVE-2019-15845, CVE-2019-16201, CVE-2019-16254, CVE-2019-16255,CVE-2019-14866, CVE-2019-12290, CVE-2019-18224, CVE-2019-13117, CVE-2019-13118, CVE-2019-18197, CVE-2019-6111, CVE-2019-10222, CVE-2019-13012, CVE-2019-12450, CVE-2019-8457, CVE-2019-12735, CVE-2019-19377, CVE-2019-19769, CVE-2020-11494, CVE-2020-11565, CVE-2020-11608, CVE-2020-11609, CVE-2020-11668, CVE-2020-12657, CVE-2020-12826, CVE-2020-8616, CVE-2020-8617, CVE-2020-11669, CVE-2020-12762, CVE-2020-3810, CVE-2019-20795, CVE-2020-12243, CVE-2018-5383, CVE-2020-2759, CVE-2020-2760, CVE-2020-2762, CVE-2020-2763, CVE-2020-2765, CVE-2020-2780, CVE-2020-2804, CVE-2020-2812, CVE-2020-2892, CVE-2020-2893, CVE-2020-2895, CVE-2020-2896, CVE-2020-2897, CVE-2020-2898, CVE-2020-2901, CVE-2020-2903, CVE-2020-2904, CVE-2020-2921, CVE-2020-2922, CVE-2020-2923, CVE-2020-2924, CVE-2020-2925, CVE-2020-2926, CVE-2020-2928, CVE-2020-2930, CVE-2019-16234, CVE-2019-19768, CVE-2020-10942, CVE-2020-11884, CVE-2020-8648, CVE-2020-9383, CVE-2019-2228, CVE-2020-3898, CVE-2019-18348, CVE-2020-8492, CVE-2020-11008, CVE-2020-5260, CVE-2020-8428, CVE-2020-8834, CVE-2020-8992, CVE-2018-14553, CVE-2019-11038, CVE-2020-8831, CVE-2020-8833, CVE-2020-8835, CVE-2018-14498, CVE-2018-19664, CVE-2018-20330, CVE-2019-2201, CVE-2018-11574, CVE-2019-19046, CVE-2020-8428, CVE-2020-15709, CVE-2020-12400, CVE-2020-12401, CVE-2020-6829, CVE-2020-15704, CVE-2020-11936, CVE-2020-15701, CVE-2020-15702, CVE-2020-14539, CVE-2020-14540, CVE-2020-14547, CVE-2020-14550, CVE-2020-14553, CVE-2020-14559, CVE-2020-14568, CVE-2020-14575, CVE-2020-14576, CVE-2020-14586, CVE-2020-14591, CVE-2020-14597, CVE-2020-14619, CVE-2020-14620, CVE-2020-14623, CVE-2020-14624, CVE-2020-14631, CVE-2020-

14632, CVE-2020-14633, CVE-2020-14634, CVE-2020-14641, CVE-2020-14643, CVE-2020-14651, CVE-2020-14654, CVE-2020-14656, CVE-2020-14663, CVE-2020-14678, CVE-2020-14680, CVE-2020-14697, CVE-2020-14702, CVE-2019-17514, CVE-2019-20907, CVE-2019-9674, CVE-2020-14422, CVE-2017-12133, CVE-2017-18269, CVE-2018-11236, CVE-2018-11237, CVE-2018-19591, CVE-2018-6485, CVE-2019-19126, CVE-2019-9169, CVE-2020-10029, CVE-2020-1751, CVE-2020-1752, USN-4377-1, CVE-2020-14309, CVE-2020-15707, CVE-2020-10713, CVE-2020-15706, CVE-2020-14311, CVE-2020-14310, CVE-2020-15705, CVE-2020-14308,CVE-2020-10711, CVE-2020-10751, CVE-2020-12768, CVE-2020-12770, CVE-2020-13143, CVE-2020-5963, CVE-2020-5967, CVE-2020-5973, CVE-2020-8169, CVE-2020-8177, CVE-2020-12049, CVE-2019-17023, CVE-2020-12399, CVE-2019-7303, CVE-2019-14855, CVE-2018-7738, CVE-2019-1547, CVE-2019-1551, CVE-2019-1563, CVE-2020-1968, CVE-2020-14386, CVE-2020-14344, CVE-2020-14363, CVE-2018-20669, CVE-2019-19947, CVE-2019-20810, CVE-2020-10732, CVE-2020-10766, CVE-2020-10767, CVE-2020-10768, CVE-2020-10781, CVE-2020-12655, CVE-2020-12656, CVE-2020-12771, CVE-2020-13974, CVE-2020-15393, CVE-2020-2439, CVE-2019-20810, CVE-2020-10757, CVE-2020-10766, CVE-2020-10767, CVE-2020-10768, CVE-2020-10781, CVE-2020-12655, CVE-2020-12656, CVE-2020-12771, CVE-2020-13974, CVE-2020-14356, CVE-2020-15393, CVE-2020-24394, CVE-2019-20810, CVE-2020-10757, CVE-2020-10766, CVE-2020-10767, CVE-2020-10768, CVE-2020-10781, CVE-2020-12655, CVE-2020-12656, CVE-2020-12771, CVE-2020-13974, CVE-2020-14356, CVE-2020-15393, CVE-2020-24394, CVE-2020-12403, CVE-2020-14367, CVE-2020-15861, CVE-2020-15862, CVE-2020-8620, CVE-2020-8621, CVE-2020-8622, CVE-2020-8623, CVE-2020-8624, CVE-2020-8231, CVE-2020-1938

- CVE-2018-19985, CVE-2018-20784, CVE-2019-0136, CVE-2019-10207, CVE-2019-10638, CVE-2019-10639, CVE-2019-11487, CVE-2019-11599, CVE-2019-11810, CVE-2019-13631,CVE-2019-13648, CVE-2019-14283, CVE-2019-14284, CVE-2019-14763, CVE-2019-15090, CVE-2019-15211, CVE-2019-15212, CVE-2019-15214, CVE-2019-15215, CVE-2019-15216, CVE-2019-15218, CVE-2019-15220, CVE-2019-15221, CVE-2019-15292, CVE-2019-3701, CVE-2019-3819, CVE-2019-3900, CVE-2019-9506, CVE-2018-21008, CVE-2019-14814, CVE-2019-14815, CVE-2019-14816, CVE-2019-14821, CVE-2019-15117, CVE-2019-15118, CVE-2019-15505, CVE-2019-15902, CVE-2019-15918, CVE-2019-14895, CVE-2019-14896, CVE-2019-14897, CVE-2019-14901, CVE-2019-16231, CVE-2019-16233, CVE-2019-18660, CVE-2019-19045, CVE-2019-19052, CVE-2019-19083, CVE-2019-19524, CVE-2019-19529, CVE-2019-19534, CVE-2019-19807, CVE-2018-18397, CVE-2018-19854, CVE-2019-6133, CVE-2018-14678, CVE-2018-18021, CVE-2018-19824, CVE-2019-3459, CVE-2019-3460, CVE-2019-6974, CVE-2019-7221, CVE-2019-7222, CVE-2019-7308, CVE-2019-8912, CVE-2019-8980, CVE-2019-9213, CVE-2018-12126, CVE-2018-

12127, CVE-2018-12130, CVE-2018-16884, CVE-2019-11091, CVE-2019-3874, CVE-2019-3882, CVE-2019-9500, CVE-2019-9503, CVE-2019-11191, CVE-2019-11477, CVE-2019-11478, CVE-2019-11479, CVE-2019-11085, CVE-2019-11815, CVE-2019-11833, CVE-2018-13053, CVE-2018-13093, CVE-2018-13096, CVE-2018-13097, CVE-2018-13098, CVE-2018-13099, CVE-2018-13100, CVE-2018-14609, CVE-2018-14610, CVE-2018-14611, CVE-2018-14612, CVE-2018-14613, CVE-2018-14614, CVE-2018-14615, CVE-2018-14616, CVE-2018-14617, CVE-2018-16862, CVE-2018-20169, CVE-2018-20511, CVE-2018-20856, CVE-2018-5383, CVE-2019-10126, CVE-2019-1125, CVE-2019-12614, CVE-2019-12818, CVE-2019-12819, CVE-2019-12984, CVE-2019-13233, CVE-2019-13272, CVE-2019-2024, CVE-2019-2101, CVE-2019-3846, CVE-2019-11191, CVE-2019-11477, CVE-2019-11478, CVE-2019-11479, CVE-2019-11085, CVE-2019-11815, CVE-2019-11833, CVE-2019-11884, USN-4115-2, CVE-2019-14835, CVE-2019-15030, CVE-2019-15031, CVE-2018-20976, CVE-2019-15538, CVE-2018-12207, CVE-2019-0154, CVE-2019-0155, CVE-2019-11135, CVE-2019-15098, CVE-2019-17052, CVE-2019-17053, CVE-2019-17054, CVE-2019-17055, CVE-2019-17056, CVE-2019-17666, CVE-2019-0155, CVE-2019-16746, CVE-2019-17075, CVE-2019-17133, CVE-2019-19060, CVE-2019-19065, CVE-2019-19075, CVE-2019-14615, CVE-2020-7053, CVE-2019-14615, CVE-2019-15099, CVE-2019-15291, CVE-2019-16229, CVE-2019-16232, CVE-2019-18683, CVE-2019-18786, CVE-2019-18809, CVE-2019-18885, CVE-2019-19057, CVE-2019-19062, CVE-2019-19063, CVE-2019-19071, CVE-2019-19078, CVE-2019-19082, CVE-2019-19227, CVE-2019-19332, CVE-2019-19767, CVE-2019-19965, CVE-2019-20096, CVE-2019-5108, CVE-2020-7053, CVE-2019-15217, CVE-2019-19046, CVE-2019-19051, CVE-2019-19056, CVE-2019-19058, CVE-2019-19066, CVE-2019-19068, CVE-2020-2732, CVE-2020-8832, CVE-2020-8428, CVE-2020-8834, CVE-2020-8992, CVE-2020-11884, CVE-2020-8648, CVE-2020-9383, CVE-2020-11494, CVE-2020-11565, CVE-2020-11669, CVE-2020-12657, CVE-2020-0067, CVE-2020-0543, CVE-2020-10751, CVE-2020-12114, CVE-2020-12464, CVE-2020-1749

Extreme Management Center and ExtremeControlengine images

- CVE-2019-7317, CVE-2020-13820, CVE-2020-13819, CVE-2019-11599, CVE-2019-9503, CVE-2019-3842, CVE-2018-12126, CVE-2018-12127, CVE-2018-12130, CVE-2019-11091, CVE-2019-3874, CVE-2019-3882, CVE-2019-6133, CVE-2018-5743, CVE-2019-0136, CVE-2019-10207, CVE-2019-11487, CVE-2019-13631, CVE-2019-15211, CVE-2019-15215, CVE-2018-21008, CVE-2019-14816, CVE-2019-14821, CVE-2019-15117, CVE-2019-15118, CVE-2019-15505, CVE-2019-15902, CVE-2018-20784, CVE-2019-10638, CVE-2019-13648, CVE-2019-14283, CVE-2019-14284, CVE-2019-3900, CVE-2019-14835, CVE-2019-15030

Extreme Management Center and ExtremeAnalyticsengine images

- CVE-2019-14895, CVE-2019-14896, CVE-2019-14897, CVE-2019-14901, CVE-2019-16231, CVE-2019-18660, CVE-2019-19045, CVE-2019-19052, CVE-2019-19524, CVE-2019-19534, CVE-2019-19529

Extreme Management Center engine image

- CVE-2019-18813, CVE-2019-19051, CVE-2019-19055, CVE-2019-19072, CVE-2019-1190, CVE-2019-1191, CVE-2019-11810, CVE-2019-11815, CVE-2016-3189, CVE-2019-12900, CVE-2019-10126, CVE-2019-1125, CVE-2019-12614, CVE-2019-13272, CVE-2019-3846, CVE-2016-10743, CVE-2019-9495, CVE-2019-9497, CVE-2019-9498, CVE-2019-9499, CVE-2019-9893, CVE-2019-11477, CVE-2019-11478, CVE-2018-20836, CVE-2019-10142, CVE-2019-11833, CVE-2019-11884, CVE-2019-2054, CVE-2019-5435, CVE-2019-5436, CVE-2019-9924, CVE-2019-11555, CVE-2018-20843, CVE-2016-6153, CVE-2017-10989, CVE-2017-13685, CVE-2017-2518, CVE-2017-2519, CVE-2017-2520, CVE-2018-20346, CVE-2018-20505, CVE-2018-20506, CVE-2019-9936, CVE-2019-9937, CVE-2019-13057, CVE-2019-13565, CVE-2019-11479, CVE-2019-16056, CVE-2019-16935, CVE-2019-14615, CVE-2019-15291, CVE-2019-18683, CVE-2019-18885, CVE-2019-19057, CVE-2019-19062, CVE-2019-19063, CVE-2019-19227, CVE-2019-19332, CVE-2018-3639, CVE-2018-3640, CVE-2018-3646, CVE-2019-3462, CVE-2018-16890, CVE-2019-3822, CVE-2019-3823, CVE-2018-20685, CVE-2019-6109, CVE-2019-1559, CVE-2015-9383, CVE-2018-20406, CVE-2018-20852, CVE-2019-10160, CVE-2019-5010, CVE-2019-9636, CVE-2019-9740, CVE-2019-9947, CVE-2019-9948, CVE-2019-5481, CVE-2019-5482, CVE-2019-15903, CVE-2019-14287, CVE-2016-10905, CVE-2017-18509, CVE-2018-20961, CVE-2019-15926, CVE-2019-14835, CVE-2019-15030, CVE-2019-15031, CVE-2016-5195, CVE-2019-5094, CVE-2018-12207, CVE-2019-0154, CVE-2019-0155, CVE-2019-11135, CVE-2019-15098, CVE-2019-16746, CVE-2019-17052, CVE-2019-17053, CVE-2019-17054, CVE-2019-17055, CVE-2019-17056, CVE-2019-17666, CVE-2019-2215, CVE-2019-16275, CVE-2019-17075, CVE-2019-17133, CVE-2019-0155, CVE-2019-11135, CVE-2019-11139, CVE-2019-18218, CVE-2019-18218, CVE-2016-10906, CVE-2017-18232, CVE-2019-14814, CVE-2019-16168, CVE-2019-19242, CVE-2019-19244, CVE-2019-5018, CVE-2019-5827, CVE-2018-20856, CVE-2018-10844, CVE-2018-10845, CVE-2018-10846, CVE-2019-3829, CVE-2019-3836, CVE-2016-7076, CVE-2017-1000368, USN-4038-3,USN-4049-3, 1999-0632

ExtremeControlengine image

- CVE-2019-10092, CVE-2019-11234, CVE-2019-11235, CVE-2018-16884, CVE-2019-9500, CVE-2018-14678, CVE-2018-18021, CVE-2018-19824, CVE-2019-3459, CVE-2019-3460, CVE-2019-6974, CVE-2019-7221, CVE-2019-7222, CVE-2019-7308, CVE-2019-8912, CVE-2019-8980, CVE-2019-9213, CVE-2018-18397, CVE-2018-19854, CVE-2019-6454, CVE-2019-14814, CVE-2019-14815, CVE-2019-15918, CVE-2018-19985, CVE-2019-10639, CVE-2019-14763, CVE-2019-15090, CVE-2019-15212, CVE-2019-15214, CVE-2019-15216, CVE-2019-15218, CVE-2019-15220, CVE-2019-15221, CVE-2019-15292, CVE-2019-3701, CVE-2019-3819, CVE-2019-9506
- CVE-2018-19985, CVE-2018-20784, CVE-2019-0136, CVE-2019-10207, CVE-2019-10638, CVE-2019-10639, CVE-2019-11487, CVE-2019-11599, CVE-2019-11810, CVE-2019-13631, CVE-2019-13648, CVE-2019-14283, CVE-2019-14284, CVE-2019-14763, CVE-2019-15090, CVE-2019-15211, CVE-2019-15212, CVE-2019-15214, CVE-2019-15215, CVE-2019-15216, CVE-2019-15218, CVE-2019-15220, CVE-2019-15221, CVE-2019-15292, CVE-2019-3701, CVE-2019-3819, CVE-2019-3900, CVE-2019-9506, CVE-2018-21008, CVE-2019-14814, CVE-2019-14815, CVE-2019-14816, CVE-2019-14821, CVE-2019-15117, CVE-2019-

15118, CVE-2019-15505, CVE-2019-15902, CVE-2019-15918, CVE-2019-14895, CVE-2019-14896, CVE-2019-14897, CVE-2019-14901, CVE-2019-16231, CVE-2019-16233, CVE-2019-18660, CVE-2019-19045, CVE-2019-19052, CVE-2019-19083, CVE-2019-19524, CVE-2019-19529, CVE-2019-19534, CVE-2019-19807, CVE-2020-15778, CVE-2018-18397, CVE-2018-19854, CVE-2019-6133, CVE-2019-7303, CVE-2018-14678, CVE-2018-18021, CVE-2018-19824, CVE-2019-3459, CVE-2019-3460, CVE-2019-6974, CVE-2019-7221, CVE-2019-7222, CVE-2019-7308, CVE-2019-8912, CVE-2019-8980, CVE-2019-9213, CVE-2018-12126, CVE-2018-12127, CVE-2018-12130, CVE-2018-16884, CVE-2019-11091, CVE-2019-3874, CVE-2019-3882, CVE-2019-9500, CVE-2019-9503, CVE-2019-11191, CVE-2019-11477, CVE-2019-11478, CVE-2019-11479, CVE-2019-11085, CVE-2019-11815, CVE-2019-11833, CVE-2019-11884, CVE-2018-13053, CVE-2018-13093, CVE-2018-13096, CVE-2018-13097, CVE-2018-13098, CVE-2018-13099, CVE-2018-13100, CVE-2018-14609, CVE-2018-14610, CVE-2018-14611, CVE-2018-14612, CVE-2018-14613, CVE-2018-14614, CVE-2018-14615, CVE-2018-14616, CVE-2018-14617, CVE-2018-16862, CVE-2018-20169, CVE-2018-20511, CVE-2018-20856, CVE-2018-5383, CVE-2019-10126, CVE-2019-1125, CVE-2019-12614, CVE-2019-12818, CVE-2019-12819, CVE-2019-12984, CVE-2019-13233, CVE-2019-13272, CVE-2019-2024, CVE-2019-2101, CVE-2019-3846, CVE-2018-12207, CVE-2019-0154, CVE-2019-0155, CVE-2019-11135, CVE-2019-15098, CVE-2019-17052, CVE-2019-17053, CVE-2019-17054, CVE-2019-17055, CVE-2019-17056, CVE-2019-17666, CVE-2019-0155, CVE-2019-16746, CVE-2019-17075, CVE-2019-17133, CVE-2019-19060, CVE-2019-19065, CVE-2019-19075, CVE-2019-14615, CVE-2020-7053, CVE-2019-14615, CVE-2019-15099, CVE-2019-15291, CVE-2019-16229, CVE-2019-16232, CVE-2019-18683, CVE-2019-18786, CVE-2019-18809, CVE-2019-18885, CVE-2019-19057, CVE-2019-19062, CVE-2019-19063, CVE-2019-19071, CVE-2019-19078, CVE-2019-19082, CVE-2019-19227, CVE-2019-19332, CVE-2019-19767, CVE-2019-19965, CVE-2019-20096, CVE-2019-5108, CVE-2020-7053, CVE-2019-12380, CVE-2019-16089, CVE-2019-19036, CVE-2019-19039, CVE-2019-19318, CVE-2019-19377, CVE-2019-19462, CVE-2019-19813, CVE-2019-19816, CVE-2020-10711, CVE-2020-12770, CVE-2020-13143, CVE-2020-11933, CVE-2020-11934, CVE-2019-20908, CVE-2020-10757, CVE-2020-11935, CVE-2020-15780, CVE-2018-20669, CVE-2019-19947, CVE-2019-20810, CVE-2020-10732, CVE-2020-10766, CVE-2020-10767, CVE-2020-10768, CVE-2020-10781, CVE-2020-12655, CVE-2020-12656, CVE-2020-12771, CVE-2020-13974, CVE-2020-15393, CVE-2020-24394, CVE-2020-14386, CVE-2019-18808, CVE-2019-19054, CVE-2019-19061, CVE-2019-19067, CVE-2019-19073, CVE-2019-19074, CVE-2019-9445, CVE-2020-12888, CVE-2020-14356, CVE-2020-16166, CVE-2018-10322, CVE-2019-19448, CVE-2020-14314, CVE-2020-16119, CVE-2020-16120, CVE-2020-25212, CVE-2020-26088, CVE-2020-26116, CVE-2020-12351, CVE-2020-12352, CVE-

2020-10543, CVE-2020-10878, CVE-2020-12723, CVE-2020-25659, CVE-2018-14036, CVE-2020-16126, CVE-2020-16127, CVE-2020-25692, CVE-2020-8694, CVE-2020-8695, CVE-2020-8696, CVE-2020-8698, CVE-2020-25694, CVE-2020-25695, CVE-2020-25696, CVE-2020-25709, CVE-2020-25710, CVE-2020-28196, CVE-2020-0423, CVE-2020-10135, CVE-2020-14351, CVE-2020-14390, CVE-2020-25211, CVE-2020-25284, CVE-2020-25643, CVE-2020-25645, CVE-2020-25705, CVE-2020-28915, CVE-2020-4788, CVE-2020-14351, CVE-2020-14390, CVE-2020-25211, CVE-2020-25284, CVE-2020-25285, CVE-2020-25641, CVE-2020-25643, CVE-2020-25645, CVE-2020-28915, CVE-2020-4788, CVE-2020-8231, CVE-2020-8284, CVE-2020-8285, CVE-2020-8286, CVE-2020-27350, CVE-2020-27351, CVE-2014-9913, CVE-2016-9844, CVE-2018-1000035, CVE-2018-18384, CVE-2019-13232

ExtremeAnalyticsengine image

- CVE-2019-16233, CVE-2019-19083, CVE-2019-19807, CVE-2018-19985, CVE-2018-20784, CVE-2019-0136, CVE-2019-10207, CVE-2019-10638, CVE-2019-10639, CVE-2019-11487, CVE-2019-11599, CVE-2019-11810, CVE-2019-13631, CVE-2019-13648, CVE-2019-14283, CVE-2019-14284, CVE-2019-14763, CVE-2019-15090, CVE-2019-15211, CVE-2019-15212, CVE-2019-15214, CVE-2019-15215, CVE-2019-15216, CVE-2019-15218, CVE-2019-15220, CVE-2019-15221, CVE-2019-15292, CVE-2019-3701, CVE-2019-3819, CVE-2019-3900, CVE-2019-9506, CVE-2018-21008, CVE-2019-14814, CVE-2019-14815, CVE-2019-14816, CVE-2019-14821, CVE-2019-15117, CVE-2019-15118, CVE-2019-15505, CVE-2019-15902, CVE-2019-15918, CVE-2019-14895, CVE-2019-14896, CVE-2019-14897, CVE-2019-14901, CVE-2019-16231, CVE-2019-16233, CVE-2019-18660, CVE-2019-19045, CVE-2019-19052, CVE-2019-19083, CVE-2019-19524, CVE-2019-19529, CVE-2019-19534, CVE-2019-19807, CVE-2020-15778, CVE-2018-18397, CVE-2018-19854, CVE-2019-6133, CVE-2019-7303, CVE-2018-14678, CVE-2018-18021, CVE-2018-19824, CVE-2019-3459, CVE-2019-3460, CVE-2019-6974, CVE-2019-7221, CVE-2019-7222, CVE-2019-7308, CVE-2019-8912, CVE-2019-8980, CVE-2019-9213, CVE-2018-12126, CVE-2018-12127, CVE-2018-12130, CVE-2018-16884, CVE-2019-11091, CVE-2019-3874, CVE-2019-3882, CVE-2019-9500, CVE-2019-9503, CVE-2019-11191, CVE-2019-11477, CVE-2019-11478, CVE-2019-11479, CVE-2019-11085, CVE-2019-11815, CVE-2019-11833, CVE-2019-11884, CVE-2018-13053, CVE-2018-13093, CVE-2018-13096, CVE-2018-13097, CVE-2018-13098, CVE-2018-13099, CVE-2018-13100, CVE-2018-14609, CVE-2018-14610, CVE-2018-14611, CVE-2018-14612, CVE-2018-14613, CVE-2018-14614, CVE-2018-14615, CVE-2018-14616, CVE-2018-14617, CVE-2018-16862, CVE-2018-20169, CVE-2018-20511, CVE-2018-20856, CVE-2018-5383, CVE-2019-10126, CVE-2019-1125, CVE-2019-12614, CVE-

2019-12818, CVE-2019-12819, CVE-2019-12984, CVE-2019-13233, CVE-2019-13272, CVE-2019-2024, CVE-2019-2101, CVE-2019-3846, CVE-2019-14835, CVE-2019-15030, CVE-2019-15031, CVE-2018-20976, CVE-2019-15538, CVE-2018-12207, CVE-2019-0154, CVE-2019-0155, CVE-2019-11135, CVE-2019-15098, CVE-2019-17052, CVE-2019-17053, CVE-2019-17054, CVE-2019-17055, CVE-2019-17056, CVE-2019-17666, CVE-2019-0155, CVE-2019-16746, CVE-2019-17075, CVE-2019-17133, CVE-2019-19060, CVE-2019-19065, CVE-2019-19075, CVE-2019-14615, CVE-2020-7053, CVE-2019-14615, CVE-2019-15099, CVE-2019-15291, CVE-2019-16229, CVE-2019-16232, CVE-2019-18683, CVE-2019-18786, CVE-2019-18809, CVE-2019-18885, CVE-2019-19057, CVE-2019-19062, CVE-2019-19063, CVE-2019-19071, CVE-2019-19078, CVE-2019-19082, CVE-2019-19227, CVE-2019-19332, CVE-2019-19767, CVE-2019-19965, CVE-2019-20096, CVE-2019-5108, CVE-2019-7053, CVE-2019-15217, CVE-2019-19046, CVE-2019-19051, CVE-2019-19056, CVE-2019-19058, CVE-2019-19066, CVE-2019-19068, CVE-2020-2732, CVE-2020-8832, CVE-2020-8428, CVE-2020-8834, CVE-2020-8992, CVE-2019-16234, CVE-2019-19768, CVE-2020-10942, CVE-2020-11608, CVE-2020-11609, CVE-2020-11668, CVE-2020-11884, CVE-2020-8648, CVE-2020-9383, CVE-2020-11494, CVE-2020-11565, CVE-2020-11669, CVE-2020-12657, CVE-2020-0067, CVE-2020-0543, CVE-2020-10751, CVE-2020-12114, CVE-2020-12464, CVE-2020-1749, CVE-2020-5963, CVE-2020-5967, CVE-2020-5973