6480 Via Del Oro
San Jose, CA 95119
+1 888-257-3000

Customer Release Notes

ExtremeCloud Appliance

Firmware Version V4.26.01.0166
August 30, 2019

INTRODUCTION:

This document provides specific information for version V4.26.01 of firmware for the ExtremeCloud Appliance ECA products.

The ExtremeCloud Appliance, the newest addition to the Smart OmniEdge portfolio, is a next generation orchestration application offering all the mobility services required for modern unified access deployments. The ExtremeCloud Appliance extends all the ease-of-use and simplified workflows of the ExtremeCloud public cloud application to on-prem/private cloud deployments. The ExtremeCloud Appliance includes comprehensive critical network services for wireless and wired connectivity, wireless device secure onboarding, distributed and centralized data paths, role-based access control through the Application Layer (Layer 7), integrated location services, and IoT device onboarding through a single platform. Built on field proven architectures with the latest technology, the embedded operating system supports containerization of applications enabling future expansion of value added applications for the unified access edge.

The E2120 is a large application appliance meeting the needs of high-density and mission critical deployments with support for up to 4,000 APs/Defenders, 800 switches and 32,000 mobility sessions in high-availability mode. An optional redundant power supply is available for ordering separately.

The E1120 is an entry to mid-level platform expandable to 250 APs/Defenders, 100 switches, and 4,000 mobility sessions in high-availability mode.

The VE6120 is an elastic virtual appliance that supports up to 1,000 APs/Defenders, up to 400 switches and 16,000 mobility sessions depending on the hosting hardware.

The ExtremeCloud Appliance offers the ability to expand capacity to meet any growing business needs. The hardware and virtual packages are available for purchase using a traditional CAPEX model, while the adoption licenses are available as an annual subscription service in 5, 25, 100, 500 and 2000 managed device increments.

E1120	ExtremeCloud Appliance hardware platform
E2120	ExtremeCloud Appliance hardware platform
VE6120	ExtremeCloud Appliance VM-ware Software platform

Extreme Networks recommends that you thoroughly review this document prior to installing or upgrading this product.

For the latest firmware versions, visit the download site at:
www.extremenetworks.com/support/

FIRMWARE SPECIFICATION:

Status	Version No.	Type	Release Date
Current Version	V.04.26.01	Feature Release (new product)	September 4th 2018

SUPPORTED APPLIANCES, ACCESS POINTS AND SWITCHES:

Product Name	Image
ExtremeCloud Appliance VE6120 VMware (ESXi 6.5)	ECA-04.26.01.0166-1.dle (.ova)
ExtremeCloud Appliance V1120	ECA-04.26.01.0166-1.sme
ExtremeCloud Appliance V2120	ECA-04.26.01.0166-1.jse
Note: The minimum release dependency for WiNG APs is ExtremeWireless WiNG v5.9.2.2. WiNG APs must be manually upgraded to v5.9.2.2 before being adopted by ExtremeCloud Appliance. After upgrade, reset the WiNG AP to the factory settings. For more information, see GTAC article: ExtremeCloud Appliance - WiNG AP will not connect to ExtremeCloud Appliance.	
AP-7612-680B30-US AP-7612-680B30-WR	AP7612-LEAN-5.9.2.2-005R.img
AP-7632-680B30-US AP-7632-680B30-WR AP-7632-680B40-US AP-7632-680B40-WR	AP7632-LEAN-5.9.2.2-005R.img
AP-7662-680B30-US AP-7662-680B30-WR AP-7662-680B40-US AP-7662-680B40-WR	AP7632-LEAN-5.9.2.2-005R.img
AP-8533-68SB30-US AP-8533-68SB30-WR	AP8533-LEAN-5.9.2.2-005R.img
AP-8533-68SB30-EU AP-8533-68SB40-US AP-8533-68SB40-WR AP-8533-68SB40-EU	AP8533-LEAN-5.9.2.2-005R.img
AP-8432-680B30-US AP-8432-680B30-WR AP-8432-680B30-EU	AP8432-LEAN-5.9.2.2-005R.img
AP3912i-FCC AP3912i-ROW	AP3912-10.41.09.0008.img
AP3915i-FCC AP3915e-FCC AP3915i-ROW AP3915e-ROW	AP3912-10.41.09.0008.img
AP3916i-FCC AP3916i-ROW	AP3912-10.41.09.0008.img
AP3917i-FCC AP3917e-FCC AP3917i-ROW AP3917e-ROW	AP3912-10.41.09.0008.img

Product Name	Image
AP3935i-FCC AP3935e-FCC AP3935i-ROW AP3935e-ROW	AP3935-10.41.09.0008.img
AP3965i-FCC AP3965e-FCC AP3965i-ROW AP3965e-ROW	AP3935-10.41.09.0008.img
210-12p-10GE2 210-24p-10GE2 210-48p-10GE2 210-12p-10GE2 POE 210-24p-10GE2 POE 210-48p-10GE2 POE	210-series_V1.02.04.0007 p-connector-3.0.34.16.pyz (cloud connector)
220-12p-10GE2 220-24p-10GE2 220-48p-10GE2 220-12p-10GE2 POE 220-24p-10GE2 POE 220-48p-10GE2 POE	220-series_V1.02.04.0007 p-connector-3.0.34.16.pyz (cloud connector)
X440G2-12t-10G4 X440G2-24t-10G4 X440G2-48t-10G4 X440G2-12t-10G4 POE X440G2-24t-10G4 POE X440G2-48t-10G4 POE	summit-21.1.5.2.xos summit-cloud_connector-3.0.34.62.xmod (cloud connector)
X620-16x	summit-21.1.5.2.xos summit-cloud_connector-3.0.34.62.xmod (cloud connector)

NETWORK MANAGEMENT SOFTWARE SUPPORT

Network Management Suite (NMS)	Version
ExtremeManagement™ Center	8.1.4.27 or higher
ExtremeControl™	8.1.4.27 or higher (per ExtremeManagement Center release)
ExtremeAnalytics™	8.1.4.27 or higher (per ExtremeManagement Center release)

Air Defense and Location	Version
ExtremeAirDefense™	9.5 or higher
ExtremeLocation™	1.2 or higher

Note:

Platform and AP Configuration functions are not supported via ExtremeManagement™.

ExtremeCloud Appliance does not yet expose support for ExtremeLocation™ Calibration procedure. ExtremeLocation will work correctly for Zone and Occupancy level analytics but does not fully support Position Tracking with this release. Enhanced support for Position Tracking will be added to a future release of ExtremeCloud Appliance.

INSTALLATION INFORMATION:

Appliance Installations	
E1120	ExtremeCloud Appliance E1120 Installation Guide
E2120	ExtremeCloud Appliance E2120 Installation Guide
VE6120	ExtremeCloud Appliance VE6120 Installation Video

NEW FEATURES, SOFTWARE CHANGES, AND ENHANCEMENTS:

ExtremeCloud Appliance 4.26.01.166

ExtremeCloud Appliance 4.26.01 is the first release of this program, offering:

- Unified Campus and Distributed WLAN orchestration for ExtremeWireless™ and ExtremeWireless™ WiNG
- Simplified management of ExtremeWireless
  - Switch health status
  - Port State/Status, VLAN assignment and LAG
- Coordinated user experience with ExtremeCloud™
- Consistent policy enforcement for Campus and Distributed deployments
- Integrated user Enrollment engine
  - BYOD and Guest Services
  - Integrated AD support
  - Integrated Captive Portal. Optional Social Log in
- Layer 2-7 policy definition
- Support for Zero touch deployment of Wireless and Wired infrastructure
- Aggregate, top level view and granular/context based dashboards
- Customizable, template-able dashboards with a rich set of contextual widgets
- Site level management
- Integrated deployment visibility
  - Floorplan locations
  - RF visibility (Coverage, Channel, RFQI, etc..)
  - Occupancy representation
  - RF Expert widgets for detailed insight into state of RF environment

- Extensive REST API of all presented functionality for easy integration, orchestration and customization with external systems.
- Complementary extension of ExtremeWireless™ installation via inter-Controller Mobility
- Active-Active or Active-Passive High Availability
- HTTP based firmware image management (HTTP upload)
- Hardware or Virtual form factor options
- Complementary Integration with Value Add Extreme software portfolio (ExtremeManagement Center™, ExtremeAnalytics™, ExtremeAirDefense™, ExtremeLocation™)

KNOWN RESTRICTIONS AND LIMITATIONS:

Known Restriction or Limitation	I.D
Multicast rules for Topolgies (VLANs) are only enforced on Centralized Site deployments (ExtremeWireless APs) The multicast rules are not enforced by Distributed Sites (ExtremeWirless WiNG APs), Topology assignment in Distributed sites does not filter multicast and therefore all such traffic is bridged between wireless and wired). AP76xx, AP8432 and AP8533 bridge all multicast traffic from wired to wireless network.	
For service authentication in Distributed Sites (ExtremeWireless WiNG), the Default Unauth Role is applied if the configured RADIUS server can't be reached for authentication.MBA Timeout Role configured for an MBA network is not applied to an End Client (Mobile Unit [MU]) session	
200 Series switches do not support redundancy for management connection. The switch management connector supports only connection with a single management entity. When deployed in a High-Availability configuration, if the connection with the primary appliance (from which the switch is being managed) fails, this family of switches does not automatically failover to the HA peer. Therefore, until it's primary appliance returns to service, the switch will not provide metrics to the ExtremeCloud Appliance engines, it will not receive any additional configuration changes, and it will be reported in a 'Down' state. This state is transparent to the connected devices. There is no service interruption – just a reporting interruption. The operation of the switch remains unaffected (operating according to its last configuration set) and continues to forward traffic. The situation self-corrects when the primary appliance returns to active service in the HA pair. This situation will be addressed in a future release.	nse002870
Certain wireless clients such as Qualcomm Killer Wireless 1535 and Intel 7265D/8260/8265 have been known to not complete the 4-way handshake in order to fulfill the association process in networks that have both PMF/MFP (802.11w) and Fast-Transition (802.11r [FT]) enabled.	nse003416

The currently recommended workaround is to remove/diable PMF/MFP configuration on the service. Such clients have been demonstrated to work correctly on services with just 802.11r (FT) enabled.	
Manual Channel settings for a Radio may not be preserved for Active-Active High Availability. When selecting radio channels manually for AP39xx in availability mode, the selected channel may not be sent to the AP when "Auto AP balancing" is "Active - Active". Workaround: When manually setting channels (not using “Auto-Channel Selection mode [ACS]) in availability setup, set "Auto AP balancing" to "Active - Passive" and configure channels on the primary ECA. After all channels are configured and all APs accept the selected channel, can the "Auto AP Balancing" mode be changed to a desired value.	nse003422
Interaction with ExtremeManagement Center – Management of ExtremeCloud Appliance by XMC will be enhanced over time with the roadmap. ExtremeManagement Center v8.1.4 is the minimum release base for integration. Version 8.1.4 provides recognition of an ExtremeCloud Appliance and representation of Wireless Clients and managed Access Points included in the Wireless tab. Additional integration will be delivered in upcoming releases.	
MAC address for Clients on ExtremeWireless WiNG™ APs are displayed in the Username column. WiNG AP sends the username as a MAC Address, causing NAC to reevaluate the rule engines. This situation will be addressed in a future release.	nse0003279
Wireless capture on Wing AP may return wrong packet captures containing wired packets and wireless packets only for uplink. This situation will be addressed in a future release.	nse0002243
Wing APs do not yet support Availabilty failover. In an High-Availabilty configuration, the WiNG AP will only connect to the appliance instance it discovers. During a service interruption of its primary controller stats from such APs will not be collected and configuration changes will not be propagated. AP may be reported in a “Down” status by the HA Peer. Once the discovered appliance rejoins the HA pair, all service and state representation is restored. This situation will be addressed in a future release.	nse0002542
Client IP address is now displayed on Clients Report for clients connected on WiNG APs. This situation will be addressed in a future release.	nse0002645
Stats for wired clients connected to a Wing AP7612 wired port are missing in the ECA reports. This situation will be addressed in a future release.	nse0002419
Global IPv6 IP addressed are not displayed in the details’ client page, local IPv6 addresses are. This situation will be addressed in a future release.	nse0002893

SUPPORTED WEB BROWSERS

For ECA management GUI, the following Web browsers were tested for interoperability:

- MS IE 8.0, IE9, IE10, IE11, Edge
- Firefox 38.0
- Google Chrome 43.0

The Wireless Clients (Captive Portal, AAA):

Browsers	Version	OS
Chrome	46.0.2490.71 dev-m	Windows server 2012
Chrome	47.0.2526.80 m	Windows 7
Chrome	38.0.2125.111m	Windows server 2012
Firefox	41.0.1	Windows server 2012
Firefox	38.0.5	Windows XP
Opera beta	34.0.2036.24	Windows 7
Safari	preinstalled with iOS9.1	iOS9.1

PORT LIST

The following list of ports may need to remain open so that the Appliances and APs will function properly on a network that includes protection equipment like a firewall.

ExtremeWireless TCP/UDP Port Assignment Reference

Comp. Source	Comp. Dest	Protocol (TCP/UDP)	Src Port	Dest Port	Service	Remark	Open Firewall Req'd
Ports for AP/Appliance Communication							
Appliance	Access Point	UDP	Any	13910	WASSP	Management and Data Tunnel between AP and Appliance	Yes
Access Point	Appliance	UDP	Any	13910	WASSP	Management and Data Tunnel between AP and Appliance	Yes
Appliance	Access Point	UDP	4500	Any	Secured WASSP	Management Tunnel between AP and Appliance	Optional

Comp. Source	Comp. Dest	Protocol (TCP/UDP)	Src Port	Dest Port	Service	Remark	Open Firewall Req'd
Access Point	Appliance	UDP	Any	4500	Secured WASSP	Management Tunnel between AP and Appliance	Optional
Access Point	Appliance	UDP	Any	13907	WASSP	AP Registration to Appliance	Yes
Access Point	Appliance	UDP	Any	67	DHCP Server	If Appliance is DHCP Server for AP	Optional
Access Point	Appliance	UDP	Any	68	DHCP Server	If Appliance is DHCP Server for AP	Optional
Access Point	Appliance	UDP	Any	427	SLP	AP Registration to Appliance	Optional
Appliance	Access Point	TCP/UDP	Any	69	TFTP	AP image transfer	Yes[1]
Access Point	Appliance	TCP/UDP	Any	69	TFTP	AP image transfer	Yes[2]
Appliance	Access Point	TCP/UDP	Any	22	SCP	AP traces	Yes
Any	Access Point	TCP	Any	2002, 2003	RCAPD	AP Real Capture (if enabled)	Optional
Any	Access Point	TCP/UDP	Any	22	SSH	Remote AP login (if enabled)	Optional
Any	Access Point	TCP/UDP	Any	445	Microsoft CIFS	LDAP support	Optional
Any	Access Point	TCP/UDP	Any	137, 138, 139	NetBIOS	LDAP support	Optional
Ports for Appliance Management							
Any	Appliance	TCP/UDP	Any	22	SSH	Appliance CLI access	Yes
Any	Appliance	TCP/UDP	Any	5825	HTTPS	Appliance GUI access	Yes
Any	Appliance	TCP/UDP	Any	161	SNMP	Appliance SNMP access	Yes

[1] TFTP uses port 69 only when the secure control tunnel is NOT enabled between the AP and controller. If the secure control tunnel is enabled, TFTP exchanges take place within the secure tunnel and port 69 is not used.

[2] TFTP uses port 69 only when the secure control tunnel is NOT enabled between the AP and controller. If the secure control tunnel is enabled, TFTP exchanges take place within the secure tunnel and port 69 is not used.

Comp. Source	Comp. Dest	Protocol (TCP/UDP)	Src Port	Dest Port	Service	Remark	Open Firewall Req'd
Any	Appliance	TCP/UDP	Any	162	SNMP Trap	Appliance SNMP access	Yes
Any	Appliance	TCP	Any	80	HTTP	Appliance SNMP access ICP Self Registration	Yes
Any	Appliance	TCP	Any	443	HTTPS	ICP Self Registration	Yes
Any	Appliance	UDP	500	500	IKE	IKE phase 1	Yes
Any	Appliance	TCP/UDP	Any	69	TFTP	TFTP support	Yes
Any	Appliance	UDP	Any	4500	IPSec	IPSec NAT traversal	Yes
Any	Appliance	UDP	Any	13907	Discovery	Used by Discovery	Yes
Any	Appliance	UDP	Any	13910	WASSP	Used by L3 WASSP	Yes
Ports for Inter Controller Mobility[3] and Availability							
Appliance	Appliance	UDP	Any	13911	WASSP	Mobility and Availability Tunnel	Yes
Appliance	Appliance	TCP	Any	427	SLP	SLP Directory	Yes
Appliance	Appliance	TCP	Any	20506	Langley	Remote Langley Secure	Yes
Appliance	Appliance	TCP	Any	60606	Mobility	VN MGR	Yes
Appliance	Appliance	TCP	Any	123	NTP	Availability time sync	Yes
Appliance	DHCP Server	UDP	Any	67	SLP	Asking DHCP Server for SLP DA	Yes
DHCP Server	Appliance	UDP	Any	68	SLP	RespoECA from DHCP Server for SLP DA request	Yes
Core Back-End Communication							
Appliance	DNS Server	UDP	Any	53	DNS	If using DNS	Optional
Appliance	Syslog Server	UDP	Any	514	Syslog	If Appliance logs to external syslog server	Optional
Appliance	RADIUS Server	UDP	Any	1812	RADIUS Authentication	If using RADIUS AAA	Optional

[3]For extension of ExtremeWireless deployment via Inter Controller Mobility.

Comp. Source	Comp. Dest	Protocol (TCP/UDP)	Src Port	Dest Port	Service	Remark	Open Firewall Req'd
					and Authorization		
Appliance	RADIUS Server	UDP	Any	1813	RADIUS Accounting	If enabled RADIUS accounting	Optional
Appliance	RADIUS server	UDP	Any	1814	RADIUS Authentication and Authorization	If using RADIUS AAA	Optional
Appliance	RADIUS server	UDP	Any	1815	RADIUS Accounting	If enabled RADIUS Accounting	Optional

IETF STANDARDS MIB SUPPORT:

RFC No.	Title	Groups Supported
Draft version of 802.11	IEEE802dot11-MIB	
1213	RFC1213-MIB	Most of the objects supported
1573	IF-MIB	ifTable and interface scalar supported
1907	SNMPv2-MIB	System scalars supported
1493	BRIDGE-MIB	EWC supports relevant subset of the MIB
2674	P-BRIDGE-MIB	EWC supports relevant subset of the MIB
2674	Q-BRIDGE-MIB	EWC supports relevant subset of the MIB

EXTREME NETWORKS PRIVATE ENTERPRISE MIB SUPPORT

Extreme Networks Private Enterprise MIBs are available in ASN.1 format upon request.

Standard MIBs

Title	Description
IEEE802dot11-MIB	Standard MIB for wireless devices
RFC1213-MIB.my	Standard MIB for system information
IF-MIB	Interface MIB
SNMPv2-MIB	Standard MIB for system information
BRIDGE-MIB	VLAN configuration information that pertains to EWC

Title	Description
P-BRIDGE-MIB	VLAN configuration information that pertains to EWC
Q-BRIDGE-MIB	VLAN configuration information that pertains to EWC

Siemens Proprietary MIB

Title	Description
HIPATH-WIRELESS-HWC-MIB.my	Configuration and statistics related to EWC and associated objects
HIPATH-WIRELESS-PRODUCTS-MIB.my	Defines product classes
HIPATH-WIRELESS-DOT11-EXTNS-MIB.my	Extension to IEEE802dot11-MIB that complements standard MIB
HIPATH-WIRELESS-SMI.my	Root for Chantry/Siemens MIB

802.11AC AND 802.11N CLIENTS

Please refer to the latest release notes for ExtremeWireless™ 10.41.09 or later and/or ExtremeWireless WiNG 5.9.02 or later for the list of compatibility test devices.

RADIUS SERVERS AND SUPPLICANTS

RADIUS Servers Used During Testing

Vendor	Model OS	Version
FreeRADIUS45	1.1.6	FreeRADIUS
FreeRADIUS21	1.0.1	FreeRADIUS
IAS	5.2.3790.3959	Microsoft Server 2003 IAS
SBR50	6.1.6	SBR Enterprise edition
NPS	6.0.6002.18005	Microsoft Server 2008 NPS

802.1x Supplicants Supported

Vendor	Model OS	Version
Juniper Networks® / Funk	Odyssey client	Version 5.10.14353.0
		Version 5.00.12709.0
		Version 4.60.49335.0
Microsoft®	Wireless Zero Configuration	Version Windows XP-4K-891859-Beta1
	Wireless Network Connection Configuration	Version Microsoft Window Server 2003, Enterprise Edition R2 SP2
	Wi-Fi Protected Access 2 (WPA2)/Wireless Provisioning Services Information Element (WPS IE) update for Windows XP with Service Pack 2	Version WindowsXP-KB893357-v2-x86-ENU.exe
Intel®	Intel PRO Set/Wireless	Version 13.0.0.x (with Windows® Intel® driver version 13.0.0.x)
Microsoft® Wireless Zero	Windows 7, 8, 8.1 Pro, 10 Pro Windows Phone 8.1, Windows Mobile 10	provided with Windows®

Appliance LAN Switch Verification

Vendor	Model OS	Version	Role
Extreme	X-460-G2	12.5.4.5	ECA connection
Extreme	X440G2-48p-10G4	21.1.1.4	ECA connectivity
Extreme	Summit 300-48	7.6e1.4	ECA connection
Extreme	VSP-4850GTS-PWR	(6.0.1.1_B003) (PRIVATE) HW Base: ERS 4850	ECA connection
Extreme	K6	08.63.02.0004	ECA connection
Extreme	K6	08.42.03.0006	ECA connection
Extreme	X440G2-48p-10GE4	*21.1.5.2*	ECA connection
Extreme	X440-G2-12p	21.1.1.4	ECA connection
Extreme	X460-48p	12.5.4.5	ECA connection
Cisco	Catalyst 3550	12.1(19)EA1c	ECA connection

CERTIFICATION AUTHORITY

Server Vendor	Model OS	Version
Microsoft CA	Windows Server 2003 Enterprise Edition	5.2.3790.1830
Microsoft CA	Windows Server 2008 Enterprise Edition	6.0
OpenSSL	Linux	0.9.8e

RADIUS ATTRIBUTES SUPPORT

RADIUS Authentication and Authorization Attributes

Attribute	RFC Source
Called-Station-Id	RFC 2865, RFC 3580
Calling-Station-Id	RFC 2865, RFC 3580
Class	RFC 2865
EAP-Message	RFC 3579
Event-Timestamp	RFC 2869
Filter-Id	RFC 2865, RFC 3580
Framed-IPv6-Pool	RFC 3162
Framed-MTU	RFC 2865, RFC 3580
Framed-Pool	RFC 2869
Idle-Timeout	RFC 2865, RFC 3580
Message-Authenticator	RFC 3579
NAS-Identifier	RFC 2865, RFC 3580
NAS-IP-Address	RFC 2865, RFC 3580
NAS-IPv6-Address	RFC 3162
NAS-Port	RFC 2865, RFC 3580
NAS-Port-Id	RFC 2865, RFC 3580
NAS-Port-Type	RFC 2865, RFC 3580
Password-Retry	RFC 2869
Service-Type	RFC 2865, RFC 3580
Session-Timeout	RFC 2865
State	RFC 2865
Termination-Action	RFC 2865, RFC 3580
Tunnel Attributes	RFC 2867, RFC 2868, RFC 3580

Attribute	RFC Source
User-Name	RFC 2865, RFC 3580
Vendor-Specific	RFC 2865

RADIUS Accounting Attributes

Attribute	RFC Source
Acct-Authentic	RFC 2866
Acct-Delay-Time	RFC 2866
Acct-Input-Octets	RFC 2866
Acct-Input-Packets	RFC 2866
Acct-Interim-Interval	RFC 2869
Acct-Output-Octets	RFC 2866
Acct-Output-Packets	RFC 2866
Acct-Session-Id	RFC 2866
Acct-Session-Time	RFC 2866
Acct-Status-Type	RFC 2866
Acct-Terminate-Cause	RFC 2866

GLOBAL SUPPORT:

By Phone: +1 800-998-2408 (toll-free in U.S. and Canada)

For the toll-free support number in your country:
https://extremeportal.force.com/

By Email: support@extremenetworks.com

By Web: https://extremeportal.force.com/

By Mail: Extreme Networks, Inc.
6480 Via Del Oro
San Jose, CA 95119 USA

For information regarding the latest software release, recent release note revisions, or if you require additional assistance, please visit the Extreme Networks Support website.