Data Sheet

ExtremeCloud IQ™ Site Engine

Highlights

Ease Cloud Transition

- Enable a migration path to cloud-based management for third-party and legacy Extreme networking devices.
- Consolidate management of cloud-native, legacy Extreme, and third-party devices.

Unify Management

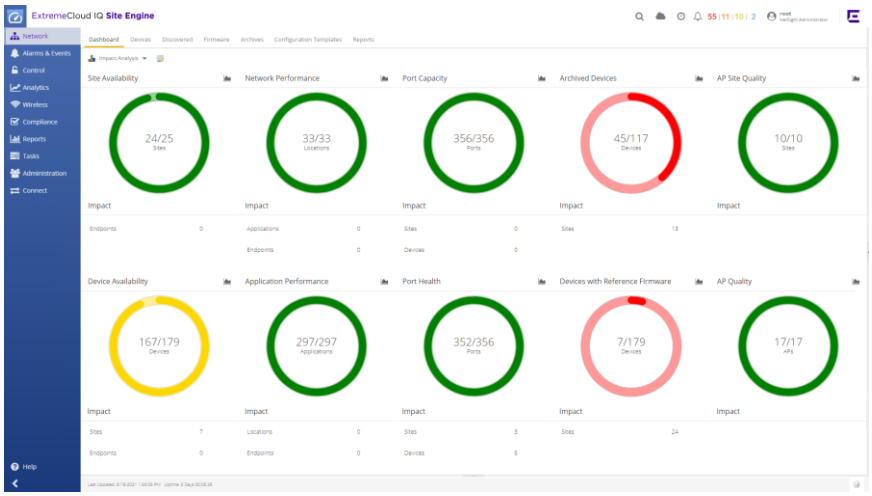
- Provide granular analysis through application telemetry and deep packet inspection (DPI).
- View topologies of the fabric-enabled sites in a network.
- Expedite root cause analysis and troubleshooting.

Automate Daily Activities

- Streamline daily activities through intuitive task automation and orchestration.
- Customize orchestration using built-in workflow tools and support for common scripting languages.
- Configure Shortest Path Bridging (SPB) and IS-IS automatically with Zero Touch Fabric Configuration.
- Facilitate integration through a comprehensive suite of open APIs.

Enhance Security and Compliance

- Address security and compliance requirements using flexible deployment options and role-based access security.
- Secure access control for guest access, bring your own device (BYOD), and Internet of Things (IoT) devices.



Transition to Cloud-Based Management, Unify Management of Third-Party Devices, and Enhance Automation

IT organizations are having to adapt to constant change while they face challenges due to growing complexity, limited integration between technologies, and a lack of operational automation. They need to decrease the overall cost of ongoing operations as well as scaling to support new business initiatives. Administrators require effective tools to help them simplify management and facilitate the transition to unified, cloud-based solutions.

Extreme unifies network management under One Cloud. As part of this strategy, ExtremeCloud™ IQ Site Engine simplifies and streamlines IT operations. It provides end-to-end network management, task automation, analytics, service assurance, and orchestration. Site Engine supports cloud-native, legacy Extreme, and third-party devices and facilitates the transition to cloud-based management. Fabric-specific visualizations and topology maps make it easier to monitor fabric-related parameters, such as Intermediate System to Intermediate System (IS-IS) areas and fabric links.

Cross-domain workflow capabilities automate routine network tasks. Site Engine provides role-based network access control (NAC) for all devices, including third-party networking devices. It also supports configuration and firmware updates across Extreme and multi-vendor devices.

Flexible deployment options address a range of security and compliance requirements. The added ability to integrate with other Extreme tools provides customers with the extensibility they need to adapt. Site Engine is a subscription-based offering based on Universal Subscriptions, so IT organizations can cost-effectively transition their entire network to cloud-based management in a way that works best for them.

Ease the Transition to One Cloud

ExtremeCloud IQ Site Engine offers end-to-end management of wired devices from the edge to the data center and across multivendor environments. It provides a centralized view of the entire network with visibility of all network devices, without having to integrate multiple applications. Site Engine enables a transition path for third-party and legacy networking devices to cloud-based network management with the ability to select which device metadata is transmitted to Extreme Platform ONE in public, private, or ExtremeCloud Edge. It also enhances Extreme Platform ONE's management capabilities with additional features for Extreme Networks Universal Platforms switches and access points (APs) and legacy devices.

Transition to Cloud-Based Management

The benefits of cloud-based management are achieved by using Site Engine together with Extreme Platform ONE in a secure mode of operation to manage the network in Extreme-hosted public or private clouds or ExtremeCloud Edge. When Site Engine is connected to Extreme Platform ONE, it can provide flexible deployment options while preserving existing investments in devices and staff training. This capability enables a transition path for third-party and legacy networking devices by allowing deployment in a connected, on-premises mode with the ability to transition to software as a service (SaaS) network management with Extreme Platform ONE when and how an IT organization chooses.

Unify Management

ExtremeCloud IQ Site Engine provides end-to-end network visibility. It reveals in-depth details into the performance of applications and the network through telemetry and deep packet inspection (DPI). Topology maps provide non-fabric and fabric visualizations, such as the ability to monitor fabric-related parameters and primary and secondary paths. Non-fabric visualizations include the visibility of virtual local area network (VLAN) presence, or the link status of the primary and secondary paths within an Ethernet Automatic Protection Switching (EAPS) scheme of an Ethernet ring architecture. Users can visualize the state of link aggregation groups (LAG) and multi-switch link aggregation groups (MLAG) and determine which devices participate in the link aggregation. They can visualize a bridge port extender (BPE) topology to determine what control bridges are used, what BPEs are present, and the state of the topology. This solution enables users to manage their networks more efficiently by providing granular analysis and fabric management to make data-driven, informed decisions.

In addition to Extreme devices, Site Engine can support Cisco, Juniper Networks, HPE Aruba, Dell, Nokia, Allied Telesis, Zyxel, Linksys, Huawei devices, and more. It uses Simple Network Management Protocol (SNMP) versions 1, 2c, and 3, as well as a command-line interface (CLI) to provide management of third-party devices. Site Engine extends support to devices that do not have robust SNMP capabilities by utilizing scripts and Telnet/SSH. As a result, it can unify management of switches, APs, firewalls, bridges, servers, sensors, and other networking and IoT devices.

Universal Licensing

Extreme Networks unifies management by offering Universal Licensing, helping customers cost-effectively transition to cloud-based network management and subscription licensing. The same subscription applies to APs, switches, third-party, and cloud-native devices. Subscriptions are pooled, so they aren't specific to a device, location, or user. The subscription pool can be accessed via the Extreme Support portal.

- **Extreme Platform ONE Standard Tier A-D** are the universal subscription tiers for the Extreme Platform ONE suite for end-to-end management. It enables enhanced policy enforcement, visibility, reporting, and configurations. It delivers configuration and management of infrastructure devices at scale, including advanced policy, segmentation, and troubleshooting.
- **Extreme Platform ONE Standard Tier 3rd party** is an alternative, lower capability subscription tier delivering third-party device management. It provides basic visibility and limited reporting, configuration management, advanced secure shell (SSH), scripting, and configuration backup.

Site Engine includes integrations with ExtremeAnalytics and ExtremeControl. ExtremeAnalytics is available as part of the Extreme Platform ONE Standard Tier A subscription tier. ExtremeControl is priced separately and is based on unique MAC addresses connected to the network within the past 24 hours. Third-party device support is available through all Extreme Platform ONE Standard Tiers.

Detailed Analytics

ExtremeAnalytics is a component of Site Engine that uses DPI to analyze application flows from every part of the network without requiring dedicated probes. The Analytics Engine within ExtremeAnalytics extends application visibility from wired and ExtremeCloud IQ Controller managed wireless devices all the way through the campus to the data center. These capabilities include a granular view of users, devices, and applications with an easy-to-understand dashboard inventory and network topology. Network administrators can accurately see and analyze network traffic across multiple layers for real-time analysis. When Site Engine is used with ExtremeAnalytics, it speeds up troubleshooting by separating network performance from application performance, so users can quickly identify root causes.

This component of Site Engine combines flow-based technology with a rich set of application fingerprint techniques that can identify over 8,000 applications and includes more than 10,000 behavioral detection-based fingerprints. It monitors shadow IT,

identifies and reports malicious or unwanted applications, and helps with security compliance. Integrations into Extreme Networks' Universal Switch Platform Series, VSP series, Summit Series, ERS series, and ExtremeCloud IQ Controller provide application layer visibility and latency calculations for traffic flows. Additionally, the integration of private cloud solutions based on VMware ESXi and Microsoft Hyper-V provides a unique capability of a single analytics toolset that covers campus and data center.

Fabric Management

Support for Extreme Fabric is natively designed into ExtremeCloud IQ Site Engine, drastically reducing time to service. Users benefit from being able to automatically change the switch operating system (OS) persona from the factory default Switch Engine OS to the Fabric Engine OS (formerly VOSS), while deploying the fabric network. Other capabilities include the configuration and customization of fabric topology, and the configuration of fabric services. This includes L2 Virtual Services Networks (VSNs), L3VSNs, Service ID, Name, and Type, distributed virtual routing (DVR) element (such as leaf, controller, and router) properties, router redundancy protocols (such as VRRP, RSMLT, and DVR), and port templates.

Site Engine includes tools to create topology and geographic maps of devices and floor plans of wireless APs on a network. The Fabric feature allows users to view topologies of the fabric-enabled sites in a network. It uses Fabric Topology templates so users can view and configure SPB, based L2 and L3 VSNs, as well as IP-shortcut based VSNs. Extreme Fabric can also be extended to non-fabric network devices. Site Engine displays global, server and proxy capable services for the network and the associated devices.

The topology map provides a high-level view and detailed information about devices and links in the topology. Fabric-specific visualizations make it easier to monitor fabric-related parameters, such as IS-IS areas and Fabric links, to locate where the IS-IS areas are present, and to determine which links are part of the fabric. Users can also visualize primary and secondary paths between two fabric switches in the network, and where in the network a specific fabric service is present to ascertain its main attributes (L2VSN versus L3VSN, or virtual routing and forwarding assignment). These key visibility capabilities help users monitor and validate their non-fabric, fabric, and combined deployments, so they can troubleshoot them more easily.

Site Engine displays the Fabric link Summary table for maps with one or more network connections and detailed information about the connections between devices. Multi-area fabrics display the IS-IS areas with the assignment of Fabric Engine (VSPs) to both Home and Remote areas. Links are displayed on topology maps as lines between devices in a network. The line colors used in the map indicate the state and status of the link. Selecting one of the links in the table highlights the link in the map.

The integration of Extreme Fabric with ExtremeCloud SD-WAN enables Site Engine to display tunnels extending services through SD-WAN and report tunnel failure between SD-WAN devices. Network operators can easily navigate from Site Engine to an SD-WAN appliance, and then use the 360 view to investigate and troubleshoot. The user can also access Site Engine from ExtremeCloud SD-WAN Orchestrator with SSO, as part of unified management.

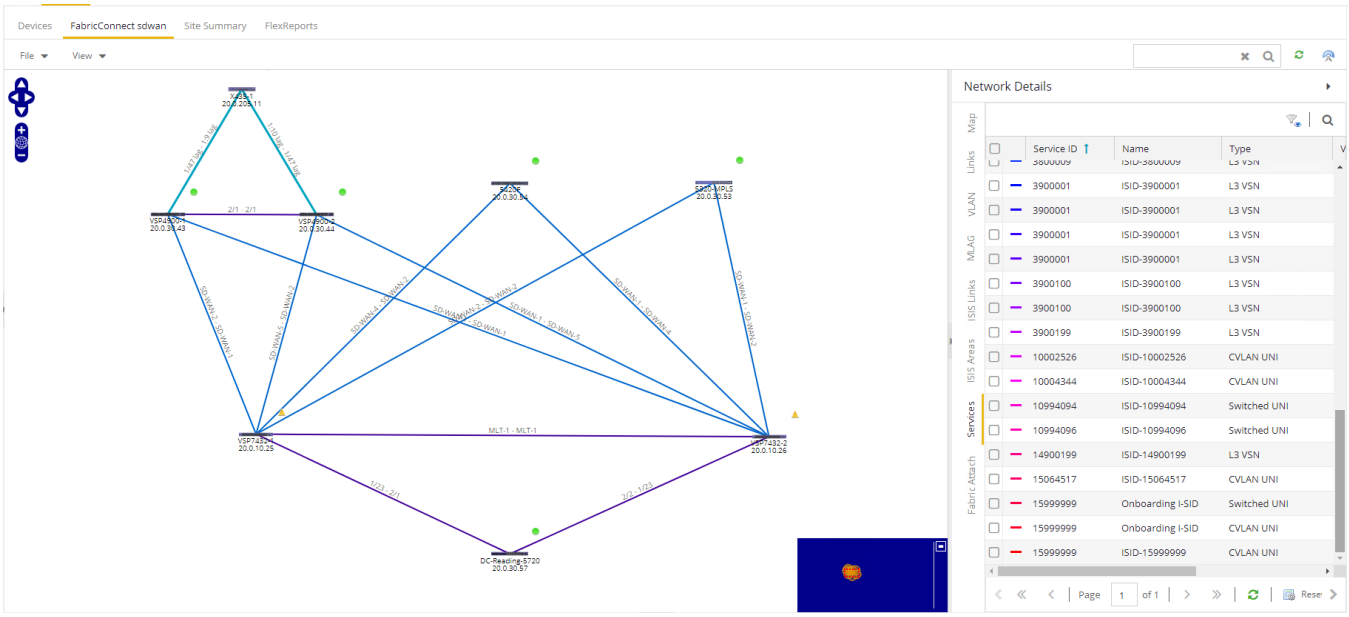


Figure 1: Topology map of Fabric over SD-WAN

Automate Daily Tasks

The full lifecycle of network management is supported by Site Engine. It supports the initial deployment planning stage with the use of configuration templates to predefine site, port, service, reference firmware, and fabric attributes, to the deployment stage with Zero-Touch Provisioning Plus (ZTP+). The ZTP+ capability enables the automated deployment of a new switch through templates and workflows. When new devices with ZTP+ enabled are connected, they are automatically discovered and can be added to Site Engine with minimal server configuration. In addition, the latest updates are automatically downloaded to the new device. Zero Touch Fabric Configuration automatically configures Shortest Path Bridging MAC (SPBM) and IS-IS without user intervention.

Site Engine provides automation for daily and on-demand operations, such as adding new services and VLANs. It extends zero-touch and a zero-trust network edge by combining the automation enabled through auto-sense ports, with both the security and automation enabled by remote authentication dial-in service (RADIUS) or NAC. The Auto-sense feature in Fabric works with Site Engine to dynamically configure the port to act as an IS-IS network-to-network interface (NNI), Fabric UNI (Flex-UNI), or voice (IP phone) interface, based on the Link Layer Discovery Protocol (LLDP) events. This automation results in significant reductions to configuration time and enhanced security.

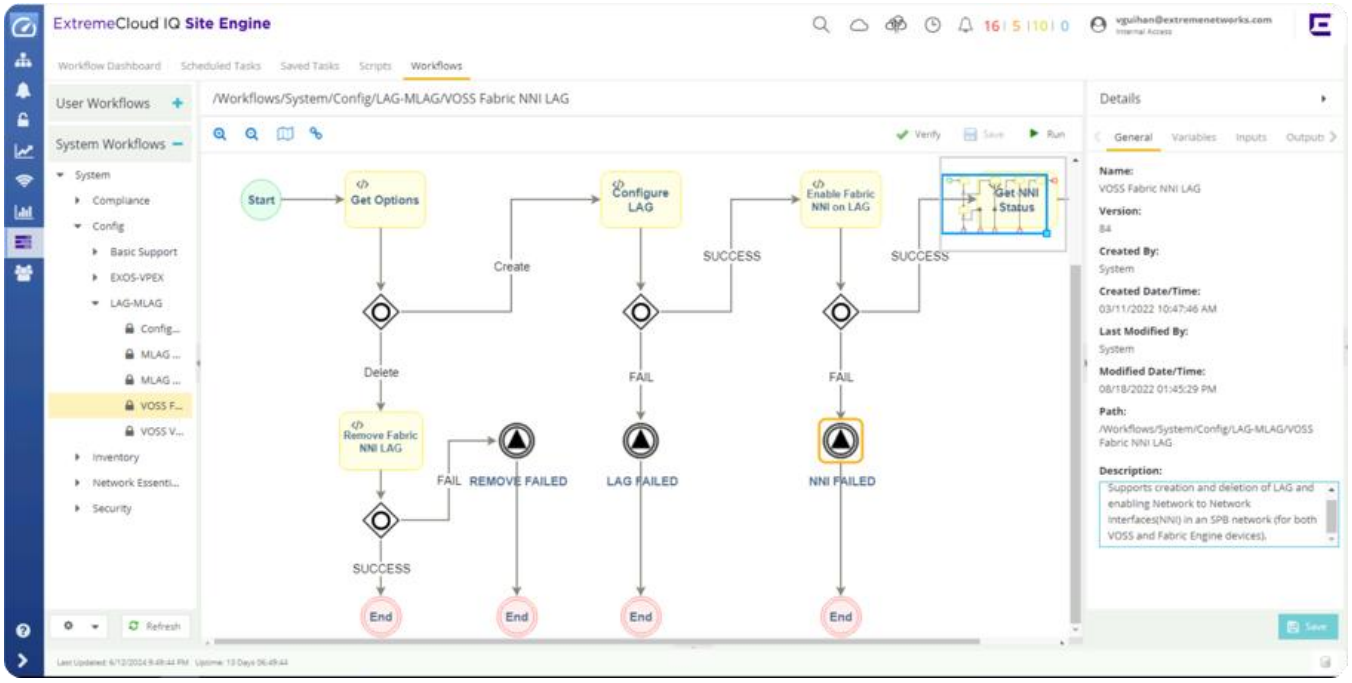


Figure 2: Example of a Fabric Configuration Workflow

The Workflow feature includes pre-defined and custom systems-defined workflows. This includes workflows for compliance, configuration, inventory, network essential, and security. Maintenance-related tasks (RMAs and service maintenance windows) can be implemented. Site Engine also supports configuration and firmware updates across third-party networking devices, reducing lengthy and error-prone manual onboarding and updates.

ExtremeCloud IQ Site Engine provides cross-domain workflow automation capabilities through an intuitive graphical approach to easily automate network tasks. It includes built-in automation and workflow tools and support for common scripting languages, such as Python. These features deliver the ability to create sequential execution of tasks in workflows for customized orchestration. Various settings in ExtremeCloud IQ Site Engine can be set through the API, and they can interact with both Extreme and non-Extreme devices. For example, a workflow can configure multiple wired, wireless, third-party, or a combination of devices with a single click. These capabilities help reduce CLI-based management, while alleviating the burden on IT personnel and the impacts of unintended downtime.

A workflow can be triggered by any event, such as when a threshold is reached or a Syslog message or trap is received, by a user action, or even by an external API call. The workflow can reconfigure the network or interact with third-party automation solutions. For example, if the reboot of a device is detected, technical logs and details can be gathered, and a help desk ticket can be created by the workflow itself. If a high CPU utilization is detected, the workflow can automatically gather additional information about the running processes.

Integrations

ExtremeCloud IQ Site Engine is integrated with key platforms from Extreme and third parties to streamline business processes. These integrations enable extended capabilities with ExtremeAnalytics, ExtremeControl, and ExtremeCloud IQ Controller. The benefits include more robust data analysis and better user experiences across both wired and wireless devices.

A comprehensive suite of open APIs is offered from Extreme's network infrastructure portfolio of switches and wireless APs. This includes the classic integration methods such as SNMP, Syslog, and more efficient integration methods such as REST-based APIs and the Swagger UI. Additional information regarding the ExtremeCloud IQ Site Engine API is available. ExtremeControl is integrated with major enterprise platforms, including solutions for network security, enterprise mobility management, analytics, cloud, and data centers. It also includes an API for customized integrations with key enterprise platforms.

Enhance Security and Compliance

ExtremeCloud IQ Site Engine enables the security of an organization's wired and wireless networks through in-depth visibility and control over users, devices, and applications. Security updates provided by Extreme Networks enhance compliance with security requirements. Flexible deployment options support a range of data security and compliance requirements and allow organizations to adapt over time.

Access Control

ExtremeControl is integrated with ExtremeCloud IQ Site Engine, and it is available with a separate subscription. When access security in ExtremeControl is enabled, it provides role-based NAC for all devices, including third-party networking and IoT devices. It provides a wide range of NAC features, such as captive portal support, automatic endpoint discovery and location tracking. It also facilitates the non-IT onboarding of users and devices. The application securely enables BYOD, guest access, and IoT device control to protect the network against external threats and to protect corporate data by proactively preventing unauthorized users and compromised endpoints from accessing the network. The service provides RADIUS, including RADIUS load balancers, and multiple RADIUS and lightweight directory access protocol (LDAP) groups.

Users can centrally manage and define granular policies to meet compliance obligations, and they can locate, authenticate, and apply targeted policies to users and devices. ExtremeControl is integrated with Extreme Networks' ecosystem of partners to expand network security and threat response. It is integrated with next-generation firewall solutions and can orchestrate endpoint isolation and remediation based on the alerts received.
The service shares contextual information such as users, IP address, and location for powerful policy enforcement at perimeter firewalls. The integration of ExtremeControl with Microsoft Entra ID extends the identify and network access authorization capabilities in the Entra ID family of products.

Flexible Deployment Options

ExtremeCloud IQ Site Engine allows IT organizations to transition to cloud-based network management at their own pace. It provides flexibility to manage networks in a local, on-premises mode and migrate to the cloud when ready. Site Engine works with Extreme Platform ONE to facilitate cloud-based network management of distributed devices and end-users. Additionally, ExtremeCloud IQ Site Engine can be deployed in an air-gapped mode to adhere to industry and regional data security and compliance requirements.

To define the shared details, users can select the device and network telemetry data forwarded from Site Engine to Extreme Platform ONE. There are four configurable options available for the data communicated from Site Engine:

1. Share data from Site Engine with Extreme Platform ONE
2. Do not share the end-system information with Extreme Platform ONE
3. Use Extreme Platform ONE as a license proxy only, no statistics are shared
4. Air gap mode, no internet connectivity is required

As an organization's strategy or requirements change, users can change the deployment model from air-gapped to connected mode and back with just a few clicks, without needing to change network hardware or firmware, reinstall software, or purchase a different subscription. Support for all deployment models is provided with uncompromised security for client data and options respecting data sovereignty requirements.

Product Specifications

Virtual Appliance Options

The ExtremeCloud IQ Site Engine virtual appliances must be deployed on a VMWare® or Hyper-V server with a disk format of VHDX.

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

Refer to the Release Notes for information on Virtual Appliance scalability.

Deployment Options for ExtremeCloud IQ Site Engines

- Red Hat Enterprise Linux 9.8
- VMware (64-bit Virtual Appliance) VMware ESXi versions 6.7, 7.0, and 8.0 Servers
- Hyper-V (64-bit Virtual Appliance) Hyper-V Server 2022, Hyper-V Server 2025
- Nutanix AHV: 20230302.101026, AOS: 6.8.1, Prism Central: 2024.2
- Universal Compute Platform 2130C

Deployment Options for ExtremeControl and ExtremeAnalytics

- VMware (64-bit Virtual Appliance) VMware ESXi versions 6.7, 7.0, and 8.0 Servers
- Hyper-V (64-bit Virtual Appliance) Hyper-V Server 2022, Hyper-V Server 2025
- Nutanix AHV: 20230302.101026, AOS: 6.8.1, Prism Central: 2024.2
- Universal Compute Platform 2130C

Supported Web Browsers

- Microsoft Edge, Mozilla Firefox, and Google Chrome

Support Services

Extreme offers a portfolio of services that adapts to your unique environment and technical support needs. Globally available technical support and professional services from our in-house team of experts provide the resiliency and optimization that accelerate your business and innovation.

Combined with Extreme Networks Platform ONE agentic support tools and workflows, Extreme Services helps you to anticipate issues and identify risks before they impact your business. For more information, visit our Services page.

Ordering Information

Part Number	Description
EP1-STD-TA-S-C-EW-1YR	Extreme Platform ONE Standard Networking Right-to-use and EW TAC OS Support for one (1) device of Tier A per year
EP1-STD-TA-S-C-PSS-1YR	Extreme Platform ONE Standard Networking Right-to-use and Partner Support Service (PSS) TAC OS Support for one (1) device of Tier A per year
EP1-STD-TB-S-C-EW-1YR	Extreme Platform ONE Standard Networking Right-to-use and EW TAC OS Support for one (1) device of Tier B per year
EP1-STD-TB-S-C-PSS-1YR	Extreme Platform ONE Standard Networking Right-to-use and Partner Support Service (PSS) TAC OS Support for one (1) device of Tier B per year
EP1-STD-TC-S-C-EW-1YR	Extreme Platform ONE Standard Networking Right-to-use and EW TAC OS Support for one (1) device of Tier C per year
EP1-STD-TC-S-C-PSS-1YR	Extreme Platform ONE Standard Networking Right-to-use and Partner Support Service (PSS) TAC OS Support for one (1) device of Tier C per year
EP1-STD-TD-S-C-EW-1YR	Extreme Platform ONE Standard Networking Right-to-use and EW TAC OS Support for one (1) device of Tier D per year
EP1-STD-TD-S-C-PSS-1YR	Extreme Platform ONE Standard Networking Right-to-use and Partner Support Service (PSS) TAC OS Support for one (1) device of Tier D per year
EP1-STD-T3RD-S-C-EW-1YR	Extreme Platform ONE Standard Networking Right-to-use and EW TAC OS Support for one (1) device of 3rd Party Tier per year
EP1-STD-T3RD-S-C-PSS-1YR	Extreme Platform ONE Standard Networking Right-to-use and PSS TAC OS Support for one (1) device of 3rd Party Tier per year

Note: Each managed device must be covered by the Extreme Platform ONE Standard subscription. For more details, check out the documentation.