FabricManager User Guide

04/2023
23.04.10
PN: 9037793-00

Legal Notices

Extreme Networks, Inc., on behalf of or through its wholly-owned subsidiary, Enterasys Networks, Inc., reserves the right to make changes in specifications and other information contained in this document and its website without prior notice. The reader should in all cases consult representatives of Extreme Networks to determine whether any such changes have been made.

The hardware, firmware, software or any specifications described or referred to in this document are subject to change without notice.

Trademarks

Extreme Networks and the Extreme Networks logo are trademarks or registered trademarks of Extreme Networks, Inc. in the United States and/or other countries.

All other names (including any product names) mentioned in this document are the property of their respective owners and may be trademarks or registered trademarks of their respective companies/owners.

For additional information on Extreme Networks trademarks, please see:
www.extremenetworks.com/company/legal/trademarks/

Contact

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

- Global Technical Assistance Center (GTAC) for Immediate Support
    - **Phone:** 1-800-998-2408 (toll-free in U.S. and Canada) or 1-603-952-5000. For the Extreme Networks support phone number in your country, visit: www.extremenetworks.com/support/contact
    - **Email:** support@extremenetworks.com. To expedite your message, enter the product name or model number in the subject line.
- GTAC Knowledge — Get on-demand and tested resolutions from the GTAC Knowledgebase, or create a help case if you need more guidance.
- The Hub — A forum for Extreme customers to connect with one another, get questions answered, share ideas and feedback, and get problems solved. This community is monitored by Extreme Networks employees, but is not intended to replace specific guidance from GTAC.
- Support Portal — Manage cases, downloads, service contracts, product licensing, and training and certifications.

Extreme Networks® Software License Agreement

This Extreme Networks Software License Agreement is an agreement ("Agreement") between You, the end user, and Extreme Networks, Inc. ("Extreme"), on behalf of itself and its Affiliates (as hereinafter defined and including its wholly owned subsidiary, Enterasys Networks, Inc. as well as its other subsidiaries). This Agreement sets forth Your rights and obligations with respect to the Licensed Software and Licensed Materials. BY INSTALLING THE LICENSE KEY FOR THE SOFTWARE ("License Key"), COPYING, OR OTHERWISE USING THE LICENSED SOFTWARE, YOU ARE AGREEING TO BE BOUND BY THE TERMS OF THIS AGREEMENT, WHICH INCLUDES THE LICENSE AND THE LIMITATION OF WARRANTY AND DISCLAIMER OF LIABILITY. IF YOU DO NOT AGREE TO THE TERMS OF THIS AGREEMENT, RETURN THE LICENSE KEY TO EXTREME OR YOUR DEALER, IF ANY, OR DO NOT USE THE LICENSED SOFTWARE AND CONTACT EXTREME OR YOUR DEALER WITHIN TEN (10) DAYS FOLLOWING THE DATE OF RECEIPT FOR A REFUND. IF YOU HAVE ANY QUESTIONS ABOUT THIS AGREEMENT, CONTACT EXTREME, Attn: LegalTeam@extremenetworks.com.

1. DEFINITIONS. "Affiliates" means any person, partnership, corporation, limited liability company, or other form of enterprise that directly or indirectly through one or more intermediaries, controls, or is controlled by, or is under common control with the party specified. "Server Application" shall refer to the License Key for software installed on one or more of Your servers. "Client Application" shall refer to the application to access the Server Application. "Licensed Materials" shall collectively refer to the licensed software (including the Server Application and Client Application), Firmware, media embodying the software, and the documentation. "Concurrent User" shall refer to any of Your individual employees who You provide access to the Server Application at any one time. "Firmware" refers to any software program or code imbedded in chips or other media. "Licensed Software" refers to the Software and Firmware collectively.
2. TERM. This Agreement is effective from the date on which You install the License Key, use the Licensed Software, or a Concurrent User accesses the Server Application. You may terminate the Agreement at any time by destroying the Licensed Materials, together with all copies, modifications and merged portions in any form. The Agreement and Your license to use the Licensed Materials will also terminate if You fail to comply with any term of condition herein.
3. GRANT OF SOFTWARE LICENSE. Extreme will grant You a non-transferable, non-exclusive license to use the machine-readable form of the Licensed Software and the accompanying documentation if You agree to the terms and conditions of this Agreement. You may install and use the Licensed Software as permitted by the license type purchased as described below in License Types. The license type purchased is specified on the invoice issued to You by Extreme or Your dealer, if any. YOU MAY NOT USE, COPY, OR MODIFY THE LICENSED MATERIALS, IN WHOLE OR IN PART, EXCEPT AS EXPRESSLY PROVIDED IN THIS AGREEMENT.
4. LICENSE TYPES.
    - *Single User, Single Computer*. Under the terms of the Single User, Single Computer license, the license granted to You by Extreme when You install the License Key authorizes You to use the Licensed Software on any one, single computer only, or any replacement for that computer, for internal use only. A separate license, under a separate Software License Agreement,

is required for any other computer on which You or another individual or employee intend to use the Licensed Software. A separate license under a separate Software License Agreement is also required if You wish to use a Client license (as described below).

- *Client*. Under the terms of the Client license, the license granted to You by Extreme will authorize You to install the License Key for the Licensed Software on your server and allow the specific number of Concurrent Users shown on the relevant invoice issued to You for each Concurrent User that You order from Extreme or Your dealer, if any, to access the Server Application. A separate license is required for each additional Concurrent User.

5. AUDIT RIGHTS. You agree that Extreme may audit Your use of the Licensed Materials for compliance with these terms and Your License Type at any time, upon reasonable notice. In the event that such audit reveals any use of the Licensed Materials by You other than in full compliance with the license granted and the terms of this Agreement, You shall reimburse Extreme for all reasonable expenses related to such audit in addition to any other liabilities You may incur as a result of such non-compliance, including but not limited to additional fees for Concurrent Users over and above those specifically granted to You. From time to time, the Licensed Software will upload information about the Licensed Software and the associated devices to Extreme. This is to verify the Licensed Software is being used with a valid license. By using the Licensed Software, you consent to the transmission of this information. Under no circumstances, however, would Extreme employ any such measure to interfere with your normal and permitted operation of the Products, even in the event of a contractual dispute.

6. RESTRICTION AGAINST COPYING OR MODIFYING LICENSED MATERIALS. Except as expressly permitted in this Agreement, You may not copy or otherwise reproduce the Licensed Materials. In no event does the limited copying or reproduction permitted under this Agreement include the right to decompile, disassemble, electronically transfer, or reverse engineer the Licensed Software, or to translate the Licensed Software into another computer language.

   The media embodying the Licensed Software may be copied by You, in whole or in part, into printed or machine readable form, in sufficient numbers only for backup or archival purposes, or to replace a worn or defective copy. However, You agree not to have more than two (2) copies of the Licensed Software in whole or in part, including the original media, in your possession for said purposes without Extreme's prior written consent, and in no event shall You operate more copies of the Licensed Software than the specific licenses granted to You. You may not copy or reproduce the documentation. You agree to maintain appropriate records of the location of the original media and all copies of the Licensed Software, in whole or in part, made by You. You may modify the machine-readable form of the Licensed Software for (1) your own internal use or (2) to merge the Licensed Software into other program material to form a modular work for your own use, provided that such work remains modular, but on termination of this Agreement, You are required to completely remove the Licensed Software from any such modular work. Any portion of the Licensed Software included in any such modular work shall be used only on a single computer for internal purposes and shall remain subject to all the terms and conditions of this Agreement. You agree to include any copyright or other proprietary notice set forth on the label of the media embodying the Licensed Software on any copy of the Licensed Software in any form, in whole or in part, or on any modification of the Licensed Software or any such modular work containing the Licensed Software or any part thereof.

7. TITLE AND PROPRIETARY RIGHTS

   a. The Licensed Materials are copyrighted works and are the sole and exclusive property of Extreme, any company or a division thereof which Extreme controls or is controlled by, or which may result from the merger or consolidation with Extreme (its "Affiliates"), and/or their suppliers. This Agreement conveys a limited right to operate the Licensed Materials and shall not be construed to convey title to the Licensed Materials to You. There are no implied rights. You shall not sell, lease, transfer, sublicense, dispose of, or otherwise make available the Licensed Materials or any portion thereof, to any other party.

   b. You further acknowledge that in the event of a breach of this Agreement, Extreme shall suffer severe and irreparable damages for which monetary compensation alone will be inadequate. You therefore agree that in the event of a breach of

this Agreement, Extreme shall be entitled to monetary damages and its reasonable attorney's fees and costs in enforcing this Agreement, as well as injunctive relief to restrain such breach, in addition to any other remedies available to Extreme.

8. PROTECTION AND SECURITY. In the performance of this Agreement or in contemplation thereof, You and your employees and agents may have access to private or confidential information owned or controlled by Extreme relating to the Licensed Materials supplied hereunder including, but not limited to, product specifications and schematics, and such information may contain proprietary details and disclosures. All information and data so acquired by You or your employees or agents under this Agreement or in contemplation hereof shall be and shall remain Extreme's exclusive property, and You shall use your best efforts (which in any event shall not be less than the efforts You take to ensure the confidentiality of your own proprietary and other confidential information) to keep, and have your employees and agents keep, any and all such information and data confidential, and shall not copy, publish, or disclose it to others, without Extreme's prior written approval, and shall return such information and data to Extreme at its request. Nothing herein shall limit your use or dissemination of information not actually derived from Extreme or of information which has been or subsequently is made public by Extreme, or a third party having authority to do so.

   You agree not to deliver or otherwise make available the Licensed Materials or any part thereof, including without limitation the object or source code (if provided) of the Licensed Software, to any party other than Extreme or its employees, except for purposes specifically related to your use of the Licensed Software on a single computer as expressly provided in this Agreement, without the prior written consent of Extreme. You agree to use your best efforts and take all reasonable steps to safeguard the Licensed Materials to ensure that no unauthorized personnel shall have access thereto and that no unauthorized copy, publication, disclosure, or distribution, in whole or in part, in any form shall be made, and You agree to notify Extreme of any unauthorized use thereof. You acknowledge that the Licensed Materials contain valuable confidential information and trade secrets, and that unauthorized use, copying and/or disclosure thereof are harmful to Extreme or its Affiliates and/or its/their software suppliers.

9. MAINTENANCE AND UPDATES. Updates and certain maintenance and support services, if any, shall be provided to You pursuant to the terms of an Extreme Service and Maintenance Agreement, if Extreme and You enter into such an agreement. Except as specifically set forth in such agreement, Extreme shall not be under any obligation to provide Software Updates, modifications, or enhancements, or Software maintenance and support services to You.

10. DEFAULT AND TERMINATION. In the event that You shall fail to keep, observe, or perform any obligation under this Agreement, including a failure to pay any sums due to Extreme, or in the event that you become insolvent or seek protection, voluntarily or involuntarily, under any bankruptcy law, Extreme may, in addition to any other remedies it may have under law, terminate the License and any other agreements between Extreme and You.

    a. Immediately after any termination of the Agreement or if You have for any reason discontinued use of Software, You shall return to Extreme the original and any copies of the Licensed Materials and remove the Licensed Software from any modular works made pursuant to Section 3, and certify in writing that through your best efforts and to the best of your knowledge the original and all copies of the terminated or discontinued Licensed Materials have been returned to Extreme.

    b. Sections 1, 7, 8, 10, 11, 12, 13, 14 and 15 shall survive termination of this Agreement for any reason.

11. EXPORT REQUIREMENTS. You are advised that the Software is of United States origin and subject to United States Export Administration Regulations; diversion contrary to United States law and regulation is prohibited. You agree not to directly or indirectly export, import or transmit the Software to any country, end user or for any Use that is prohibited by applicable United States regulation or statute (including but not limited to those countries embargoed from time to time by the United States government); or contrary to the laws or regulations of any other governmental entity that has jurisdiction over such export, import, transmission or Use.

12. UNITED STATES GOVERNMENT RESTRICTED RIGHTS. The Licensed Materials (i) were developed solely at private expense; (ii) contain "restricted computer software" submitted with restricted rights in accordance with section 52.227-19 (a) through (d) of the Commercial Computer Software-Restricted Rights Clause and its successors, and (iii) in all respects is proprietary data belonging

to Extreme and/or its suppliers. For Department of Defense units, the Licensed Materials are considered commercial computer software in accordance with DFARS section 227.7202-3 and its successors, and use, duplication, or disclosure by the U.S. Government is subject to restrictions set forth herein.

13. LIMITED WARRANTY AND LIMITATION OF LIABILITY. The only warranty that Extreme makes to You in connection with this license of the Licensed Materials is that if the media on which the Licensed Software is recorded is defective, it will be replaced without charge, if Extreme in good faith determines that the media and proof of payment of the license fee are returned to Extreme or the dealer from whom it was obtained within ninety (90) days of the date of payment of the license fee. NEITHER EXTREME NOR ITS AFFILIATES MAKE ANY OTHER WARRANTY OR REPRESENTATION, EXPRESS OR IMPLIED, WITH RESPECT TO THE LICENSED MATERIALS, WHICH ARE LICENSED "AS IS". THE LIMITED WARRANTY AND REMEDY PROVIDED ABOVE ARE EXCLUSIVE AND IN LIEU OF ALL OTHER WARRANTIES, INCLUDING IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE, WHICH ARE EXPRESSLY DISCLAIMED, AND STATEMENTS OR REPRESENTATIONS MADE BY ANY OTHER PERSON OR FIRM ARE VOID. ONLY TO THE EXTENT SUCH EXCLUSION OF ANY IMPLIED WARRANTY IS NOT PERMITTED BY LAW, THE DURATION OF SUCH IMPLIED WARRANTY IS LIMITED TO THE DURATION OF THE LIMITED WARRANTY SET FORTH ABOVE. YOU ASSUME ALL RISK AS TO THE QUALITY, FUNCTION AND PERFORMANCE OF THE LICENSED MATERIALS. IN NO EVENT WILL EXTREME OR ANY OTHER PARTY WHO HAS BEEN INVOLVED IN THE CREATION, PRODUCTION OR DELIVERY OF THE LICENSED MATERIALS BE LIABLE FOR SPECIAL, DIRECT, INDIRECT, RELIANCE, INCIDENTAL OR CONSEQUENTIAL DAMAGES, INCLUDING LOSS OF DATA OR PROFITS OR FOR INABILITY TO USE THE LICENSED MATERIALS, TO ANY PARTY EVEN IF EXTREME OR SUCH OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. IN NO EVENT SHALL EXTREME OR SUCH OTHER PARTY'S LIABILITY FOR ANY DAMAGES OR LOSS TO YOU OR ANY OTHER PARTY EXCEED THE LICENSE FEE YOU PAID FOR THE LICENSED MATERIALS.
Some states do not allow limitations on how long an implied warranty lasts and some states do not allow the exclusion or limitation of incidental or consequential damages, so the above limitation and exclusion may not apply to You. This limited warranty gives You specific legal rights, and You may also have other rights which vary from state to state.

14. JURISDICTION. The rights and obligations of the parties to this Agreement shall be governed and construed in accordance with the laws and in the State and Federal courts of the State of California, without regard to its rules with respect to choice of law. You waive any objections to the personal jurisdiction and venue of such courts. None of the 1980 United Nations Convention on the Limitation Period in the International Sale of Goods, and the Uniform Computer Information Transactions Act shall apply to this Agreement.

15. GENERAL.
    a. This Agreement is the entire agreement between Extreme and You regarding the Licensed Materials, and all prior agreements, representations, statements, and undertakings, oral or written, are hereby expressly superseded and canceled.
    b. This Agreement may not be changed or amended except in writing signed by both parties hereto.
    c. You represent that You have full right and/or authorization to enter into this Agreement.
    d. This Agreement shall not be assignable by You without the express written consent of Extreme. The rights of Extreme and Your obligations under this Agreement shall inure to the benefit of Extreme's assignees, licensors, and licensees.
    e. Section headings are for convenience only and shall not be considered in the interpretation of this Agreement.
    f. The provisions of the Agreement are severable and if any one or more of the provisions hereof are judicially determined to be illegal or otherwise unenforceable, in whole or in part, the remaining provisions of this Agreement shall nevertheless be binding on and enforceable by and between the parties hereto.
    g. Extreme's waiver of any right shall not constitute waiver of that right in future. This Agreement constitutes the entire understanding between the parties with respect to the subject matter hereof, and all prior agreements, representations,

statements and undertakings, oral or written, are hereby expressly superseded and canceled. No purchase order shall supersede this Agreement.

h. Should You have any questions regarding this Agreement, You may contact Extreme at the address set forth below. Any notice or other communication to be sent to Extreme must be mailed by certified mail to the following address:

Extreme Networks, Inc.
145 Rio Robles
San Jose, CA 95134 United States
ATTN: General Counsel

Table of Contents

Fabric Manager Installation

Install the Fabric Manager virtual machine (VM) to enable Fabric Manager in ExtremeCloud IQ - Site Engine.

Pre-Installation

The Fabric Manager is distributed in a deployable VMware-based .OVA template, which is similar to the other ZTP+ (Zero Touch Provisioning Plus)-based engines (for example,ExtremeControl).

The Fabric Manager supports two initial configuration modes for ExtremeCloud IQ - Site Engine discovery and registration:

- DHCP Mode
- Static Mode

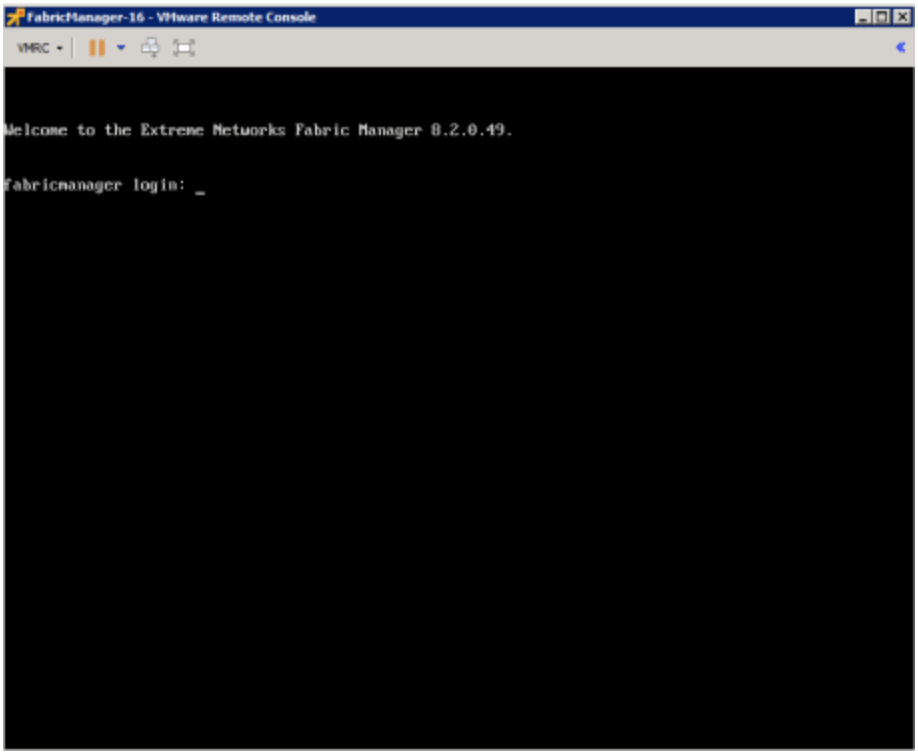
The DHCP mode is the default configuration mode during the Fabric Manager VM's initial startup. Use the static mode when providing a predefined set of networking configurations.

Fabric Manager Installation Static Mode

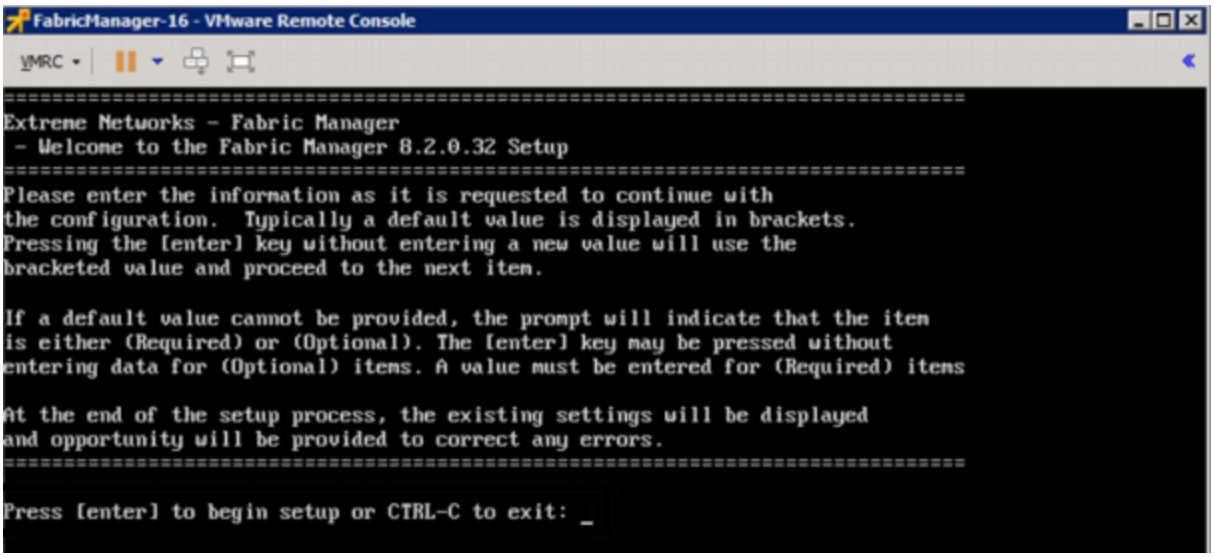
Fabric Manager begins installation in DHCP mode by default. Switch to static mode at any time during the initial installation by pressing the ENTER key.

Use the following instructions to install Fabric Manager in static mode:

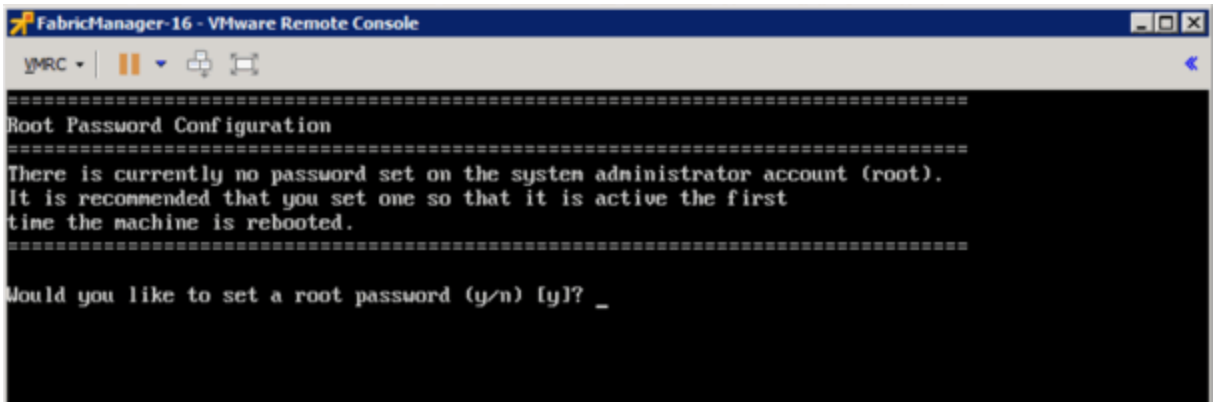
1. In the Console tab of the vSphere client, login as root with no password and press Enter.



2. Follow the installation process to complete installation of static mode:
    a. Begin the set-up.

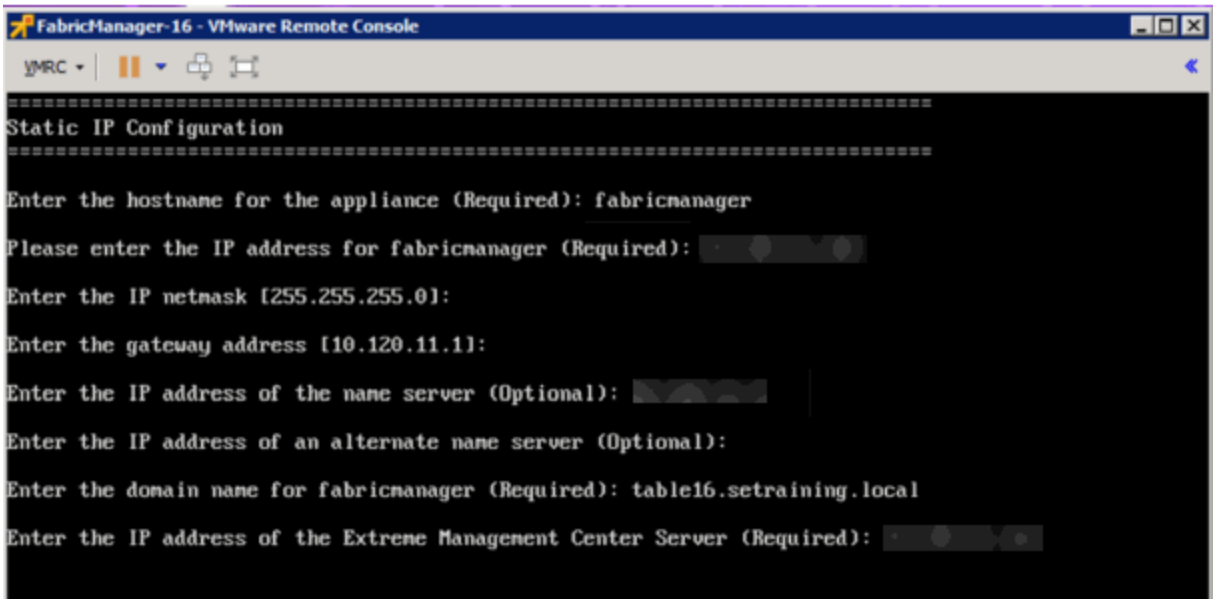


    b. Set a root password by entering y.



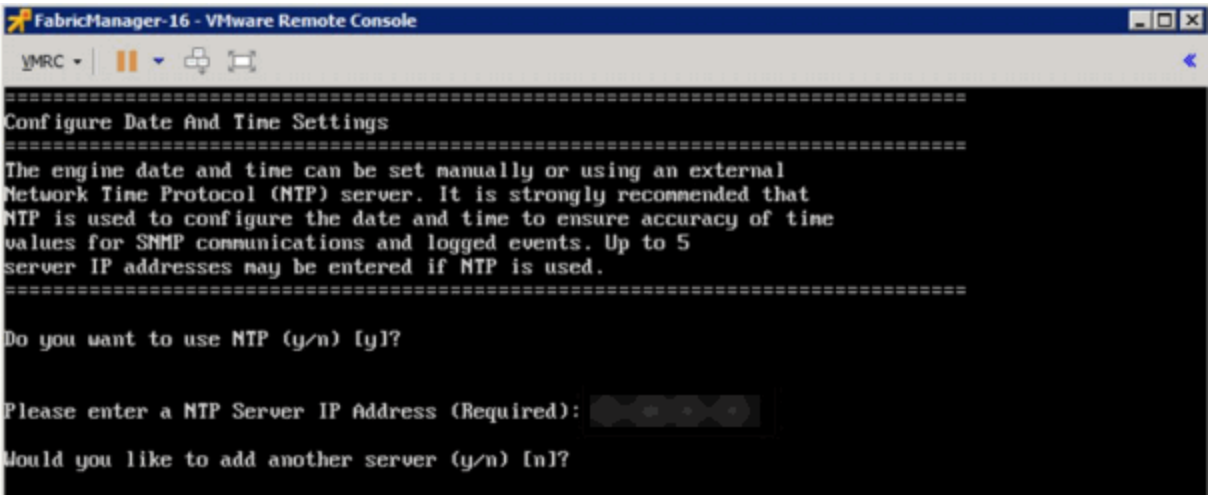
    c. Enter and re-type a UNIX password at the next prompt.

    The Static Configuration screen opens.



d. Enter a hostname.
e. Enter the IP address for the VM engine.
f. Enter the default IP Network netmask address.
g. Enter the default Gateway address.
h. Enter the IP address of the name server.
i. Enter the domain name specific to the table.
j. Enter the ExtremeCloud IQ - Site Engine server IP address.

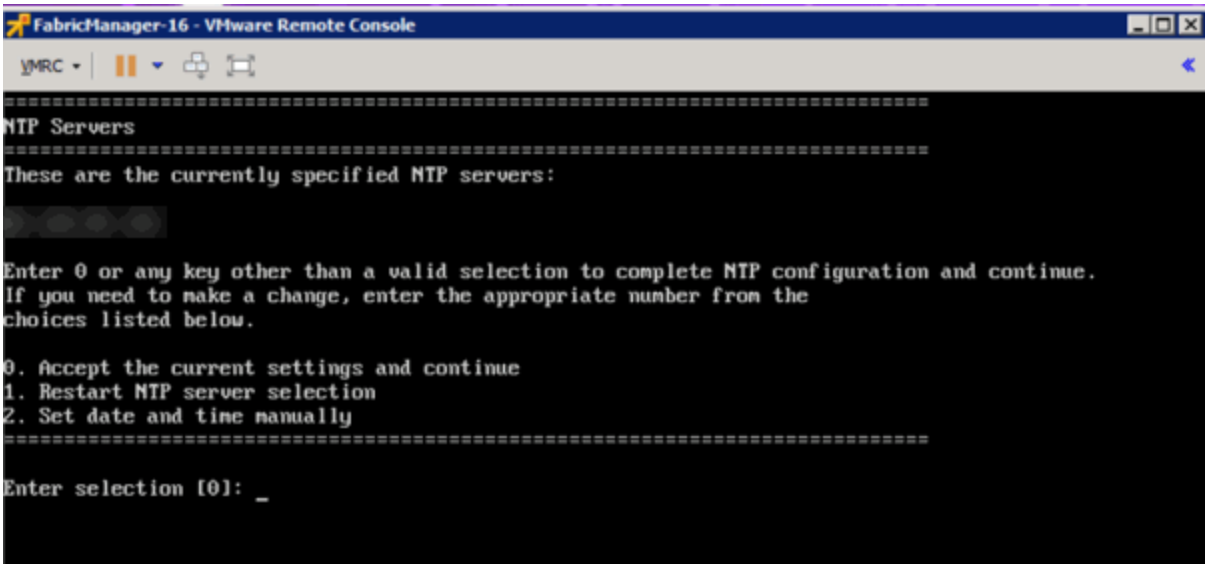
   The Date and Time Configuration screen opens.



k. Enter `y` at the next prompt to use NTP (Network Time Protocol).

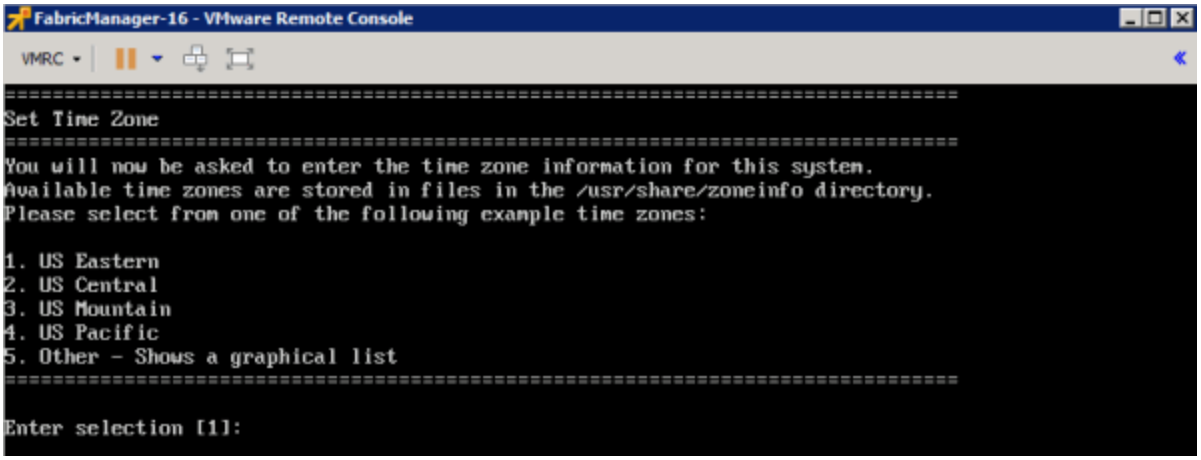
l. Enter the NTP Server IP Address.

m. Enter `n` at the next prompt to skip adding another NTP server. This is optional.



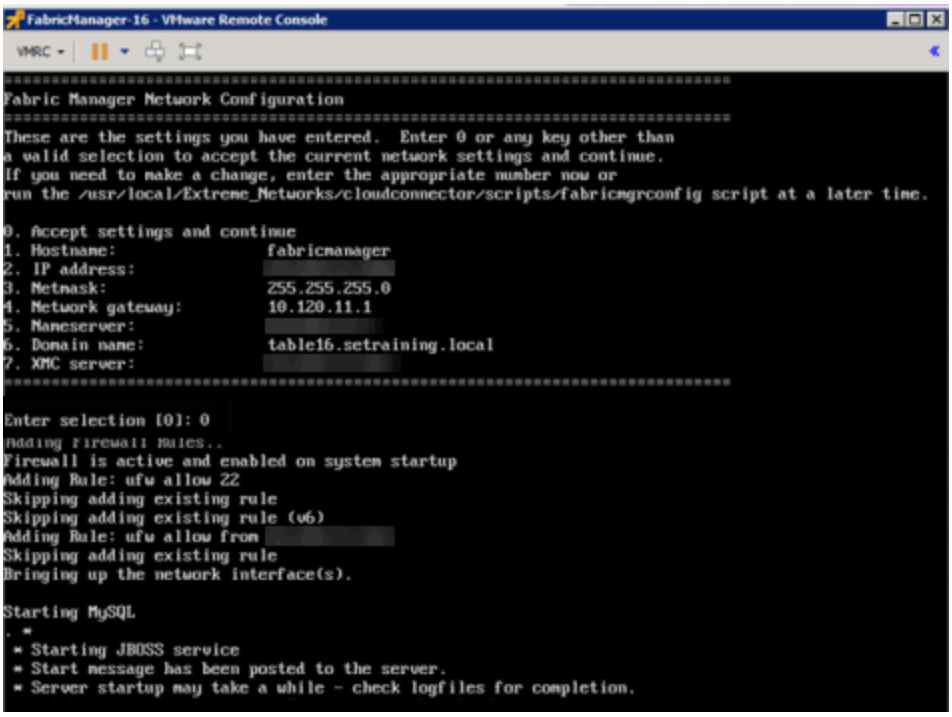
n. Enter the default `0` and accept the current settings and continue.

o. Select the correct Time Zone for your network.



p. Enter the number that corresponds to your time zone.

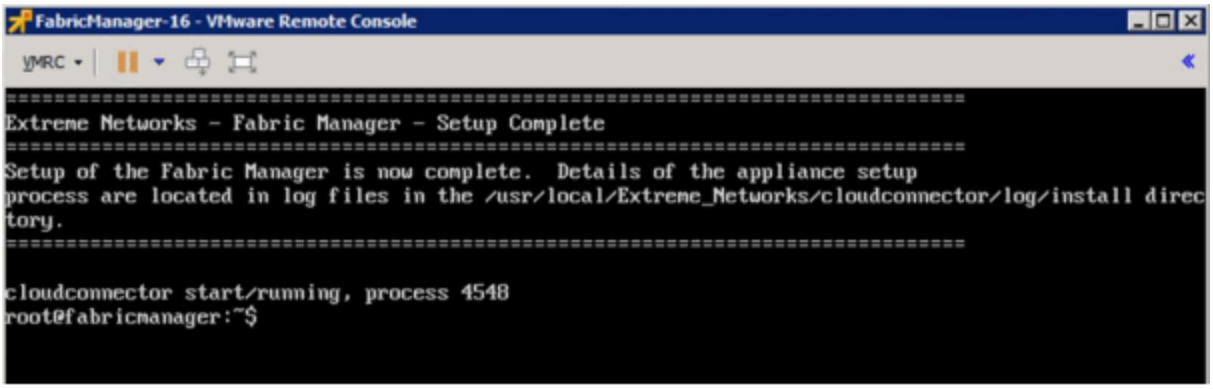
The Fabric Manager Network Configuration screen displays a summary of the configuration options you selected.



q. Enter 0 to confirm all the selections displayed are correct.

To modify any selection, enter the corresponding number of the item you want to change.

r. A Setup Complete message displays when installation is complete.



Adding Fabric Manager to ExtremeCloud IQ - Site Engine

After you install the Fabric Manager virtual machine (VM), you can add it to ExtremeCloud IQ - Site Engine and enable it via ZTP+ (Zero Touch Provisioning Plus) functionality.

NOTE: You need to upgrade the firmware in ExtremeCloud IQ - Site Engine to add and launch the Fabric Manager engine.

- How to Upgrade Firmware in ExtremeCloud IQ - Site Engine
- Fabric Manager ZTP+ Configuration in ExtremeCloud IQ - Site Engine
- ExtremeCloud IQ - Site Engine Fabric

Fabric Topology Definition on the Sites Tab

Use the **Fabric Topology Definition** tab to create a fabric topology definition, configure fabric topology settings, and review fabric topology paths and sites. You can also rename or delete a fabric topology definition.

Create a Topology Definition

You can create a Topology Definition on the **Sites** tab in ExtremeCloud IQ - Site Engine. After you create topology definitions, you can add them to sites in your network to build a fabric topology map.

To create a topology definition:

1. Access the **Devices** tab.
2. Select **Sites** from the left-panel drop-down list.
3. Navigate to **Topology Definitions** in the left-panel tree.
4. Right-click **Topology Definitions**.
5. Select **Create Topology Definition**.

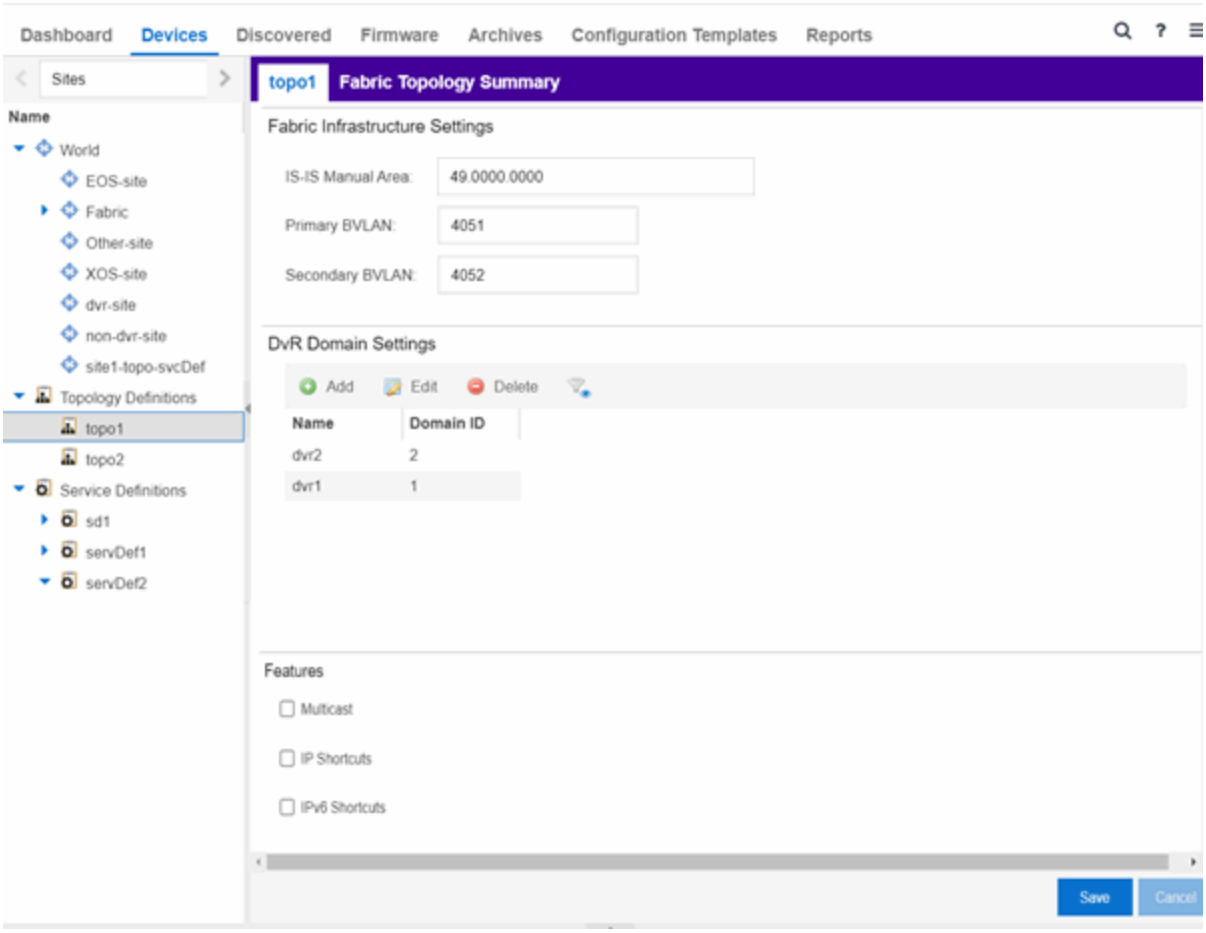
   The **Create Topology Definition** window opens.
6. Enter a name in the **Name** field.
7. Select **Fabric Connect** from the **Fabric Type** drop-down.
8. Select **OK** to create the topology definition.

Configure a Topology Definition

After the topology definition is created, it is available in the **Sites tab** left-panel tree. Select it to open a new right panel that includes the Fabric Name tab and a Fabric Summary tab.

Fabric Name Tab

Use the **Fabric Name** tab to configure the topology definition.



The Topology Definition tab includes the following sections:

Fabric Infrastructure Settings

The following fields are included in the Fabric Infrastructure Settings section:

- ISIS Manual Area - Use a xx.xxxx.xxxx.xxxx.xxxx.xxxx.xxxx format (1-13 bytes).
- Primary BVLAN - Enter the Primary Backbone VLAN (BVLAN).
- Secondary BVLAN - Enter the Secondary BVLAN.

DvR Domain Settings

The following fields are included in the DvR Domain Settings section:

- Name - The Domain name assigned to the DvR Domain. Select the down arrow to open the drop-down list to access sort, hide columns and search filter functionality for the domain name column.
- Domain ID - The identifying number assigned to the DvR Domain. Select the down arrow to open the drop-down list to access sort, hide columns and numeric filter functionality for the Domain ID column.

You can also Add, Edit, or Delete DvR Domain settings.

Features

The following fields are included in the Features section:

- Multicast - Select the check box to configure to distribute data to multiple recipients.
- IP Shortcuts - Select the check box to enable IPv4 Shortcuts for the topology definition.
- IPv6 Shortcuts - Select the check box to enable IPv6 Shortcuts for the topology definition.

Select **Save** to save the topology definition settings you selected.

After the topology definition is created and configured, you can apply it to a site within your network. After fabric topologies have been assigned to a site, they cannot be deleted.

Fabric Summary tab

The Fabric Summary tab lists any fabric topologies you have created and the sites to which they are assigned.

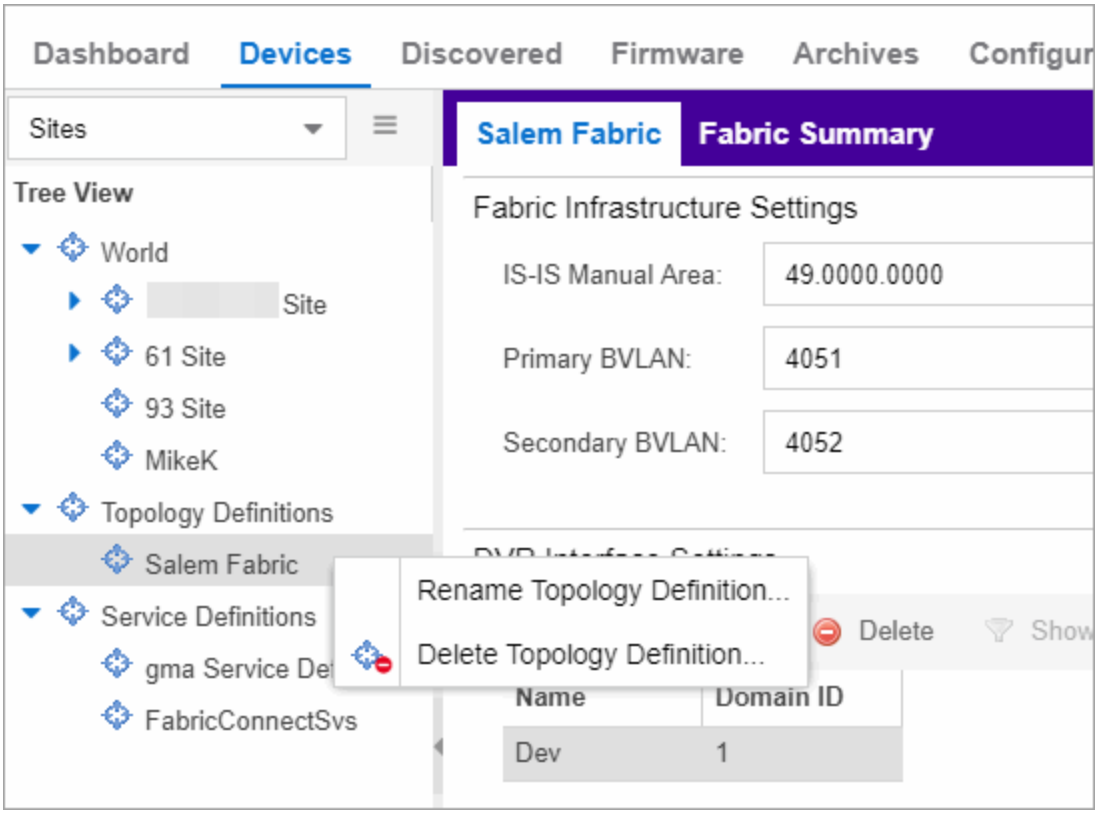
Rename a Topology Definition

After a topology definition has been created and configured, you can change or modify its name.

To rename a topology definition:

1. Open the **Devices** tab.
2. Select **Sites** from the left-panel tree drop-down list.
3. Expand **Topology Definitions** in the left-panel.

4. Right-click the topology definition you are renaming.



5. Select **Rename Topology Definition**.
6. Enter a new name in the **Name** field.
7. Select **OK** to change the topology name.

Delete a Topology Definition

After a topology definition has been created and configured, you can delete it; however, a topology definition cannot be deleted if it has been assigned to a site.

To delete a topology definition:

1. Open the **Devices** tab.
2. Select **Sites** from the left-panel tree drop-down list.
3. Expand the **Topology Definitions** in the left-panel.
4. Right-click the topology definition you are deleting.
5. Select **Delete Topology Definition**.
6. Select **Yes** to delete the topology definition you selected.

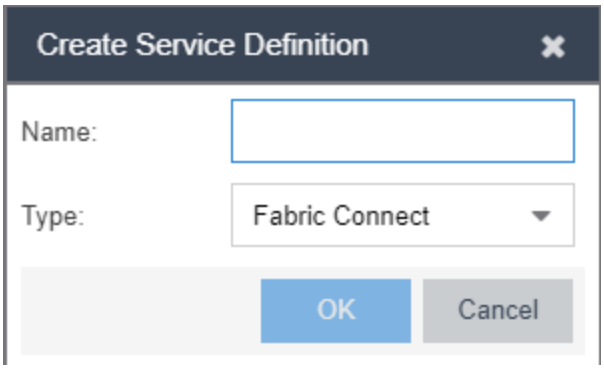
How to Create a Fabric Service Definition

You can create a service definition in the **Sites tab** in ExtremeCloud IQ - Site Engine. Service definitions display information configured in service applications definitions. When created, service definitions are added to sites in your network and are used to build a fabric topology map.

Create a Service Definition

To create a service definition:

1. Open the **Devices** tab.
2. Select **Sites** from the left-panel drop-down list.
3. Select **Service Definitions** in the left-panel.
4. Right-click **Service Definitions**.
5. Select **Create Service Definition**.



   The **Create Service Definition** window opens.
6. Enter a name in the **Name** field.
7. Select **Fabric Connect** from the **Type** drop-down list.
8. Select **OK** to create the service definition.

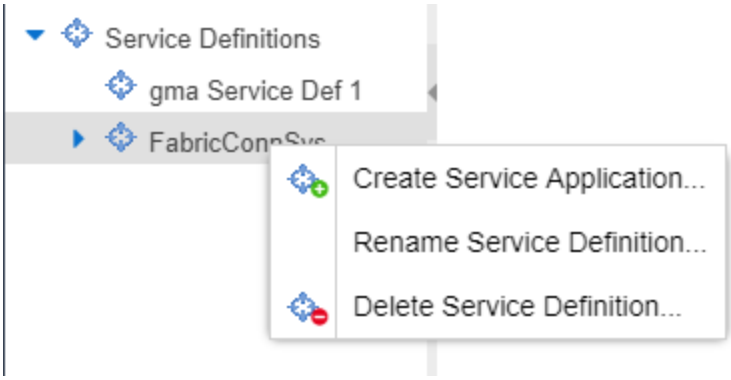
After the service definition is created and configured, you can apply it to a site within your network. When fabric services have been assigned to a site, they cannot be deleted.

Service Definition Panel

After the service definition is created, it is available in the left-panel tree. Select it to open a new right panel that includes a **Services** tab and a **Service Summary** tab.

Rename a Service Definition

After a service definition has been created and configured, you can change or modify its name.

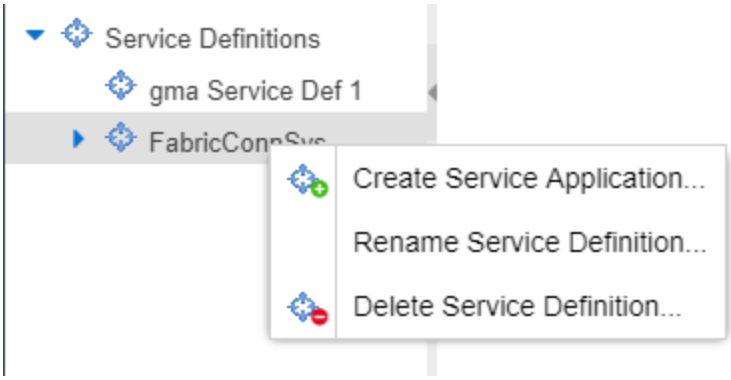


To rename a service definition:

1. Open the **Devices** tab.
2. Select **Sites** from the left-panel tree drop-down list.
3. Expand **Service Definitions** in the left-panel.
4. Right-click the service definition you are renaming.
5. Select **Rename Service Definition**.
6. Enter a new name in the **Name** field.
7. Select **OK** to rename the service definition.

Delete a Service Definition

When a service definition has been created and configured, you can delete it; however, a service definition or any of its associated service applications cannot be deleted if it has been assigned to a site.



To delete a service definition:

1. Open the **Devices** tab.
2. Select **Sites** from the left-panel drop-down list.
3. Expand **Service Definitions** in the left-panel.
4. Right-click the service definition you are deleting.
5. Select **Delete Service Definition**.
6. Select **Yes** to delete a service definition.

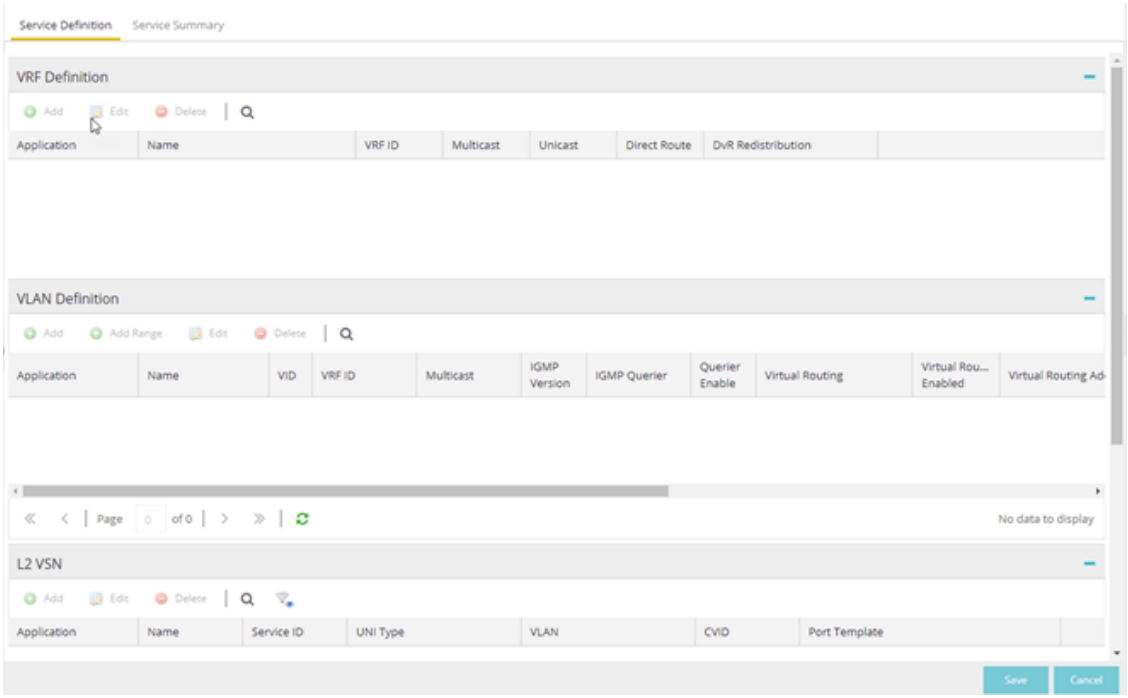
For information on related topics:

- Services
- Fabric
- Sites
- Devices

Services

The **Services** tab displays virtual routing and forwarding functionality configured as part of a service application, the virtual local area networks defined for the service application, as well as all of the services included in a service application or all of the services included in a service definition, depending if you select a service application or a service definition in the left-panel, respectively.

The **Services** tab is included in the **Sites** tab.



The Services tab includes three tables:

- VRF Definition — Create and configure VRF (Virtual Routing and Forwarding) definitions for the service application. VRFs allow for networking paths to be segmented without using multiple devices.
- VLAN Definition — Create and configure VLAN (Virtual Local Area Network) definitions for the service application.
- L2 VSN — Configure the L2 Virtual Services Networks (VSNs).
- L3 VSN — Configure the L3 Virtual Services Networks (VSNs).

VRF Definition

The VRF Definition table allows you to configure virtual routing and forwarding definitions included as part of the service.

Name
The name of the VRF definition.

VRF ID
The ID number assigned to the VRF definition.

VLAN Definition

The VLAN Definition table allows you to configure virtual local area network definitions included as part of the service.

Name
The name of the VLAN definition.

VID
The ID number assigned to the VLAN.

VRF ID
The ID number assigned to the VRF definition.

Multicast
Indicates the service sends IP packets to a group of hosts on the network.

IGMP Version
Indicates which version of IGMP is utilized on the port (Version 1 or Version 2).

IGMP Querier
The address of the IGMP Querier. This feature is used when there is no multicast router in the VLAN to originate the queries.

Querier Enable
Indicates whether an IGMP Query is enabled.

Virtual Routing

Displays the version of VRRP the default gateway is using:

- NONE — Virtual routing is not configured on the VLAN.
- VRRPv2 — VRRP version 2 is configured on the VLAN. VRRP version 2 only supports IP addresses in IPv4 format.
- VRRPv3 — VRRP version 3 is configured on the VLAN. VRRP version 3 supports IP addresses in both IPv4 and IPv6 formats.
- DvR - DvR functionality is configured on the VLAN.

NOTE: Virtual Routing is only supported on VOSS/Fabric Engine devices.

Virtual Routing Enable

Indicates whether virtual routing is enabled for the VLAN.

Virtual Routing Address

The IP address for the virtual routing interface. The Virtual Routing address must be in the same subnet as the VLAN subnet address.

VRRP ID

An identifier devices use to determine peer devices that participate in a virtual routing interface.

VRRP Priority

A value used by VRRP peers to determine the role of each of the devices in the VLAN. The default value is 100. The device with the largest value is assigned the role of Master. For example, in a VLAN with two routers, one with a VRRP Priority of 200 and one with a VRRP Priority of 100, the router with a VRRP Priority of 200 becomes the Master. In the event of identical priority numbers, the devices use the MAC address to determine priority.

VRRP Backup Master

This option determines if the backup router is able to forward traffic independently outside of the VLAN (enabled), or must forward the traffic to the Master router before it is forwarded outside of the VLAN (disabled).

VRRP Advertisement Interval

Indicates frequency (in seconds) that protocol packets are sent from the virtual router in the VLAN.

VRRP Hold Down Timer

Indicates the amount of time (in hundredths of a second) that the backup router waits for the primary router to respond before it becomes the primary router.

DHCP Snooping

Indicates whether DHCP snooping is enabled for the VLAN. DHCP Snooping is a Layer 2 security feature, that provides network security by filtering untrusted DHCP messages received from the external network causing traffic attacks within the network. DHCP Snooping is based on the concept of trusted versus untrusted switch ports. Switch ports configured as trusted can forward DHCP Replies, and the untrusted switch ports cannot. DHCP Snooping acts like a firewall between untrusted hosts and DHCP servers.

ARP Inspection

Indicates whether ARP inspection is enabled. Dynamic ARP Inspection (DAI) is a security feature that validates ARP packets in the network. Without DAI, a malicious user can attack hosts, switches, and routers connected to the Layer 2 network by poisoning the ARP caches of systems connected to the subnet, and intercepting traffic intended for other hosts on the subnet. DAI prevents these attacks by intercepting, logging, and discarding the ARP packets with invalid IP to MAC address bindings. The switch dynamically builds the address binding table from the information gathered from the DHCP requests and replies when DHCP Snooping is enabled. The switch pairs the MAC address from the DHCP request with the IP address from the DHCP reply to create an entry in the DHCP binding table. When you enable DAI, the switch filters ARP packets on untrusted ports based on the source MAC and IP addresses seen on the switch port. The switch forwards an ARP packet when the source MAC and IP address matches an entry in the address binding table. Otherwise, the switch drops the ARP packet.

NOTE: DHCP Snooping must be enabled to use ARP Inspection.

Service Application Name

The Service Application Name table displays all of the services included in a service application or all of the services included in a service definition, depending if you select a service application or a service definition in the left-panel, respectively. The Services tab is included in the Sites tab.

Services are created within service applications. You can include multiple services within an application. Service applications are then included within service definitions. You can also include multiple service applications within a service definition. A service definition that includes a complete set of services is then assigned to a site, which configures the fabric-enabled devices within that site.

The Services tab is only configurable when you select a service application. The services displayed when selecting a service definition are read-only.

L2 VSN

Name

The name of the Layer 2 service.

Service ID

The I-SID, which is the system-defined ID number assigned to the fabric service.

UNI Type

The User-Network-Interface (UNI) of the fabric service. The following interface types are available:

- Switched — A VLAN-ID and a port (VID, port) mapped to a Layer 2 VSN I-SID. With UNI type, VLAN-IDs can be reused on other ports and mapped to different ISIDs.
- Transparent - A physical port maps to a Layer 2 VSN I-SID (all traffic through the port, 802.1Q tagged or untagged, ingress and egress maps to the I-SID).

NOTE: All VLANs on a Transparent Port UNI interface now share the same single MAC learning table of the Transparent Port UNI I-SID.

- CVLAN — a platform customer VLAN-ID.

CVLAN

The customer VLAN-ID of the associated CVLAN UNI type.

VLAN

The VLAN assigned to the fabric service.

CVID

Specifies the customer VLAN ID of the associated switched UNI port.

AutoSense Service Type

Defines if the L2 VSN service is auto-assigned by the switch-level AutoSense detection. The following types are available:

- AP Untagged — If the AutoSense feature detects Access Point, then this service is automatically assigned to the port.
- Camera Untagged — If the AutoSense feature detects Camera then this service is automatically assigned to the port.
- Voice Untagged — If the AutoSense feature detects a VoIP device then this service is automatically assigned to the port.
- Voice Tagged — If the AutoSense feature detects a VoIP device then this service is automatically assigned to the port.
- Proxy Switch Auth Tagged — If the AutoSense feature detects a Fabric Attach switch capable of authenticating (ERS devices) then this service is automatically assigned to the port.
- Proxy Switch No Auth Untagged — If the AutoSense feature detects a Fabric Attach switch is not capable of authenticating (EXOS/Switch Engine devices) then this service is automatically assigned to the port.
- Proxy Switch Auth & Proxy Switch No Auth — If the AutoSense feature detects any physical Fabric Attach switch (ERS/EXOS/Switch Engine device) then this service is automatically assigned to the port.
- Data Untagged — If the AutoSense feature does not detect a device type then this service is automatically assigned to the port.
- None — AutoSense is not related to this L2VSN service.

NOTE: Each AutoSense Service Type can only be used once on a switch. The switch cannot use two different service IDs with the same AutoSense Service Type.

AutoSense Service CVID

The AutoSense Service CVID value defines the 802.1q VLAN tag sent from the switch to the device. If the AutoSense Service Type is Voice Tagged or Proxy Switch Auth Tagged or Proxy Switch Auth & Proxy Switch No Auth then AutoSense Service CVID must be defined. The value range is 1-4094.

Port Template

If the UNI Type is Switched or Transparent you can select from the Global Port templates to define the purpose of the port.

L3 VSN

Name

The name of the Layer 3 service.

Service ID

The I-SID, which is the system-defined ID number assigned to the service.

VRF

Select the virtual routing and forwarding definition included as part of the service.

Multi Cast

Select to indicate that the service sends IP packets to a group of hosts on the network.

Unicast

Select to indicate that the service sends IP packets to a single recipient on the network.

Direct Route

Select to indicate that the service sends IP packets directly to another device without going through a third device.

Fabric

The ExtremeCloud IQ - Site Engine Fabric technology is a solution to manage your domains seamlessly and interdependently across both physical and virtual servers, storage, and networks. It is designed to be highly efficient, flexible enough to adapt to your network's varying traffic volume, and easily maintained with minimal intervention. You can provision Fabric functionality on the Sites tab in ExtremeCloud IQ - Site Engine.

For additional information about Fabric functionality, see the *Configuring Fabric Basics and Layer 2 Services on the VOSS Operating System Software VSP 8600* guide for the latest VSP 8600 release.

ExtremeCloud IQ - Site Engine's fabric solution consists of two major components:

- Fabric Manager — A virtual engine that provides ExtremeCloud IQ - Site Engine with fabric topology information and allows you to configure fabric functionality on your fabric-enabled devices.
- Fabric Tab — The tab within ExtremeCloud IQ - Site Engine that allows you to view and configure the fabric functionality on your devices.

NOTE: Beginning with ExtremeCloud IQ - Site Engine version 8.5.5, the Ubuntu Operating System has upgraded to version 18.04.5 for the Fabric Manager.

The Fabric Manager engine must be installed and running on your network for the Fabric tab in ExtremeCloud IQ - Site Engine to receive and display fabric topology information.

Once the Fabric Manager engine is running in ExtremeCloud IQ - Site Engine, the Fabric tab on the Devices tab displays information about the fabric topologies currently configured on your devices.

NOTES: The following device types support fabric functionality:

ERS35xx with firmware version 5.3.7 and later, ERS36xx with firmware version 6.2.0 and later, ERS48xx with firmware version 5.12.0 and later, ERS49xx with firmware version 7.6.0 and later, ERS59xx with firmware version 7.6.0 and later, VSP7024 with firmware version 10.4.6 and later, VSP4xxx with firmware version 6.1.3 and later, VSP7xxx with firmware version 6.1.3 and later,VSP8xxx with firmware version 6.1.3 and later

For minimum requirements, see ExtremeCloud IQ - Site Engine Configuration and Requirements.

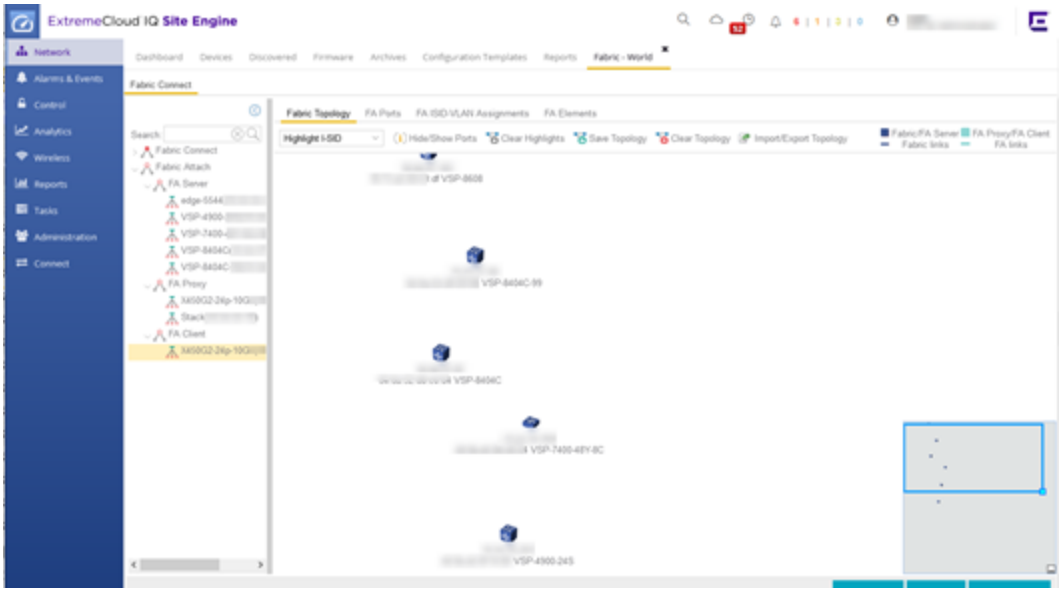
Accessing Fabric in ExtremeCloud IQ - Site Engine

After adding the Fabric Manager engine in ExtremeCloud IQ - Site Engine, view the fabric topologies configured on your devices on the Fabric tab.

To access the Fabric tab:

1. Open the **Devices** tab.
2. Select **Sites** from the left-panel drop-down list.
3. Right-click a site in the left-panel tree.
4. Select **More Views** > **Fabric Topology** from the menu.

   The **Fabric** tab opens.



Fabric Tab

The **Fabric** tab includes three sub-tabs:

- Fabric Topology — Displays the fabric topologies configured on your fabric-enabled devices.
- FA Ports — Displays the ports on which fabric is configured.
- FA ISID-VLAN Assignments — Allows you to view Virtual Extensible LANs (VXLANs) that tunnel Layer 2 traffic over a Layer 3 network in the fabric topologies you configure.

For information on related topics:

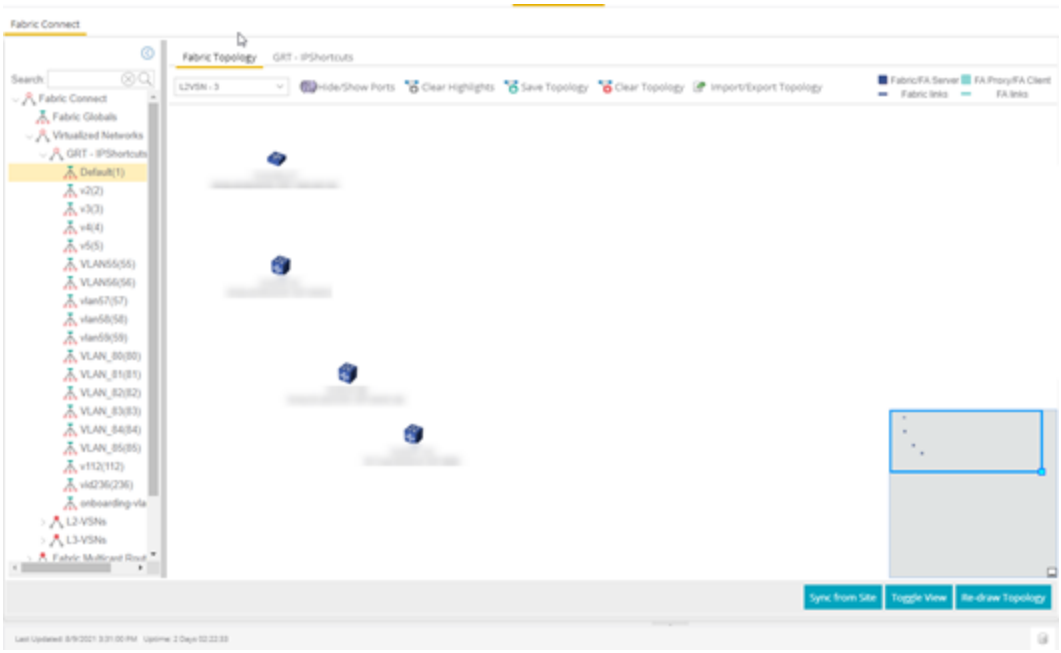
- Services
- Service Summary
- Fabric Connect
- Fabric Assist

Fabric Connect

ExtremeCloud IQ - Site Engine's **Fabric Connect** within the Fabric Manager engine displays your network's fabric technology and extended fabric functionality. Fabric Connect uses Fabric Topology templates that allow you to view and to configure SPBm (Shortest Path Bridging), based L2 and L3 Virtual Services Networks (VSNs), as well as IP-shortcut based VSNs. The Fabric Attach extends Fabric technology functionality to network elements or hosts that are not SPB-capable.

The Fabric Connect tab allows you to view topologies with the fabric-enabled sites in your network. Select the **Toggle View** button to display fabric services for individual devices.

NOTE: Fabric Connect uses Fabric Topology templates that define the topologies, services and service applications that comprise the Fabric Topology. Create the topology and service definitions via the Sites tab before you assign the Fabric Connect Topology to a site and access the **Fabric Connect** tab.



The Fabric Connect tab is divided into two sections: the left-panel tree view and a Fabric Topology right-panel map view.

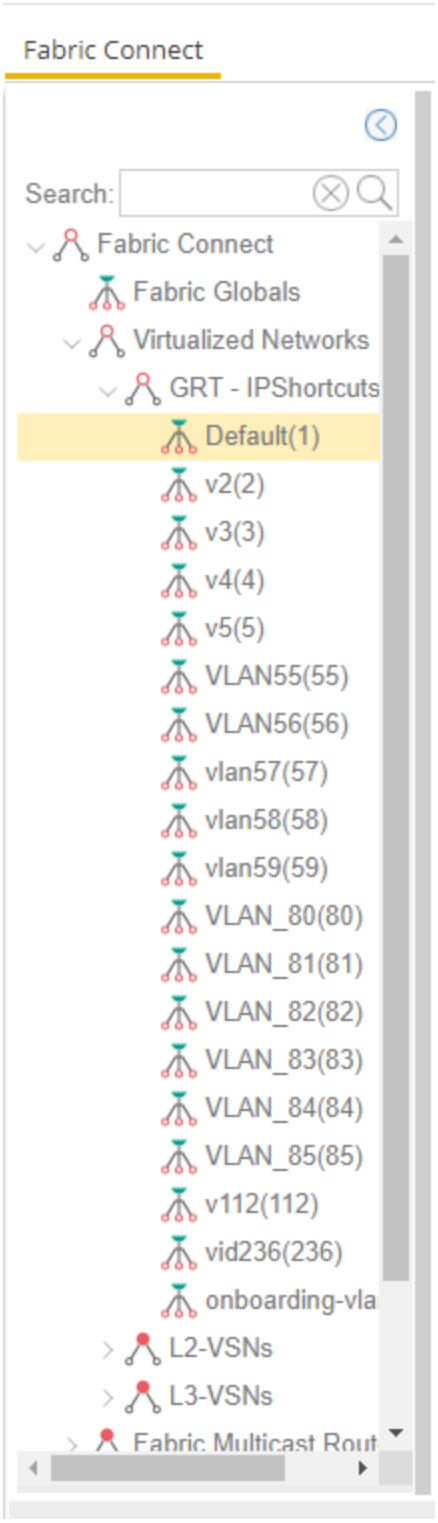
Left-Panel Tree

Beginning in version 23.04.10, ExtremeCloud IQ - Site Engine supports two Fabric technology infrastructures: Fabric Connect and Fabric Attach (FA). The left-panel tree includes Fabric

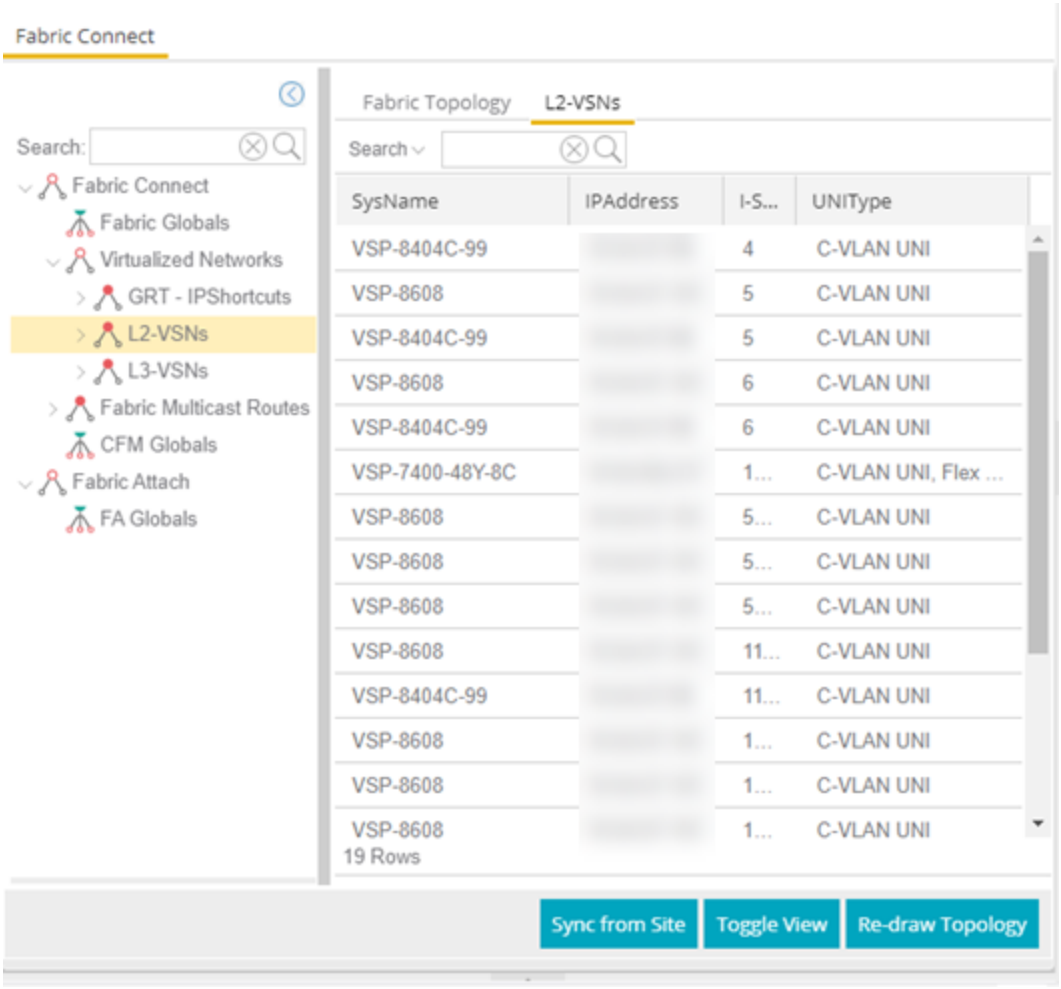
Connect and Fabric Attach folders that expand to display all fabric services you have configured in your network.

Fabric Connect Folder

Select the Fabric Connect tab to display the fabric topologies configured on the devices in the site.



Select a service in the Fabric Connect folder to open a fabric topology map and a service name tab in the right panel. The map displays the devices enabled with the services you selected and the service name tab displays a table with details about that service.



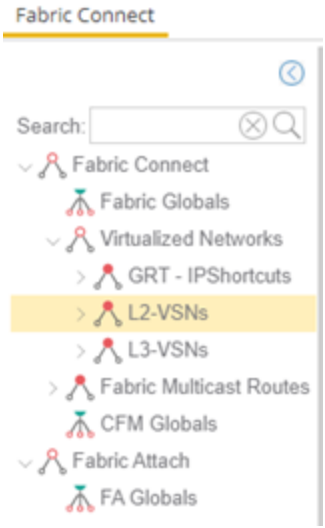
Select the **Toggle View** button to display Fabric Connect fabric services for individual devices.

Fabric Attach Folder

The Fabric Attach (FA) extends Fabric technology functionality to network devices that are not SPB-capable. The Fabric Attach tab displays global, server and proxy capable services for your network and devices.

NOTE: You can enable Fabric Attach on the following switches:

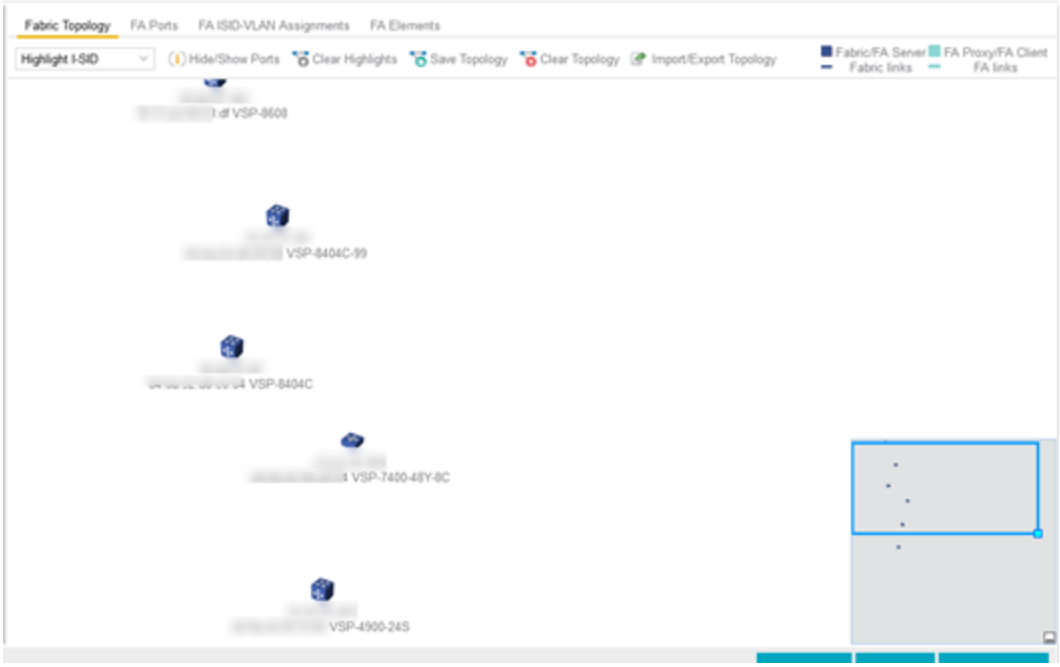
FA Server — for VOSS/Fabric Engine, ERS 49xx v5.9.2 and later, ERS 4850 v5.9.2 and later, and ERS 59xx series devices; FA Proxy (client proxy) — for ERS 35xx, ERS 48xx, ERS 49xx, ERS 55xx, ERS 56xx, ERS 59xx, and VSP 70xx series devices; FA Standalone Proxy (client proxy) — for ERS 35xx, ERS 48xx, ERS 55xx, ERS 56xx, ERS 59xx, and VSP 70xx series devices



Select a service in the Fabric Attach folder to open a fabric topology map and a VSN tab in the right panel. The map displays the devices enabled with the service you selected and the VSN Home tab displays a table with details about the VSNs enabled on the site. Select the **Toggle View** button to display Fabric Attach services for individual devices.

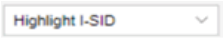
Right-Panel Topology Map

The Fabric Topology panel includes the **Fabric Topology** tab that displays a topology map of the fabric-enabled sites or devices in your network. You can use the topology map to gain a high-level view of your network, or to view detailed information about devices and links in the topology. Drag your device icons in the topology map to rearrange the map. Additionally, you can modify and save your map layouts in the Fabric Topology tab.



Topology Tab Tools

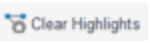
The Fabric Topology tab includes the following tools:

Fabric Service 

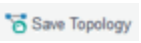
Lists fabric services in your network. Select a service from the drop-down list to display it in the topology map.

Hide/Show Ports

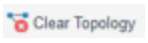
Use to hide or display fabric enabled ports in your network.

Clear Highlights 

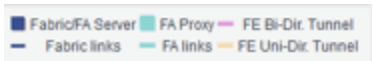
Use to clear existing highlights on the topology map.

Save Topology 

Use to save your topology map.

Clear Topology 

Use to remove the devices in your topology map.

Color Legend 

The types of fabric services are coded by colors in the topology map.

Topology Tab Buttons

The Fabric Topology tab also includes the following buttons that allow you to further manipulate the fabric service and topology data:

Sync From Site
Use to copy the fabric service configuration for the site to all the devices in the map.

Toggle View
Select to display fabric topology, services and tables for individual devices.

Re-draw Topology
Select to display an alternate topology arrangement.

Help
Select to access ExtremeCloud IQ - Site Engine help.

For information on related topics:

- Services
- Service Summary
- Sites
- Devices
- Fabric Assist

Fabric Assist

The purpose of Fabric Assist is to help you set up your Fabric Connect network as quickly as possible. It will also eliminate the need to perform manual operations repetitively.

Fabric Assist helps you to migrate your existing VLAN-centric network to a Fabric Connect network. Fabric Assist accomplishes the migration by enhancing VLAN provisioning using the following features:

- VLAN Trunk Mode – Identifies a port as a VLAN trunk and automatically adds all the device VLANs as tagged.
- VLAN Range - Imports many VLANs to the device instead of manually adding and editing one entry at a time.
- Layer 2 VSN Service Creation - Automatically maps VLAN entries to Layer 2 VSNs.
- VLAN Pruning - Prevents the unnecessary configuration of VLANs that have no egress.
- Import to Service Definition - Enables you to import a device's active configuration into a Service Application, which you can then use as a configuration template for other devices managed by ExtremeCloud™ IQ - Site Engine.

IMPORTANT: With the VLAN Trunk Mode and Layer 2 VSN Service Creation features, you can provision VLAN trunk ports and Layer 2 VSNs automatically. Do not use these features if the device is running Fabric Attach. Fabric Attach dynamically makes equivalent configuration changes, and if Fabric Assist is enabled, it will change those settings to static on the device.

For information on related topics:

- Provision VLAN Trunks Automatically
- How to Edit a Port Template
- Add a Range of VLANs at the Device Level
- Add a Range of VLANs at the Site Level
- Add a Range of VLANs at the Service Definition Level
- Enable Fabric Assist
- Fabric Assist L2 VSN Considerations

Fabric Manager ZTP+ Configuration

Fabric Manager is a resilient, scalable, and highly efficient network management application that allows your network domains to operate interdependently, efficiently, and with minimal

intervention. Fabric Manager allows you to monitor the fabric topology and service applications on your network.

Fabric Manager is deployed as a separate virtual machine (VM) in ExtremeCloud IQ - Site Engine, and is enabled via ZTP+ (Zero Touch Provisioning Plus) functionality.

General Network Configuration

Fabric Manager supports two initial configuration modes for ExtremeCloud IQ - Site Engine discovery and registration: DHCP mode and Static mode. DHCP is the default configuration mode.

Use the Static mode when providing a predefined set of networking configurations.

Use the DHCP mode so the engine can communicate with the ExtremeCloud IQ - Site Engine server. The following DHCP settings and DNS mapping of **extremecontrol** are for when Fabric Manager is installed in DHCP Mode:

- The DHCP Server needs to return a DNS Server and Domain Name to the ZTP+ device. It is the default mode of configuration during the Fabric Manager VM's initial bootup cycle.
- The DNS Server needs to map the name **extremecontrol.<*domain-name*>** to the IP address of the ExtremeCloud IQ - Site Engine server.

Once ExtremeCloud IQ - Site Engine and the ZTP+ device are pre-configured, you can add the site definition to the ExtremeCloud IQ - Site Engine database. For information, see How to Add Fabric Manager.

For information on related topics:

- Sites
- Profiles
- Add Device
- Edit Device
- Devices

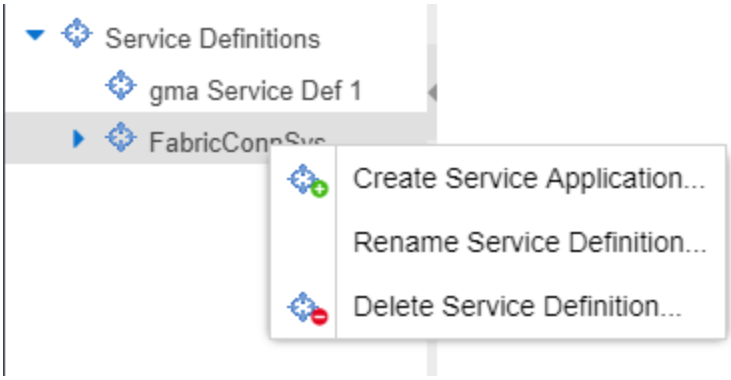
How to Create a Service Application

You can create a service application via the **Sites** tab in ExtremeCloud IQ - Site Engine. Service definitions display information from service applications. When created, service applications are added to sites in your network and are used to build a topology map.

Create a Service Application

To create a service application:

1. Access the **Devices** tab.
2. Select **Sites** from the left-panel drop-down list.
3. Expand **Service Definitions** in the left-panel.
4. Right-click the service definition in which you want to create the service application.



5. Select **Create Service Application**.

   The **Create Service Application** window opens.
6. Enter a name in the **Name** field.
7. Select **OK**.
8. Select the newly created service application.
9. Use the Services tab and a Service Summary tab to configure the service application.

The service application is created. After the service application is created and configured, you can apply it to a site within your network. After services have been assigned to a site, they cannot be deleted.

NOTE: A Service Application must have the same fabric type as its associated Service Definition. For example, if a Service Definition is created with Fabric Connect type, it can only have Service Applications of Fabric Connect type. Currently, Fabric Connect is the only fabric type available.

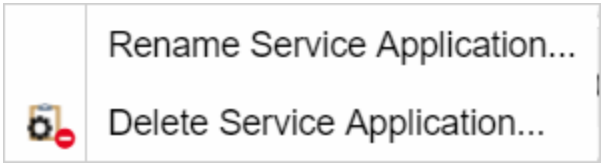
After the service application is created, it is available in the left-panel tree and a new right panel opens that includes a Services tab and a Service Summary tab.

Rename a Service Application

To change the name of a service application:

1. Open the **Devices** tab.
2. Select **Sites** from the left-panel tree drop-down list.
3. Expand **Service Definitions** in the left-panel.

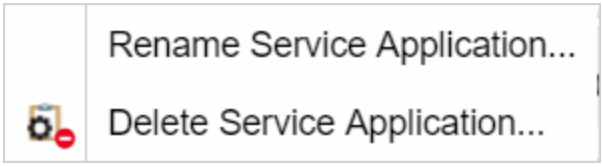
4. Right-click the service application you are renaming.



5. Select **Rename Service Application**.
6. Enter a new name in the **Name** field.
7. Select **OK** to change the name of the service application.

Delete a Service Application

You can delete all user-defined service applications, unless the service application or any of its associated service definitions are assigned to a site.



To delete a service application:

1. Open the **Devices** tab.
2. Select **Sites** from the left-panel drop-down list.
3. Expand **Service Definitions** in the left-panel.
4. Right-click the service application you are deleting.
5. Select **Delete Service Application**.
6. Select **Yes** to delete the service application.

For information on related topics:

- Services
- Fabric
- Sites
- Devices

How to Add Fabric Manager

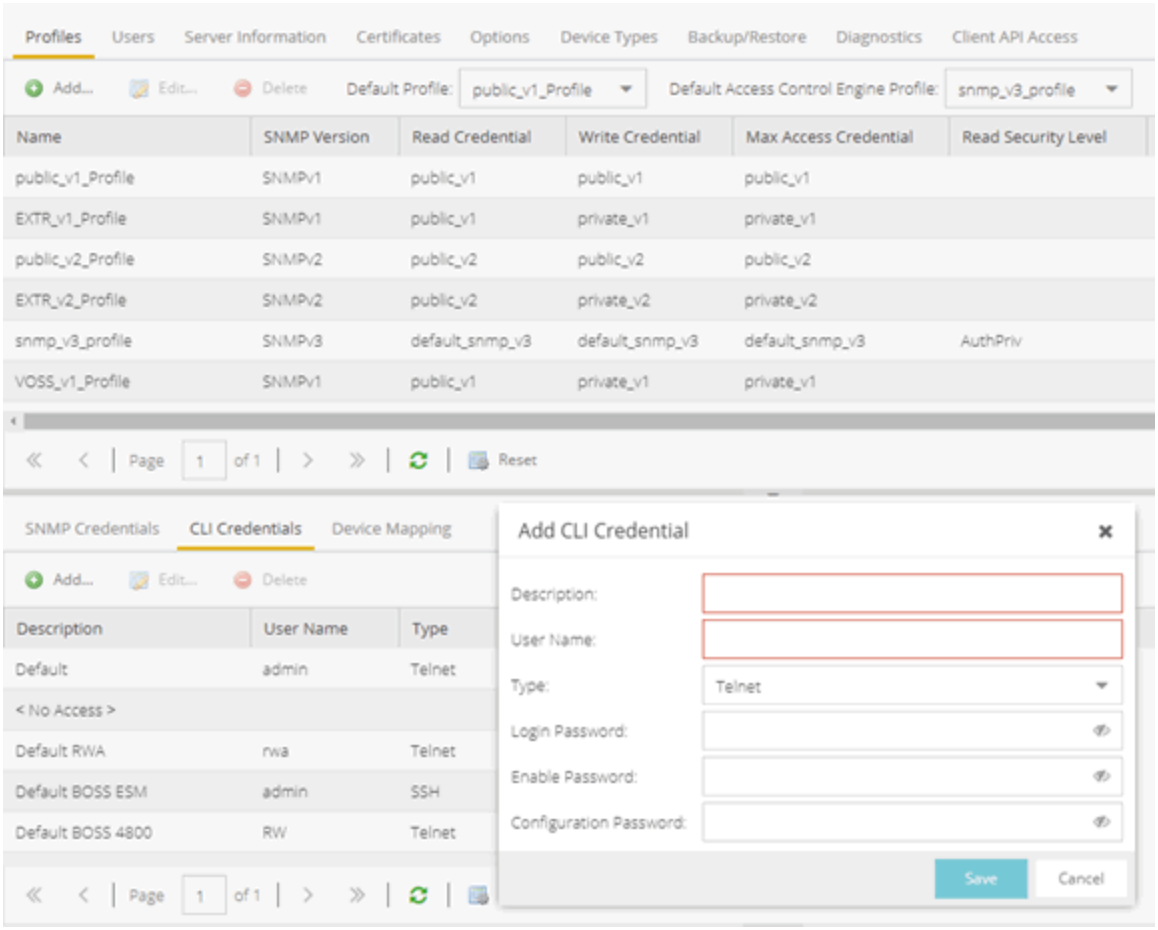
Once you install the Fabric Manager virtual machine (VM), you can add it to ExtremeCloud IQ - Site Engine and enable it via ZTP+ (Zero Touch Provisioning Plus) functionality.

Adding Fabric Manager to ExtremeCloud IQ - Site Engine

Prior to adding the Fabric Manager engine, you must create an Administration Profile for the Fabric Manager with CLI credentials. Fabric Manager uses the Administrator Profile as an additional user account.

Add CLI Credentials

1. Launch ExtremeCloud IQ - Site Engine.
2. Open the **Administration > Profiles** tab.
3. In the bottom panel, select the **CLI Credentials** tab.

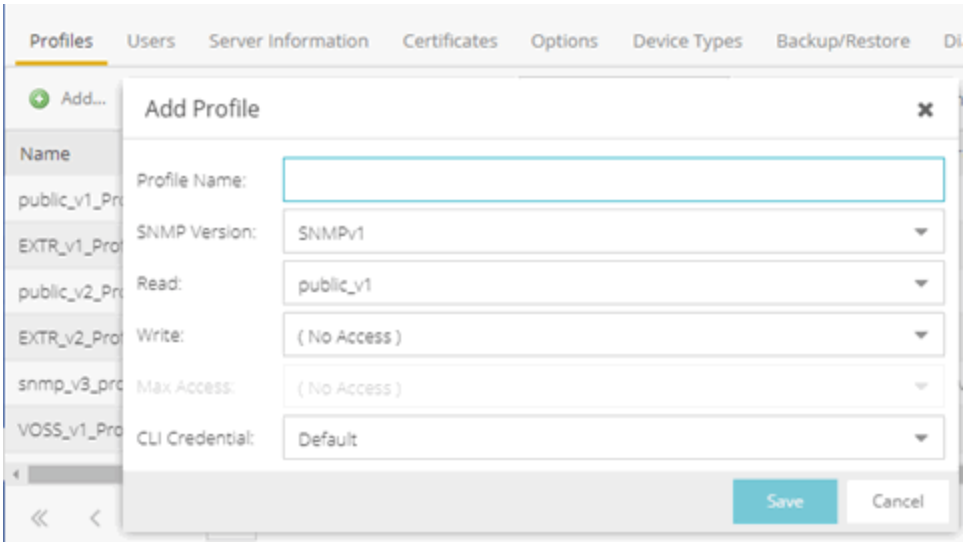


4. Select the **Add** button (Add) to open the **Add CLI Credential** window.
5. Enter a name for the CLI Credential in the **Description** field.
6. Enter **root** in the **User Name** field.

7. Select **SSH** from the **Type** drop-down list.
8. Enter a password in the **Login Password** field.
   This password must be the same password that you provided in Step 2b of the Fabric Manager Installation Static Mode topic.
9. Enter a password in the **Enable Password** field.
10. Enter a password in the **Configuration Password** field.
11. Select **Save**.

Create Administration Profile

1. At the top of the **Profiles** tab, select the **Add** button (Add) to open the **Add Profile** window.



2. In the **Profile Name** field, enter a name for this profile.
3. In the **SNMP Version** field, select **SNMPv1**.
   Fabric Manager does not use SNMP; the SNMP credentials here are just placeholders.
4. In the **Read** field, select **Ping Only**.
5. In the **Write** field, select either **No Access** or **Ping Only**.
6. In the **CLI Credential** field, select the same CLI Credential that you created in Step 4 of the Add CLI Credentials topic.
7. Select **Save**.

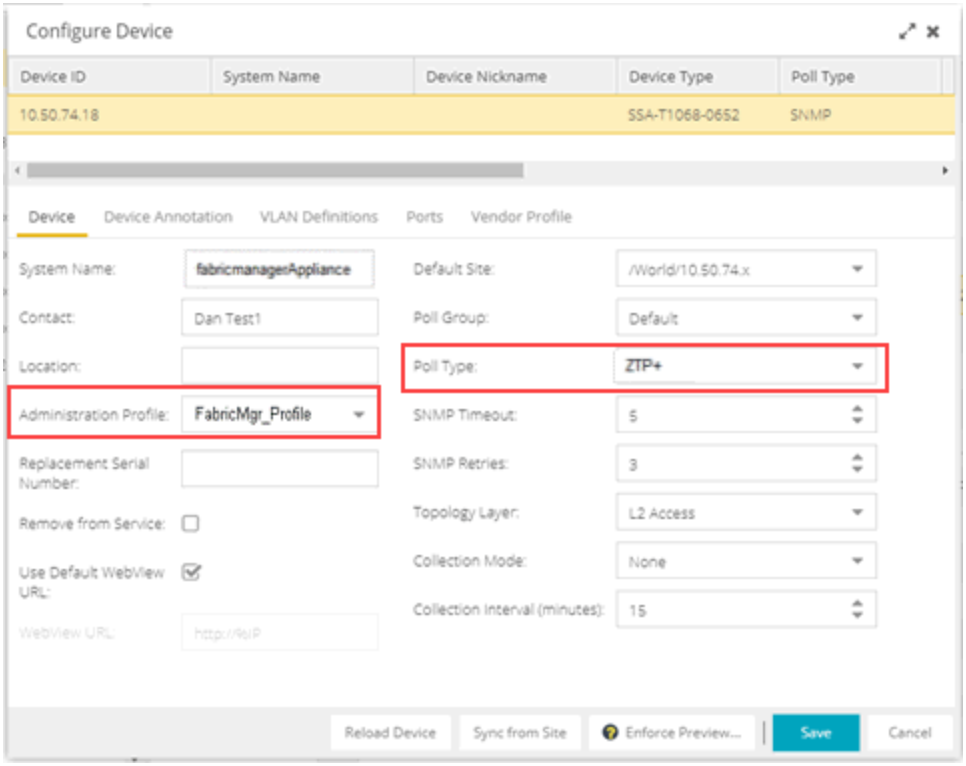
Add Administration Profile to the Fabric Manager engine

1. Open the **Network** > Discovered tab in ExtremeCloud IQ - Site Engine.

NOTE: The Fabric Manager appears as a device on the **Discovered** tab. It is listed with a **Status** of **ZTP+ Pending Edit**, indicating the configuration needs to be edited before adding it to the ExtremeCloud IQ - Site Engine server.

2. Right-click the new Fabric Manager file and select **Configure Devices** tab from the drop-down list.

   The **Configure Device** window opens.



3. Select the profile you created from the **Administration Profile** drop-down list.
4. Select **ZTP+** from the **Poll Type** drop-down list.
5. Select the **ZTP+ Device Settings** tab in the **Configure Device** window.
6. Configure the fields on the ZTP+ Device Settings tab to determine how the Fabric Manager is managed by ExtremeCloud IQ - Site Engine using ZTP+ functionality.

ZTP+ Discovery

Once the ZTP+ discovery process is complete, the Fabric Manager engine is added to the ExtremeCloud IQ - Site Engine database and moves from the **Network** > **Discovered** tab to the **Network** > **Devices** tab. The ZTP+ discovery process may take up to five minutes to complete.

NOTES: If you did not select **Automatically Add Devices** on the **Site** tab, the Fabric Manager engine remains on the **Discovered** tab with a **Status** of **ZTP+ Complete**. Select the file, select the **Add Devices** button (the Add Device window appears), and select the **Add** button to add the device to the ExtremeCloud IQ - Site Engine database.

In the event a configuration is not correctly transmitted to the switch or if connectivity is lost during any part of this process, the file resets and allows the process to restart.

The Fabric Manager engine **Status** (displayed on the Discovered tab) is now **ZTP+ Staged**, indicating ExtremeCloud IQ - Site Engine will push the configuration to the device the next time the device contacts ExtremeCloud IQ - Site Engine.

When ExtremeCloud IQ - Site Engine pushes the configuration to the Fabric Manager engine, the **Status** is **ZTP+ Complete**.

- ExtremeCloud IQ - Site Engine Fabric
- Fabric Connect

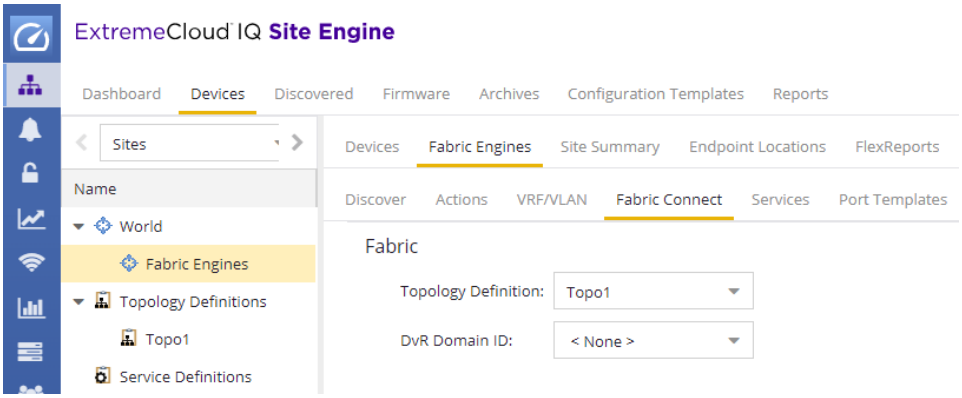
Applying Fabric Services

When you have created and configured your fabric topology, service and service application services, you can apply them to sites within your network. When fabric topology and services have been assigned to a site, they cannot be deleted.

NOTE: Services not assigned to a service definition (where NONE has been selected) can be deleted from a site after they have been assigned to that site.

Applying a Fabric Topology to a Site

1. Open the **Network > Devices** tab.
2. Select **Sites** from the left-panel tree drop-down list.
3. Select a site in the left-panel tree.
4. Select the site name tab in the **Devices** sub-tab.

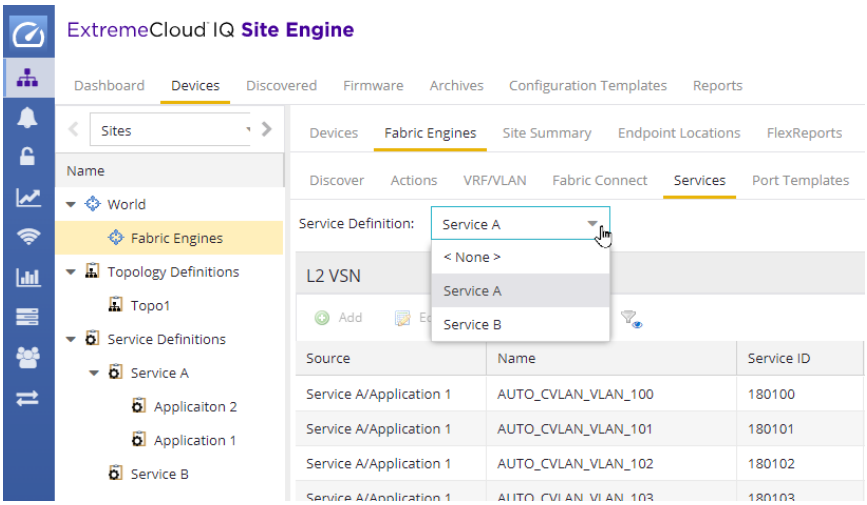


5. Select the **Fabric Connect** tab.
6. Select the topology you want to apply to the site from the **Topology Definition** drop-down list.
7. Select the DVR Domain from the **DVR Domain** drop-down list.
8. Select **Save**.

NOTE: Only one Fabric Topology and one DVR Domain can be assigned a site in ExtremeCloud IQ - Site Engine.

Applying a Service Application to a Site

1. Open the **Network > Devices** tab.
2. Select **Sites** from the left-panel tree drop-down list.
3. Select a site in the left-panel tree.
4. Select the site name tab in the **Devices** sub-tab.
5. Select the **Services** tab.
6. Select the service definition you want to apply to the site from the **Service Definition** drop-down list. The service application details that you configured to the service definition display in the L2 VPN and L3 VPN tables.



7. Select Save to apply the services to the site.

Applying Fabric to Port Templates

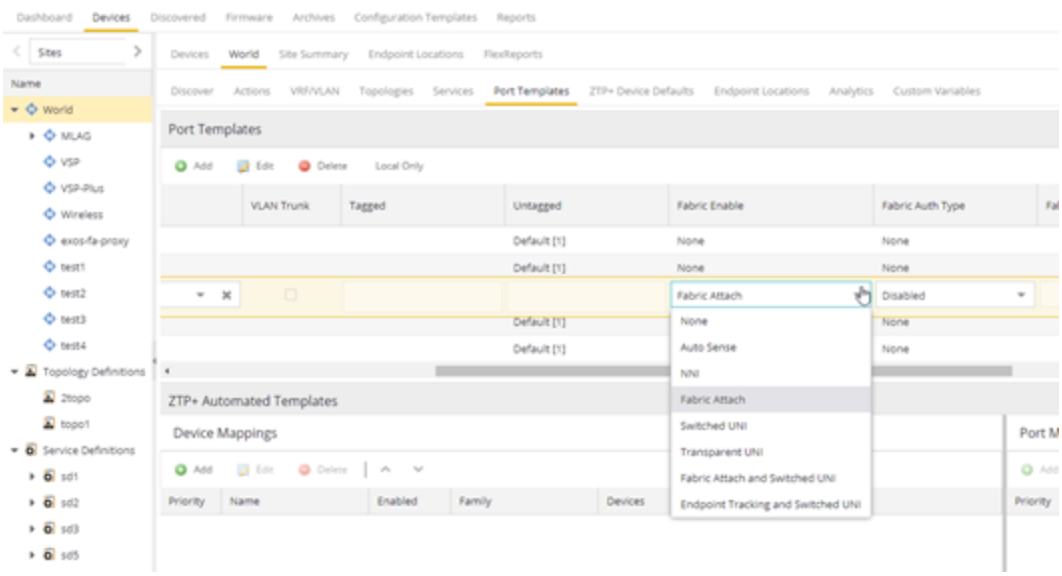
The Port Templates Configuration window enables you to configure ports with a Fabric role. When complete, you can apply the Port Templates configuration to a device.

ExtremeCloud IQ - Site Engine supports the following Fabric roles:

- None
- NNI
- Fabric Attach
- Switched UNI
- Transparent UNI
- Fabric Attach and Switched UNI

NOTE: The Fabric Attach (FA) and Switched UNI (S-UNI) option means that the port is configured for both features, but only one feature is active at any one time. The mode is determined by which mapping request the port receives first (FA or S-UNI). Ports receive mapping requests via LLDP TLVs.

The following screen capture shows the Port Templates window, which you can access from either the World view or from a specific Site.



Use the following steps to configure fabric to a port template:

NOTE: Port templates for which you configure Fabric Enable values must be configured as Global port templates. To create a Global port template, select the World site and select **Global** from the **Source** drop-down list.

1. Open the **Network > Devices** tab.
2. Select **World** or a specific Site, and then the **Port Templates** tab.
3. Select a template, and then the Edit (Edit) button.
4. Under Fabric Enable, select a fabric mode.
5. Under Fabric Auth Type, select an authentication type.
6. Under Fabric Auth Key, select an authentication key if available.
7. Select **Save**

Applying Fabric to Ports

The Port Configuration window enables you to edit the fabric information about the ports on a device.

ExtremeCloud IQ - Site Engine supports the following Fabric roles:

- None
- NNI
- Fabric Attach
- Switched UNI

- Transparent UNI
- Fabric Attach and Switched UNI

NOTE: The Fabric Attach (FA) and Switched UNI (S-UNI) option means that the port is configured for both features, but only one feature is active at any one time. The mode is determined by which mapping request the port receives first (FA or S-UNI). Ports receive mapping requests via LLDP TLVs.

Use the following steps to configure fabric to a port:

1. Open the **Network > Devices** tab.
2. Select **Devices**.
3. Select the **Menu** icon (☰) or right-click on a device.
4. Select **Configure**.
   The Configure Device window opens.
5. Select **Ports**.
6. Select a port, and then the Edit (Edit) button.
7. Under Fabric Enable, select a fabric mode.
8. Under Fabric Auth Type, select an authentication type.
9. Under Fabric Auth Key, select an authentication key if available.
10. Select **Save**.

Applying Fabric Services to a Device

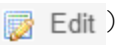
After you have applied fabric topologies and services to a site, you can also apply the fabric services to devices assigned to that site.

Applying Fabric Topology to a Device

1. Open the **Network > Devices** tab.
2. Select **Sites** from the left-panel tree drop-down list.
3. Right-click a site in the left-panel tree.
4. Select **Configure Device** from the drop-down list. The **Configure Device** window opens.
5. Select the **Fabric Connect** tab.
6. Select the **Sync from Site** button to populate the tab with the fabric topology details you applied to the site. The topology details you applied to the site will be applied to the device, as long as the device you have selected is assigned to the same site.
7. To populate the tab manually, select the **Enable Fabric** checkbox.
8. Select a **Fabric Role** from the drop-down list.
9. Enter a system ID number in the **System ID** field.

10. Enter a nickname in the **SPBM Nickname** field.
11. Check the **Multicast** checkbox, if needed.
12. Check the **IP Shortcuts** checkbox, if needed.
13. Enter the system name in the **System Name** field.
14. Select the **Enforce Preview** button.

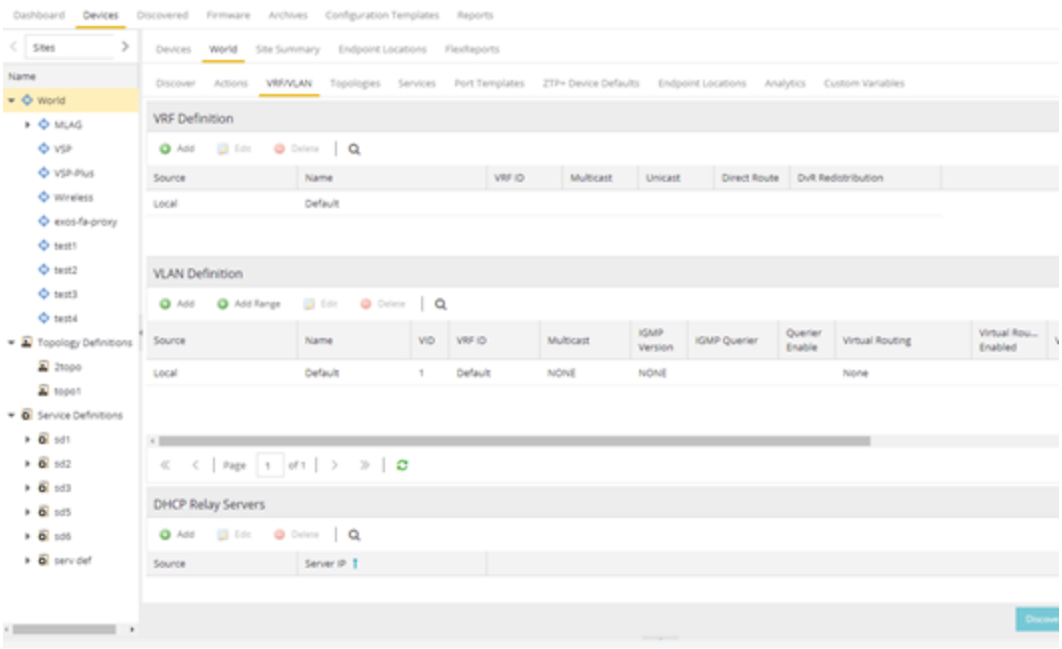
Applying Fabric Services to a Device

1. Open the **Network > Devices** tab.
2. Select **Sites** from the left-panel tree drop-down list.
3. Right-click a site in the left-panel tree.
4. Select **Configure Device** from the drop-down list. The **Configure Device** window opens.
5. Select the **Services** tab. The service details that you configured to the site display in the L2 VPN and L3 VPN tables.
6. Select the **Sync from Site** button to populate the tab with the fabric service details you applied to the site. The service details you applied to the site will be applied to the device, as long as the device you have selected is assigned to the same site.
7. Select the Add () button to add an L2 VSN or L3 VSN service to the device.
8. Select the Edit () button to edit service details that were populated from the site.
9. Select the **Enforce Preview** button.

NOTE: The L3VPN table is disabled when the device is set as a DVR Leaf node.

Adding and Deleting VRF Definitions

1. Open the **Network > Devices tab**.
2. Select **Sites** from the left-panel tree drop-down list.
3. Right-click a site in the left-panel tree.
4. Select **Configure Device** from the drop-down list. The **Configure Device** window opens.
5. Select the **VRF/VLAN** tab.



The top table on the **VRF/VLAN** tab in the **Configure Device** window displays read-only VRF details you applied to the site. You can add a new VRF to the device.

1. Select the Add (Add) button.
2. Enter the name of a VRF in the **Name** field.
3. Enter the ID number in the **VRF ID** field.
4. Select **Update** to add the VRF to the device.
5. Select the **Enforce Preview** button.

You can delete a VRF from the **VRF/VLAN** tab.

1. Select a VRF in the table.
2. Select the **Delete** (Delete) button.
3. Select **Yes** to remove the VRF.

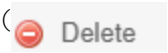
Adding and Deleting VLAN Definitions

1. Open the **Network > Devices** tab.
2. Select **Sites** from the left-panel tree drop-down list.
3. Right-click a site in the left-panel tree.
4. Select **Configure Device** from the drop-down list. The **Configure Device** window opens.
5. Select the **VRF/VLAN** tab.

The middle table on the **VRF/VLAN** tab in the Configure Device window displays read-only VLAN details you applied to the site. You can add a new VLAN to the device.

1. Select the Add () button.
2. Enter the name of a VLAN in the **Name** field.
3. Enter the ID number in the **VLAN ID** field.
4. Select **Update** to add the VLAN to the device.
5. Select the **Enforce Preview** button.

You can delete a VLAN from the **VRF/VLAN** tab.

1. Select a VLAN in the table.
2. Select the **Delete** () button.
3. Select **Yes** to remove the VLAN.

Enforcing the Fabric Configurations

After you enforce previews on the **Fabric Connect**, **Services**, and **VRF/VLAN** tabs, use the **Compare Device Configuration** window to enforce the configurations to the device. Additionally, the **VLAN Definition** tab allows you to enforce the **VLAN** and **Ports** fabric configurations.

Enforcing Fabric Connect

1. Select **Enforce Preview** on the **Fabric Connect** tab in the **Configure Device** window.
2. The Compare Device window opens.
3. Select the Fabric Connect Enforce Option.
4. Select **Enforce**.

Enforcing Fabric VRF

1. Select **Enforce Preview** on the **VRF/VLAN** tab in the **Configure Device** window.
2. The Compare Device window opens.
3. Select the **VRF/VLAN** tab.
4. Select **Enforce**.

Enforcing Fabric Services

1. Select **Enforce Preview** on the **Services** tab in the **Configure Device** window.
2. The Compare Device window opens.
3. Select the Services Enforce Option.

4. Select the **L2 VPN** tab.
5. Select **Enforce**.
6. Select the **L3 VPN** tab.
7. Select **Enforce**.

Enforcing Fabric VLAN

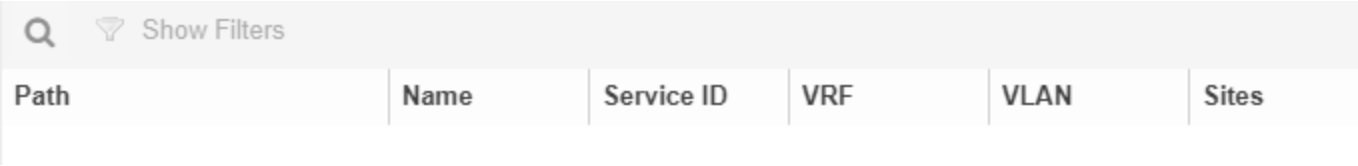
1. Select **Enforce Preview** on the **VLAN** tab in the **Configure Device** window.
2. The Compare Device window opens.
3. Select the VLAN Definition Enforce Option.
4. Select **Enforce**.

Enforcing Fabric Port

1. Select **Enforce Preview** on the **Ports** tab in the **Configure Device** window.
2. The Compare Device window opens.
3. Select the Ports Enforce Option.
4. Select **Enforce**.

Service Summary

The **Service Summary** tab displays a summary of the fabric services you create and the sites to which they are assigned.



Path
The path to the Service Application in which the service is located.

Name
The name of the fabric service included in the service application or definition.

Service ID
The I-SID, which is the system-defined ID number assigned to the service.

VRF
The ID number assigned to the VRF definition.

VLAN
The ID number assigned to the VLAN.

Sites
The site to which the fabric service is assigned.

- Services
- Fabric
- Sites

Fabric Topology Definition on the Sites Tab

Use the **Fabric Topology Definition** tab to create a fabric topology definition, configure fabric topology settings, and review fabric topology paths and sites. You can also rename or delete a fabric topology definition.

Create a Topology Definition

You can create a Topology Definition on the **Sites** tab in ExtremeCloud IQ - Site Engine. After you create topology definitions, you can add them to sites in your network to build a fabric topology map.

To create a topology definition:

1. Access the **Devices** tab.
2. Select **Sites** from the left-panel drop-down list.
3. Navigate to **Topology Definitions** in the left-panel tree.
4. Right-click **Topology Definitions**.
5. Select **Create Topology Definition**.

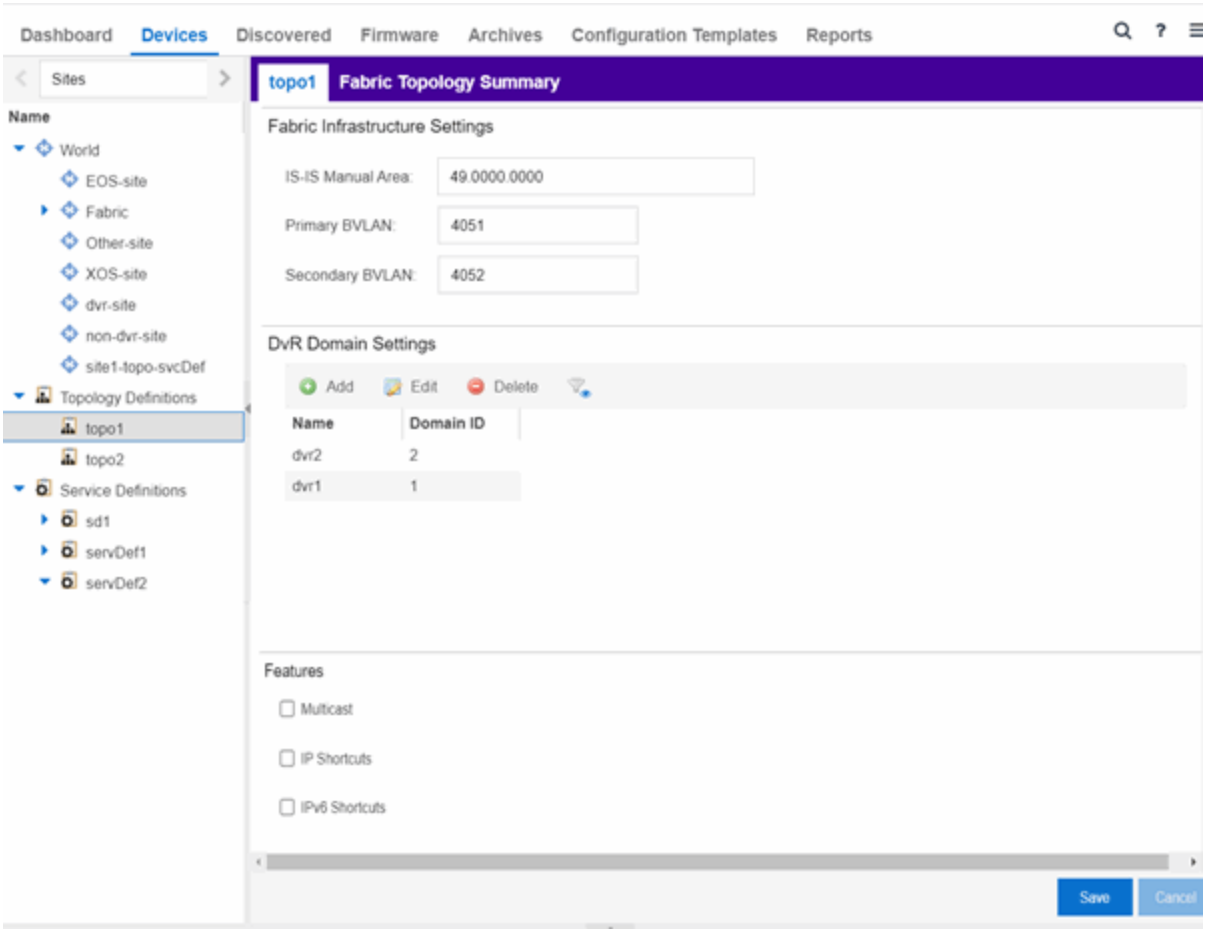
   The **Create Topology Definition** window opens.
6. Enter a name in the **Name** field.
7. Select **Fabric Connect** from the **Fabric Type** drop-down.
8. Select **OK** to create the topology definition.

Configure a Topology Definition

After the topology definition is created, it is available in the **Sites tab** left-panel tree. Select it to open a new right panel that includes the Fabric Name tab and a Fabric Summary tab.

Fabric Name Tab

Use the **Fabric Name** tab to configure the topology definition.



The Topology Definition tab includes the following sections:

Fabric Infrastructure Settings

The following fields are included in the Fabric Infrastructure Settings section:

- ISIS Manual Area - Use a xx.xxxx.xxxx.xxxx.xxxx.xxxx.xxxx format (1-13 bytes).
- Primary BVLAN - Enter the Primary Backbone VLAN (BVLAN).
- Secondary BVLAN - Enter the Secondary BVLAN.

DvR Domain Settings

The following fields are included in the DvR Domain Settings section:

- Name - The Domain name assigned to the DvR Domain. Select the down arrow to open the drop-down list to access sort, hide columns and search filter functionality for the domain name column.
- Domain ID - The identifying number assigned to the DvR Domain. Select the down arrow to open the drop-down list to access sort, hide columns and numeric filter functionality for the Domain ID column.

You can also Add, Edit, or Delete DvR Domain settings.

Features

The following fields are included in the Features section:

- Multicast - Select the check box to configure to distribute data to multiple recipients.
- IP Shortcuts - Select the check box to enable IPv4 Shortcuts for the topology definition.
- IPv6 Shortcuts - Select the check box to enable IPv6 Shortcuts for the topology definition.

Select **Save** to save the topology definition settings you selected.

After the topology definition is created and configured, you can apply it to a site within your network. After fabric topologies have been assigned to a site, they cannot be deleted.

Fabric Summary tab

The Fabric Summary tab lists any fabric topologies you have created and the sites to which they are assigned.

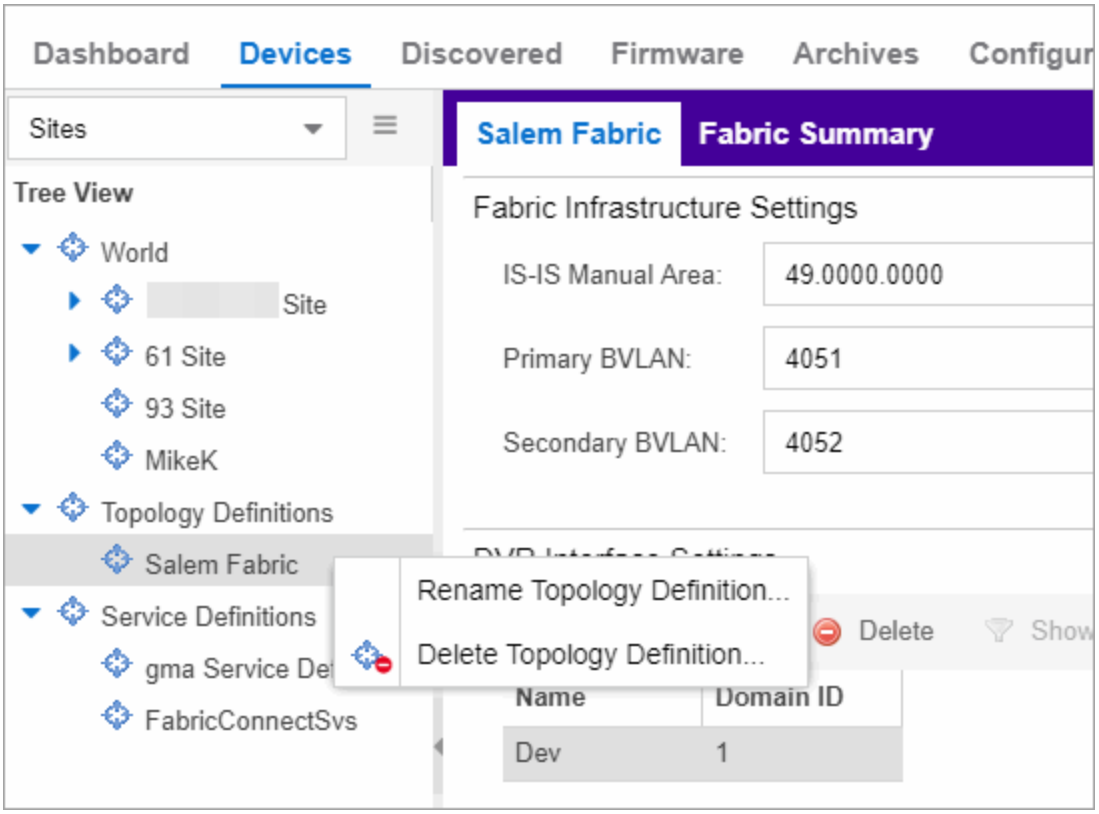
Rename a Topology Definition

After a topology definition has been created and configured, you can change or modify its name.

To rename a topology definition:

1. Open the **Devices** tab.
2. Select **Sites** from the left-panel tree drop-down list.
3. Expand **Topology Definitions** in the left-panel.

4. Right-click the topology definition you are renaming.



5. Select **Rename Topology Definition**.
6. Enter a new name in the **Name** field.
7. Select **OK** to change the topology name.

Delete a Topology Definition

After a topology definition has been created and configured, you can delete it; however, a topology definition cannot be deleted if it has been assigned to a site.

To delete a topology definition:

1. Open the **Devices** tab.
2. Select **Sites** from the left-panel tree drop-down list.
3. Expand the **Topology Definitions** in the left-panel.
4. Right-click the topology definition you are deleting.
5. Select **Delete Topology Definition**.
6. Select **Yes** to delete the topology definition you selected.

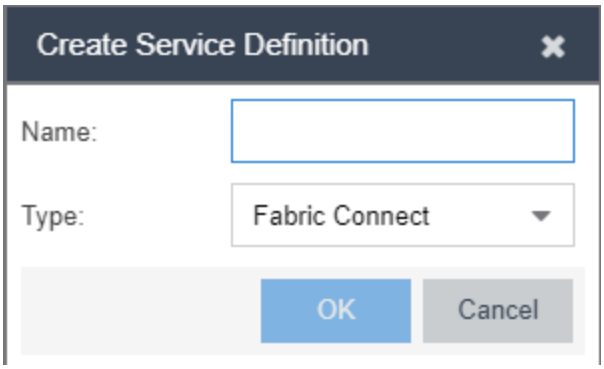
How to Create a Fabric Service Definition

You can create a service definition in the **Sites tab** in ExtremeCloud IQ - Site Engine. Service definitions display information configured in service applications definitions. When created, service definitions are added to sites in your network and are used to build a fabric topology map.

Create a Service Definition

To create a service definition:

1. Open the **Devices** tab.
2. Select **Sites** from the left-panel drop-down list.
3. Select **Service Definitions** in the left-panel.
4. Right-click **Service Definitions**.
5. Select **Create Service Definition**.



   The **Create Service Definition** window opens.
6. Enter a name in the **Name** field.
7. Select **Fabric Connect** from the **Type** drop-down list.
8. Select **OK** to create the service definition.

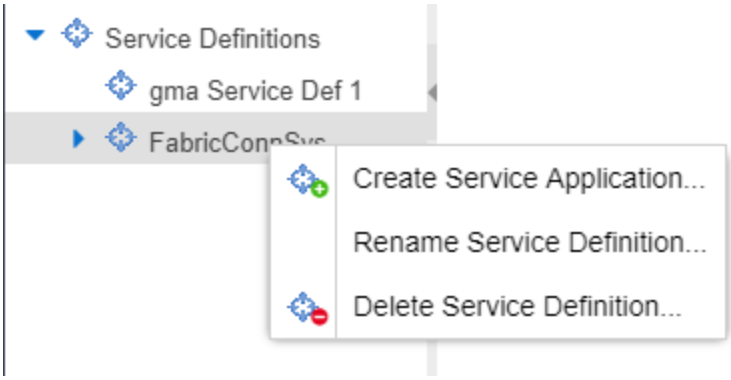
After the service definition is created and configured, you can apply it to a site within your network. When fabric services have been assigned to a site, they cannot be deleted.

Service Definition Panel

After the service definition is created, it is available in the left-panel tree. Select it to open a new right panel that includes a **Services** tab and a **Service Summary** tab.

Rename a Service Definition

After a service definition has been created and configured, you can change or modify its name.

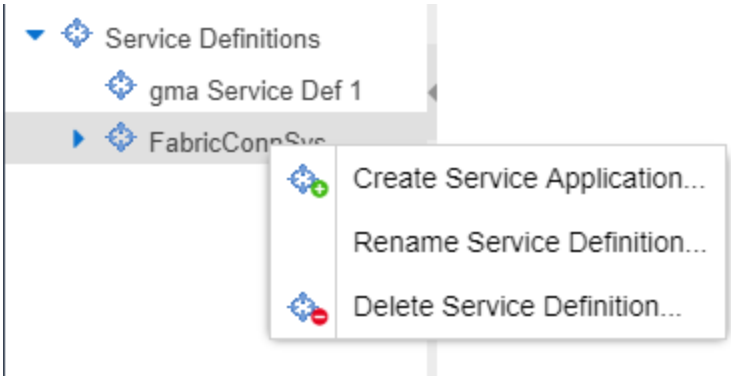


To rename a service definition:

1. Open the **Devices** tab.
2. Select **Sites** from the left-panel tree drop-down list.
3. Expand **Service Definitions** in the left-panel.
4. Right-click the service definition you are renaming.
5. Select **Rename Service Definition**.
6. Enter a new name in the **Name** field.
7. Select **OK** to rename the service definition.

Delete a Service Definition

When a service definition has been created and configured, you can delete it; however, a service definition or any of its associated service applications cannot be deleted if it has been assigned to a site.



To delete a service definition:

1. Open the **Devices** tab.
2. Select **Sites** from the left-panel drop-down list.
3. Expand **Service Definitions** in the left-panel.
4. Right-click the service definition you are deleting.
5. Select **Delete Service Definition**.
6. Select **Yes** to delete a service definition.

For information on related topics:

- Services
- Fabric
- Sites
- Devices

Upgrading Fabric Manager

Use the following procedure to upgrade your version Fabric Manager.

Prerequisites

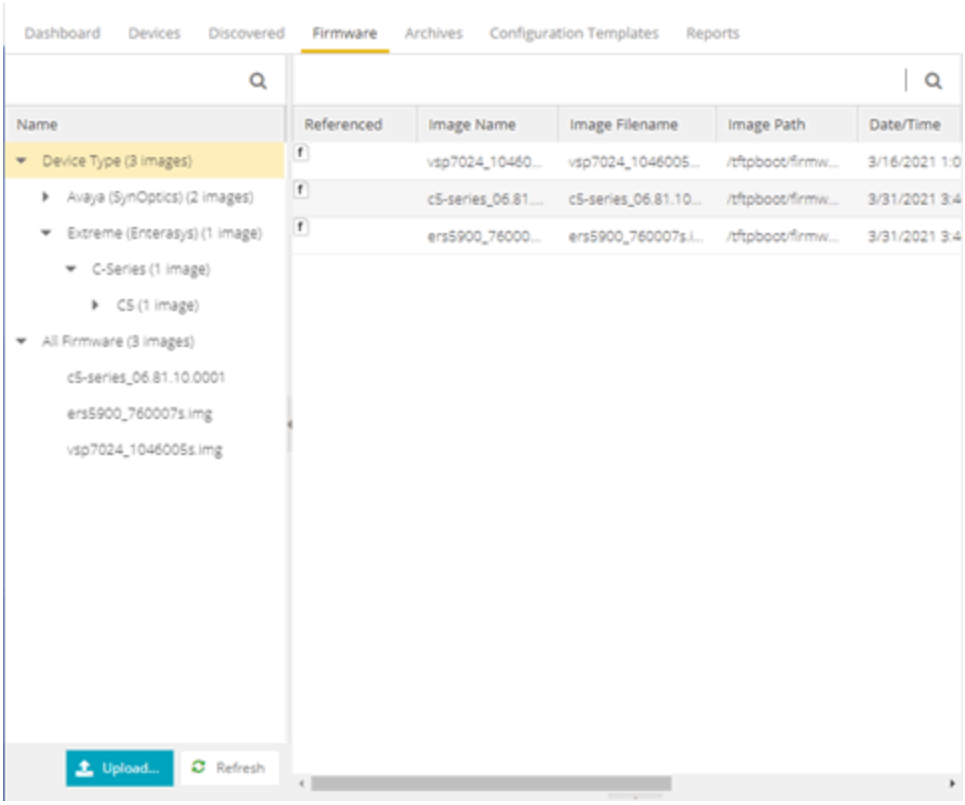
- Upgrade ExtremeCloud IQ - Site Engine to the later version before you upgrade Fabric Manager to the corresponding build number.
- Ensure that both the current and target ExtremeCloud IQ - Site Engine and Fabric Manager build numbers are the same.
- Download the latest upgrade bundle from the Extreme Networks software download Portal.
- Change **Login Information** from **Anonymous** to appropriate SCP credentials in the SCP Server Properties section in the **Administration** > **Options** > **Inventory Manager** > **File Transfer** tab.

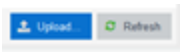
NOTE: After you deploy Fabric Manager and then register with ExtremeCloud IQ - Site Engine, only the user credential associated with the Fabric Manager profile has SSH login access.

Upgrade Procedure

1. Open the **Network** tab in ExtremeCloud IQ - Site Engine.

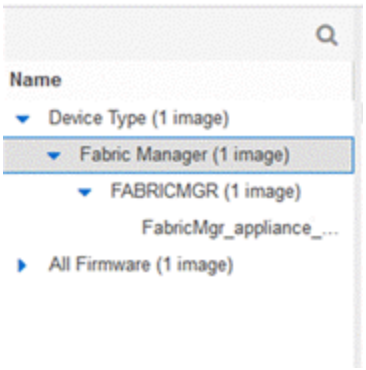
2. Select the **Firmware** tab.



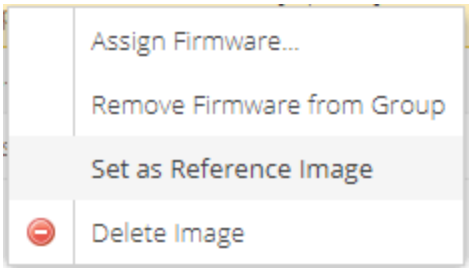
3. On the left panel, select **Upload**  .
4. In the Directory field, select the **SCP** radio button and select **Upload**.

5. Select on **Drop files here or select to browse** and select the previously downloaded upgrade bundle.
6. Select the **Upload** button to initiate the bundle upload to the ExtremeCloud IQ - Site Engine server.

   Once the upload is completed successfully, if not previously added after selecting the **Refresh** button, a new entry appears under Device Type called Fabric Manager.

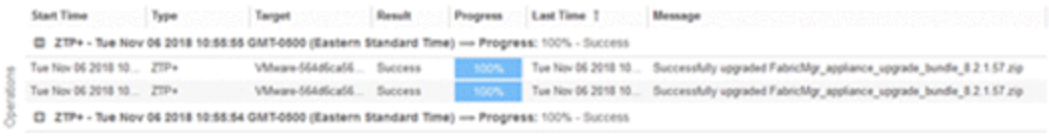


7. Navigate through the newly added Device type until you see the bundle image listed.
8. Right-click the bundle listed on the main panel and select **Set as Reference Image**.

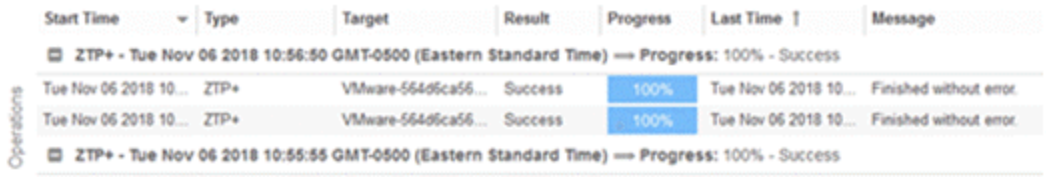


This step sets this image bundle as the Reference upgrade image for Fabric Manager. The upgrade process to get triggered by default can take **up to five minutes** depending on the poll interval set on ExtremeCloud IQ - Site Engine.

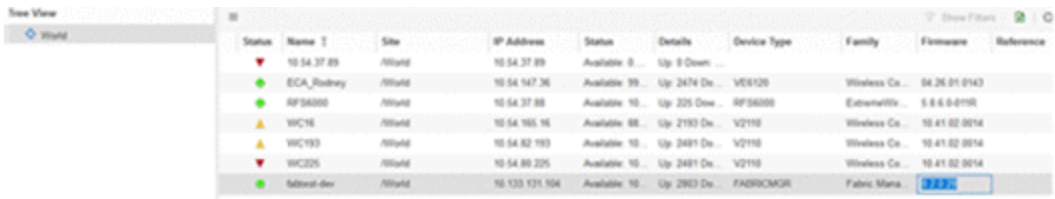
9. Open the **Operations** log on ExtremeCloud IQ - Site Engine and wait until a log of type 'ZTP+' with the message `Successfully upgraded FabricMgr_appliance_upgrade_bundle_<version_number>.zip` appears.



This is followed by a message `Finished without error` to indicate the upgrade operation has been completed by the ZTP+.



10. When the upgrade is complete, the details on Fabric Manager are updated to the latest version.



Post Upgrade Steps

1. Ensure that the same user credential associated with the Fabric Manager profile has SSH login access.
2. Navigate to the previously added and referenced upgrade image and un-reference it by right selecting the bundle and then selecting **Unset as Reference Image**.

- ExtremeCloud IQ - Site Engine Fabric
- Fabric Connect

Troubleshooting

This troubleshooting guide provides a list of items to check when ExtremeCloud IQ - Site Engine functionality is failing to perform correctly. Locate a problem in the left column and then review the troubleshooting information in the right column.

Problem	Troubleshooting Steps
Error contacting a wireless controller. The controller shows a Warning icon. 	1. Verify that the Configuration password in the CLI Credential used for this device is properly configured. a. From ExtremeCloud IQ - Site Engine, access **Administration** > **Profiles** tab. b. Select the **CLI Credentials** subtab. c. Select the CLI Credential being used by the controller's Profile, and select **Edit**. d. Verify the user name and password used in the credential. For wireless controllers, add the Login password to the Configuration password field instead of the Login password field. The username and Configuration password specified here must match the username and Login password configured on the controller. e. Verify the SSH connection type is selected. f. Select **OK**. g. Use this CLI Credential in the controller's Profile. **NOTE:** When configuring profiles for ExtremeWireless Controllers, you must ensure that controllers are discovered using an SNMPv2c or SNMPv3 profile. The profile must also contain SSH CLI credentials for the controller. Wireless Manager uses the controller's CLI to retrieve required information and to configure managed controllers. 2. Verify that the following ports are accessible through firewalls for the ExtremeCloud IQ - Site Engine Server and Wireless Controllers to communicate: SSH: 22 SNMP: 161, 162 Langley: 20506