



Fabric User Guide

05/2021
9037068-00
Subject to Change Without Notice

Copyright © 2021 Extreme Networks, Inc. All Rights Reserved.

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 User Guide	1
Extreme Networks® Software License Agreement	4
Table of Contents	10
Fabric Manager Installation	14
Pre-Installation	14
Fabric Manager Installation Static Mode	14
Adding Fabric Manager to ExtremeCloud IQ - Site Engine	19
Getting Started	20
Requirements	20
ExtremeCloud IQ - Site Engine Access Requirements	21
Use Case 1: Full Read/Write Access	22
Use Case 2: Read-Only Access	23
Use Case 3: Limited Read-Only Access	24
Use Case 4: End-System Information, Read-Only Access	24
Use Case 5: End-System Information, Read/Write Access	24
Browser Requirements	25
Screen Resolution	25
Enable Report Data Collection	25
Enable Device Statistics Collection	25
Enabling Device Statistics Collection	26
Enable Interface Statistics Collection	27
Enabling Interface Statistics Collection	28
Enable Wireless Controller Statistics Collection	29

Enabling Wireless Controller Statistics Collection	29
Enable Flow Collection	30
Enable Flow Collection on a Device	30
Enable Flow Collection on an Interface	30
ExtremeCloud IQ - Site Engine Scalability	31
ExtremeCloud IQ - Site Engine Timeout	31
How to Obtain and Apply an ExtremeCompliance License	32
Fabric Topology Definition on the Sites Tab	33
Create a Topology Definition	33
Configure a Topology Definition	34
Fabric Name Tab	34
Fabric Summary tab	36
Rename a Topology Definition	36
Delete a Topology Definition	37
How to Create a Fabric Service Definition	38
Create a Service Definition	39
Service Definition Panel	39
Rename a Service Definition	40
Delete a Service Definition	40
Services	41
VRF Definition	42
VLAN Definition	43
Service Application Name	46
L2 VSN	47
L3 VSN	48

Fabric	50
Accessing Fabric in ExtremeCloud IQ - Site Engine	51
Fabric Tab	53
Fabric Connect	54
Left-Panel Tree	55
Fabric Connect Folder	55
Fabric Attach Folder	56
Right-Panel Topology Map	57
Topology Tab Tools	58
Topology Tab Buttons	59
Fabric Manager ZTP+ Configuration	59
General Network Configuration	60
How to Create a Service Application	61
Create a Service Application	61
Rename a Service Application	62
Delete a Service Application	62
How to Add Fabric Manager	63
Adding Fabric Manager to ExtremeCloud IQ - Site Engine	63
Add CLI Credentials	64
Create Administration Profile	65
Add Administration Profile to the Fabric Manager engine	65
ZTP+ Discovery	67
Applying Fabric Services	67
Applying a Fabric Topology to a Site	68
Applying a Service Application to a Site	69

Applying Fabric to Port Templates	69
Applying Fabric to Ports	71
Applying Fabric Services to a Device	73
Applying Fabric Topology to a Device	73
Applying Fabric Services to a Device	73
Adding and Deleting VRF Definitions	74
Adding and Deleting VLAN Definitions	76
Enforcing the Fabric Configurations	77
Enforcing Fabric Topology	77
Enforcing Fabric VRF	78
Enforcing Fabric Services	79
Enforcing Fabric VLAN	79
Enforcing Fabric Port	80
Service Summary	81
Fabric Topology Definition on the Sites Tab	82
Create a Topology Definition	82
Configure a Topology Definition	83
Fabric Name Tab	83
Fabric Summary tab	85
Rename a Topology Definition	85
Delete a Topology Definition	86
How to Create a Fabric Service Definition	87
Create a Service Definition	88
Service Definition Panel	88
Rename a Service Definition	89

Delete a Service Definition	89
Upgrading Fabric Manager	90
Prerequisites	91
Upgrade Procedure	91
Post Upgrade Steps	95
Troubleshooting	96

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

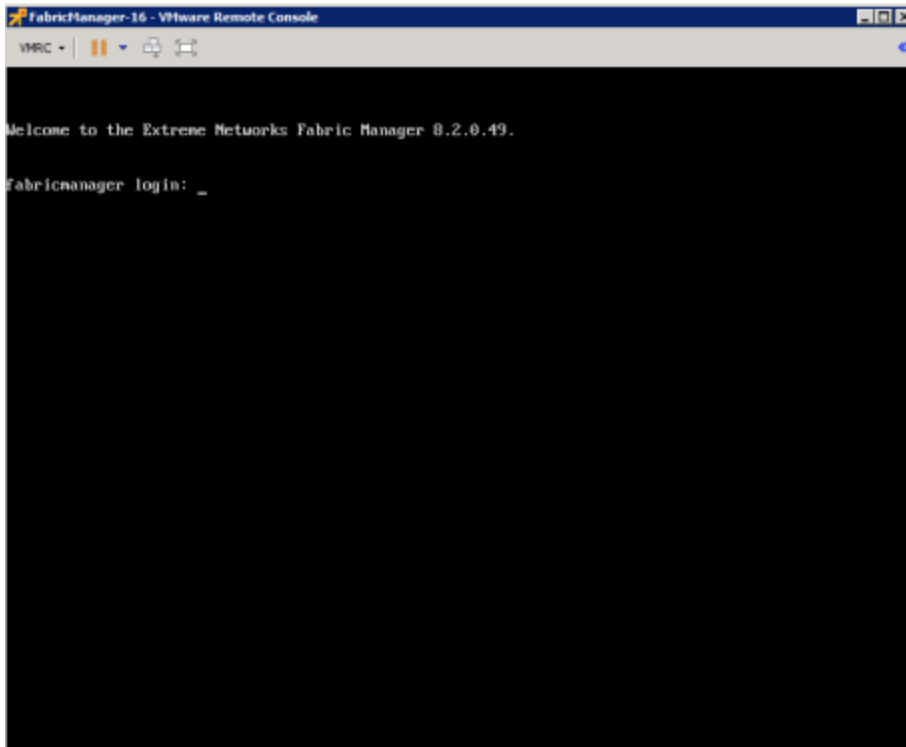
The DHCP mode is the default configuration mode during the Fabric Manager VM's initial startup. Use the static mode when providing a predefined set of networking configurations.

Fabric Manager Installation Static Mode

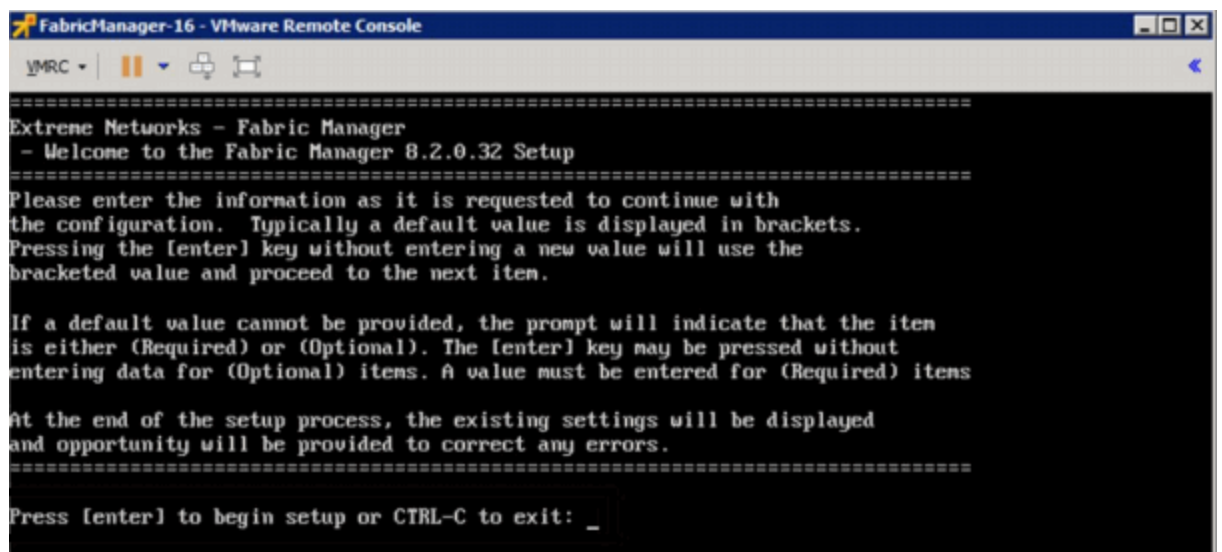
Fabric Manager begins installation in DHCP mode by default. Switch to static mode at any time during the initial installation by pressing the **ENTER** key.

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

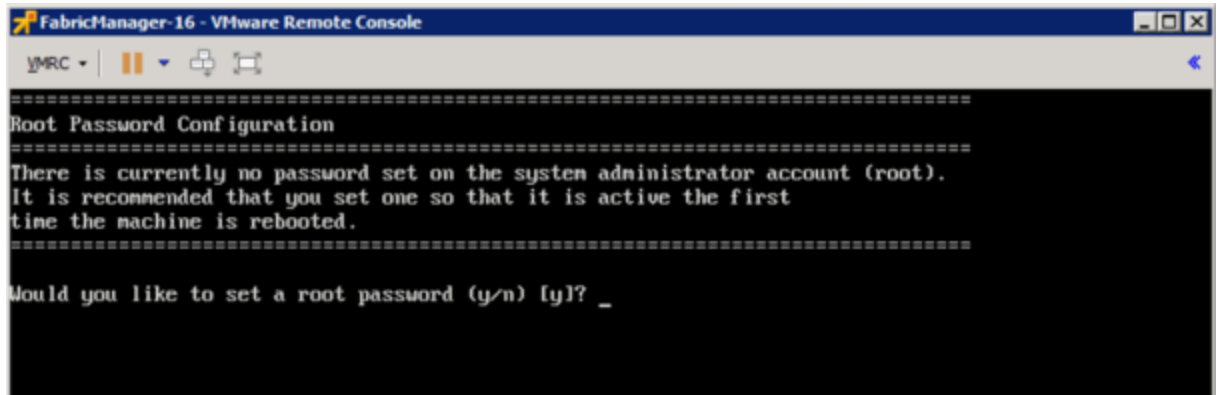
1. In the Console tab of the vSphere client, login as root with no password and press Enter.



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



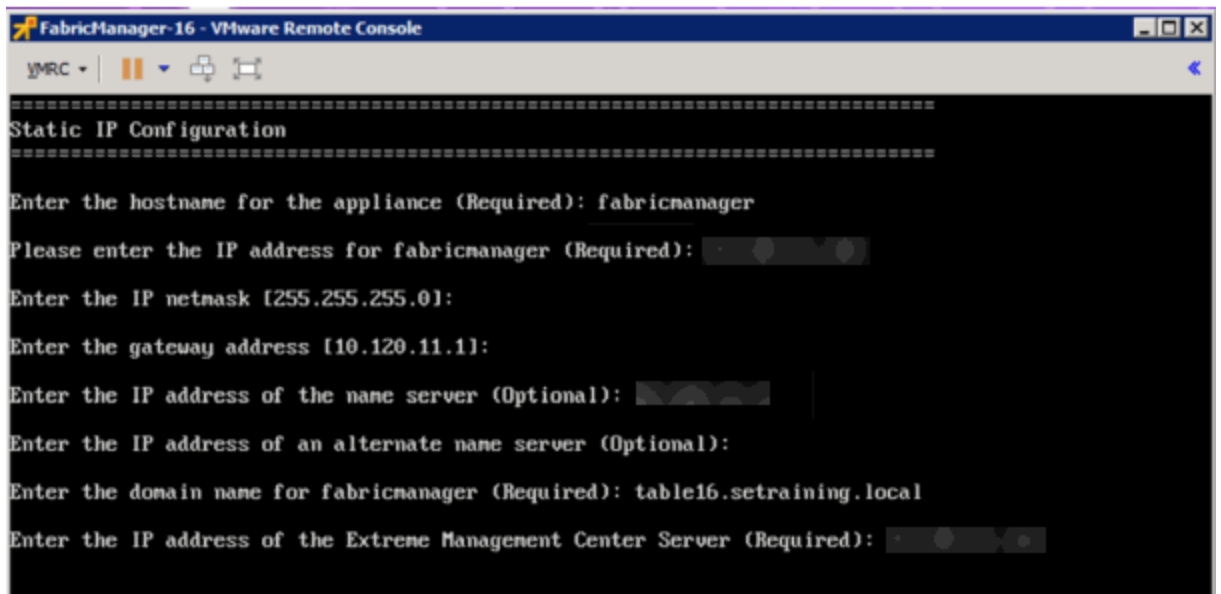
- b. Set a root password by entering `y`.



```
FabricManager-16 - VMware Remote Console
VMRC | [Icons]
=====
Root Password Configuration
=====
There is currently no password set on the system administrator account (root).
It is recommended that you set one so that it is active the first
time the machine is rebooted.
=====
Would you like to set a root password (y/n) [y]? _
```

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

The Static Configuration screen opens.

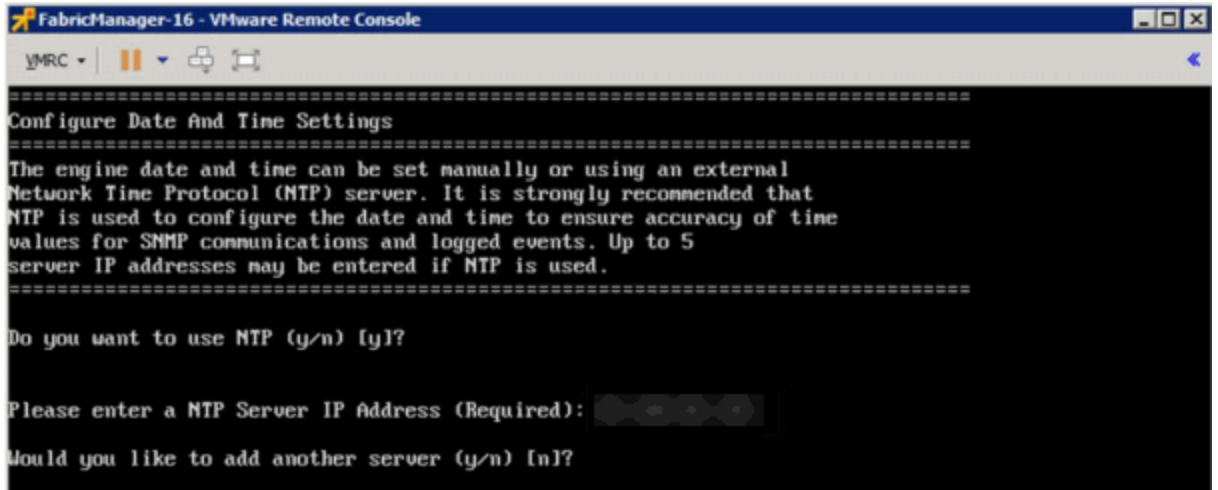


```
FabricManager-16 - VMware Remote Console
VMRC | [Icons]
=====
Static IP Configuration
=====
Enter the hostname for the appliance (Required): fabricmanager
Please enter the IP address for fabricmanager (Required):
Enter the IP netmask [255.255.255.0]:
Enter the gateway address [10.120.11.1]:
Enter the IP address of the name server (Optional):
Enter the IP address of an alternate name server (Optional):
Enter the domain name for fabricmanager (Required): table16.setraining.local
Enter the IP address of the Extreme Management Center Server (Required):
```

- 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.

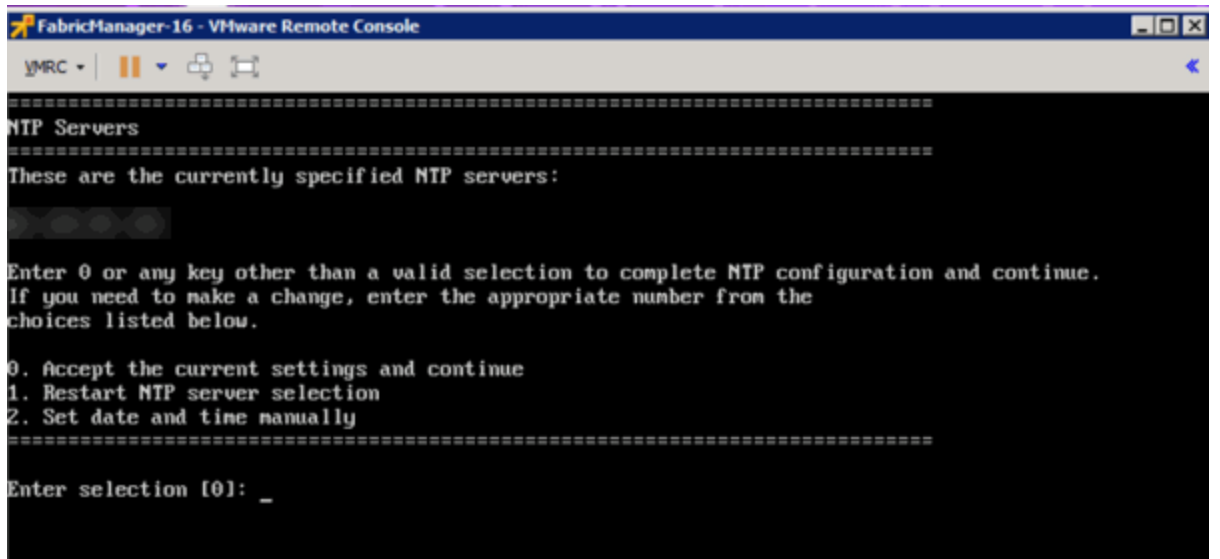
- j. Enter the ExtremeCloud IQ - Site Engine server IP address.

The Date and Time Configuration screen opens.



```
=====  
FabricManager-16 - VMware Remote Console  
VMRC | [Icons]  
=====  
Configure Date And Time Settings  
=====  
The engine date and time can be set manually or using an external  
Network Time Protocol (NTP) server. It is strongly recommended that  
NTP is used to configure the date and time to ensure accuracy of time  
values for SNMP communications and logged events. Up to 5  
server IP addresses may be entered if NTP is used.  
=====  
Do you want to use NTP (y/n) [y]?  
  
Please enter a NTP Server IP Address (Required): [Input Field]  
Would you like to add another server (y/n) [n]?
```

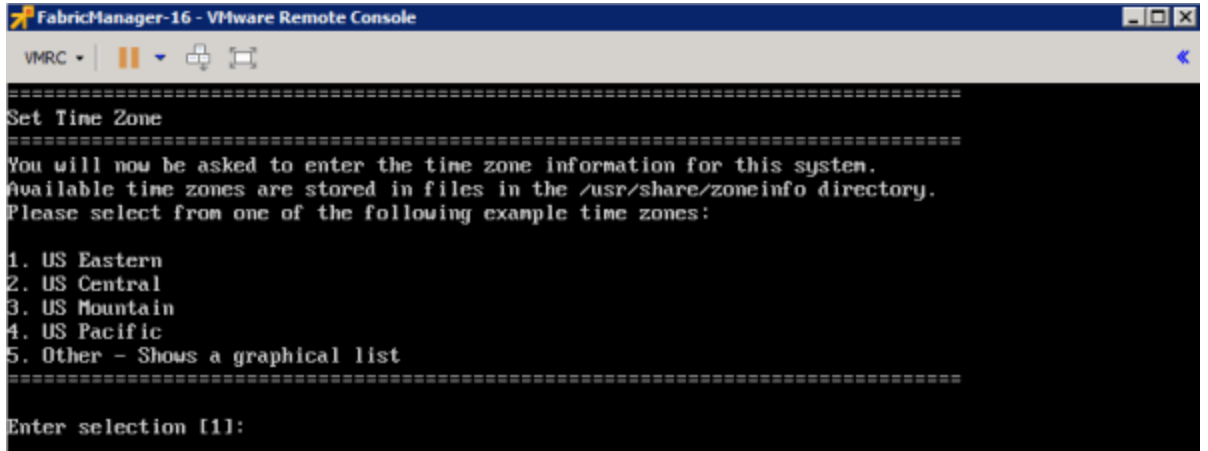
- k. Enter `y` at the next prompt to use NTP (Network Time Protocol).
l. Enter the NTP Server IP Address.
m. Enter `nat` at the next prompt to skip adding another NTP server. This is optional.



```
=====  
FabricManager-16 - VMware Remote Console  
VMRC | [Icons]  
=====  
NTP Servers  
=====  
These are the currently specified NTP servers:  
[Input Field]  
  
Enter 0 or any key other than a valid selection to complete NTP configuration and continue.  
If you need to make a change, enter the appropriate number from the  
choices listed below.  
  
0. Accept the current settings and continue  
1. Restart NTP server selection  
2. Set date and time manually  
=====  
Enter selection [0]: 0
```

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

- o. Select the correct Time Zone for your network.



```

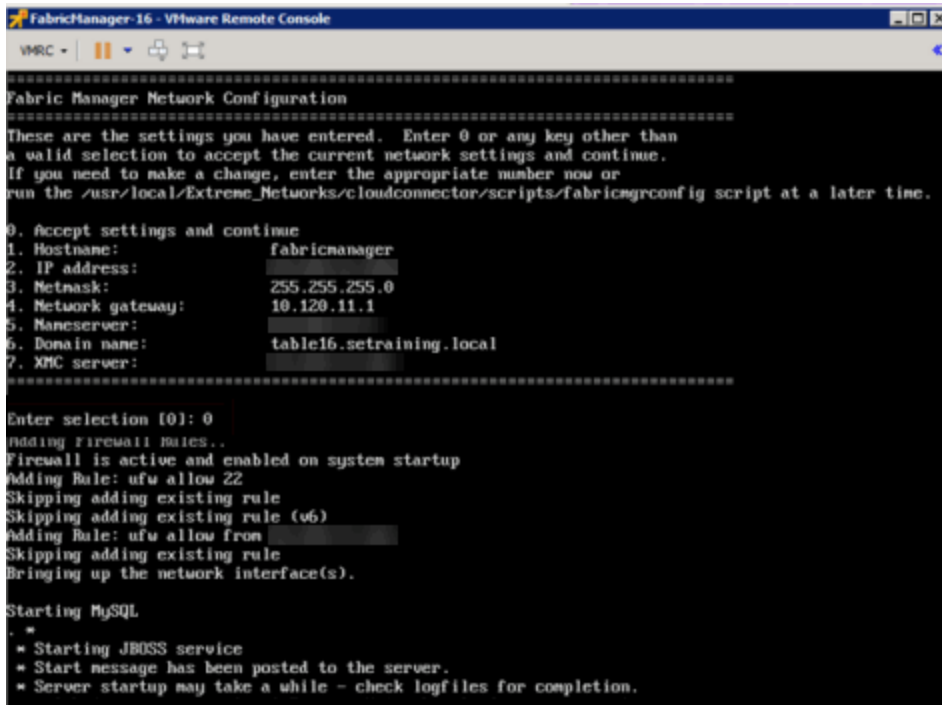
=====
Set Time Zone
=====
You will now be asked to enter the time zone information for this system.
Available time zones are stored in files in the /usr/share/zoneinfo directory.
Please select from one of the following example time zones:

1. US Eastern
2. US Central
3. US Mountain
4. US Pacific
5. Other - Shows a graphical list
=====
Enter selection [1]:

```

- 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.



```

=====
Fabric Manager Network Configuration
=====
These are the settings you have entered. Enter 0 or any key other than
a valid selection to accept the current network settings and continue.
If you need to make a change, enter the appropriate number now or
run the /usr/local/Extreme_Networks/cloudconnector/scripts/fabricmgrconfig script at a later time.

0. Accept settings and continue
1. Hostname:          fabricmanager
2. IP address:       10.120.11.1
3. Netmask:          255.255.255.0
4. Network gateway: 10.120.11.1
5. Nameserver:       10.120.11.1
6. Domain name:     table16.setraining.local
7. XMC server:       10.120.11.1
=====
Enter selection [0]: 0
Adding Firewall Rules..
Firewall is active and enabled on system startup
Adding Rule: ufw allow 22
Skipping adding existing rule
Skipping adding existing rule (v6)
Adding Rule: ufw allow from 10.120.11.1
Skipping adding existing rule
Bringing up the network interface(s).

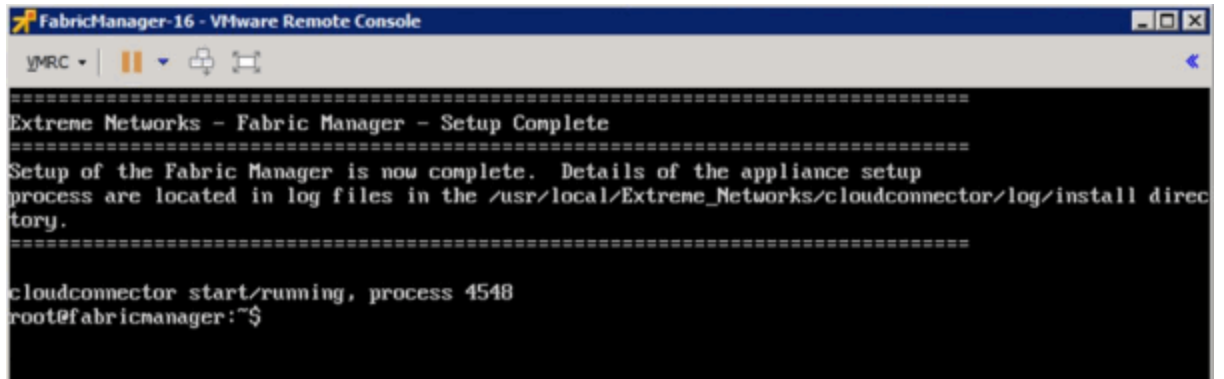
Starting MySQL
. *
  * Starting JBOSS service
  * Start message has been posted to the server.
  * Server startup may take a while - check logfiles for completion.

```

- 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 once installation is complete.



```
FabricManager-16 - VMware Remote Console
VMRC | [Icons]
=====
Extreme Networks - Fabric Manager - Setup Complete
=====
Setup of the Fabric Manager is now complete. Details of the appliance setup
process are located in log files in the /usr/local/Extreme_Networks/cloudconnector/log/install direc
tory.
=====

cloudconnector start/running, process 4548
root@fabricmanager:~$
```

Adding Fabric Manager to ExtremeCloud IQ - Site Engine

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.

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

Related Information

For information on related tabs:

- [How to Upgrade Firmware in ExtremeCloud IQ - Site Engine](#)
- [Fabric Manager ZTP+ Configuration in ExtremeCloud IQ - Site Engine](#)
- [ExtremeCloud IQ - Site Engine Fabric](#)

Getting Started

This topic provides information to help you get started using ExtremeCloud IQ - Site Engine to view network data. It includes information on configuring ExtremeCloud IQ - Site Engine access requirements, including several different access scenarios. It also provides steps for enabling the statistics and flow collection that provides ExtremeCloud IQ - Site Engine reporting data, and information on ExtremeCloud IQ - Site Engine scalability.

- [Requirements](#)
 - [ExtremeCloud IQ - Site Engine Access Requirements](#)
 - [Full Read/Write Access](#)
 - [Read-Only Access](#)
 - [Limited Read-Only Access](#)
 - [End-System Information, Read-Only Access](#)
 - [End-System Information, Read/Write Access](#)
 - [Browser Requirements](#)
 - [Screen Resolution](#)
- [Enable Report Data Collection](#)
 - [Enable Device Statistics Collection](#)
 - [Enable Interface Statistics Collection](#)
 - [Enable Wireless Controller Statistics Collection](#)
- [Enable Flow Collection](#)
 - [Enable Flow Collection on a Device](#)
 - [Enable Flow Collection on an Interface](#)
- [ExtremeCloud IQ - Site Engine Scalability](#)
- [ExtremeCloud IQ - Site Engine Timeout](#)

Requirements

This section provides information on license requirements for the different ExtremeCloud IQ - Site Engine features, as well as access requirements, browser

requirements, and screen resolution requirements.

ExtremeCloud IQ - Site Engine Access Requirements

Access to the ExtremeCloud IQ - Site Engine application and its features is determined by the user's membership in an ExtremeCloud IQ - Site Engine authorization group and the group's assigned capabilities. The following table lists the different ExtremeCloud IQ - Site Engine access options and features, and their corresponding capabilities.

To have full read/write access to all ExtremeCloud IQ - Site Engine functionality, a user must be a member of an authorization group with the capabilities shown in the following table. Optionally, users can be configured to have read-only and limited read-only access to ExtremeCloud IQ - Site Engine functionality by selecting a combination of capabilities.

ExtremeCloud IQ - Site Engine Access Options and Features	Required Capabilities
Launch ExtremeCloud IQ - Site Engine. Allows the ability to launch the ExtremeCloud IQ - Site Engine application.	NetSight OneView > Access OneView
View ExtremeCloud IQ - Site Engine Reports. Adds the ability to view reporting data.	NetSight OneView > Access OneView Reports
View ExtremeCloud IQ - Site Engine Maps. Adds the ability to view maps.	NetSight OneView > Maps > Maps Read Access
View and Configure ExtremeCloud IQ - Site Engine Maps. Adds the ability to view and configure maps.	NetSight OneView > Maps > Maps Read/Write Access
View ExtremeCloud IQ - Site Engine Wireless. Adds the ability to view wireless data.	NetSight Console > Wireless Manager > Launch
View ExtremeCloud IQ - Site Engine Administration. Adds access to the ExtremeCloud IQ - Site Engine administration tools and the ability to enable data collection.	NetSight OneView > Access OneView Administration
View ExtremeCloud IQ - Site Engine Search. Adds the ability to use the ExtremeCloud IQ - Site Engine Search functionality.	NetSight OneView > Access OneView Search
View ExtremeCloud IQ - Site Engine Network and Alarms and Events. Adds the ability to view device information and event log details.	NetSight OneView > Events and Alarms > OneView Event Log Access
View ExtremeCloud IQ - Site Engine alarms. Adds the ability to view current alarms in the Alarms and Events page.	NetSight OneView > Events and Alarms > OneView Alarms Read Access
View and clear ExtremeCloud IQ - Site Engine alarms. Adds the ability to view and clear alarms in the Alarms and Events page.	NetSight OneView > Events and Alarms > OneView Alarms Read/Write Access
View ExtremeCloud IQ - Site Engine Control. Adds the ability to view Dashboard, System, Health, and Data Center reports under the Control tab.	NetSight OneView > Identity and Access > Access OneView Identity and Access Reports
View ExtremeCloud IQ - Site Engine Control end-systems table. Adds the ability to view end-system information under the Control tab.	NetSight OneView > Identity and Access > OneView End-Systems Read Access
View and modify ExtremeCloud IQ - Site Engine Control end-systems table. Adds the ability to perform actions in the end-systems table, such as forcing reauthentication and changing an end-system's group membership.	NetSight OneView > Identity and Access > OneView End-Systems Read/Write Access

ExtremeCloud IQ - Site Engine Access Options and Features	Required Capabilities
View ExtremeCloud IQ - Site Engine Control Group Information. Adds the ability to launch the Group Editor tool from the Control tab > End-Systems view, and view group information.	NetSight OneView > Identity and Access > OneView Group Read Access
View and Edit ExtremeCloud IQ - Site Engine Control tab Group Information. Adds the ability to launch the Group Editor tool from the Control tab > End-Systems view, and add, edit, and delete groups.	NetSight OneView > Identity and Access > OneView Group Read/Write Access
View ExtremeCloud IQ - Site Engine Flows. Adds the ability to view NetFlow data for devices in the network.	NetSight OneView > NetFlow Read Access
View ExtremeCloud IQ - Site Engine Flows and allow NetFlow Sensor Write access. Adds the ability to view NetFlow data and configure the Console NetFlow Sensor Configuration view.	NetSight OneView > NetFlow Read/Write Access
Allow Web FlexView read access. Adds the ability to launch a FlexView from the ExtremeCloud IQ - Site Engine Network tab.	NetSight OneView > FlexView > OneView FlexView Read Access
Allow Web FlexView Write access. Adds the ability to launch and edit a FlexView from the ExtremeCloud IQ - Site Engine Network tab.	NetSight OneView > FlexView > OneView FlexView Read/Write Access
Allow Wireless Controller Automatic WebView Login ability. Adds the ability to launch local management for wireless controllers without requiring a login, as long as the user's credentials are good. Users who do not have this capability are required to log in.	NetSight Suite > Device Local Management WebView > Auto Login to Web Local Management for ExtremeWireless Wireless Controllers
Allow Check for Firmware Updates ability. Adds the ability to check for firmware updates from the ExtremeCloud IQ - Site Engine Network tab.	NetSight Suite > NetSight All User Options > Request and Configure ExtremeNetworks.com Support
Allow Create Policy Rule ability. Adds the ability to create a policy rule in NetFlow tables.	NetSight Policy Manager > Read/Write capabilities for Policy Enforcement and Management
Add Devices. Adds the ability to add devices in the ExtremeCloud IQ - Site Engine Network tab.	NetSight Suite > Devices > Add, Discover and Import
Delete Devices. Adds the ability to delete devices in the ExtremeCloud IQ - Site Engine Network tab.	NetSight Suite > Devices > Delete
Compare Configurations. Adds the ability to compare archived device configurations in either the ExtremeCloud IQ - Site Engine Network tab or the Archive Details Report available in the ExtremeCloud IQ - Site Engine Reports tab.	Inventory Manager > Configuration Archive Management > View/Compare Configurations

Here are several scenarios that show how different ExtremeCloud IQ - Site Engine user access levels can be configured based on assigned capabilities.

Use Case 1: Full Read/Write Access

To provide full read/write access to all ExtremeCloud IQ - Site Engine functionality, configure user membership in an authorization group assigned the following capabilities:

- NetSight OneView > Access OneView
- NetSight OneView > Access OneView Reports

- NetSight OneView > Access OneView Search
- NetSight OneView > Access OneView Administration
- NetSight OneView > NetFlow Read/Write Access
- NetSight OneView > Maps > Maps Read/Write Access
- NetSight Console > Wireless Manager > Launch
- NetSight OneView > Events and Alarms > OneView Event Log Access
- NetSight OneView > Events and Alarms > OneView Alarms Read/Write Access
- NetSight OneView > FlexView > OneView FlexView Read/Write Access
- NetSight OneView > Identity and Access > Access OneView Identity and Access Reports
- NetSight OneView > Identity and Access > OneView End-Systems Read/Write Access
- NetSight OneView > Identity and Access > OneView Group Read/Write Access
- NetSight Policy Manager > Read/Write capabilities for Policy Enforcement and Management
- NetSight Suite > Device Local Management WebView > Auto Login to Web Local Management for ExtremeWireless Wireless Controllers
- NetSight Suite > NetSight All User Options > Request and Configure ExtremeNetworks.com Support
- NetSight Suite > Devices > Add, Discover and Import
- NetSight Suite > Devices > Delete
- Inventory Manager > Configuration Archive Management > View/Compare Configurations

Use Case 2: Read-Only Access

To provide read-only access to all ExtremeCloud IQ - Site Engine reports and FlexViews, configure user membership in an authorization group assigned the following capabilities:

- NetSight OneView > Access OneView
- NetSight OneView > Access OneView Reports
- NetSight OneView > Access OneView Search
- NetSight OneView > NetFlow Read Access

- NetSight OneView > Maps > Maps Read Access
- NetSight Console > Wireless Manager > Launch
- NetSight OneView > Events and Alarms > OneView Event Log Access
- NetSight OneView > Events and Alarms > OneView Alarms Read Access
- NetSight OneView > FlexView > OneView FlexView Read Access
- NetSight OneView > Identity and Access > Access OneView Identity and Access Reports
- NetSight OneView > Identity and Access > OneView End-Systems Read Access
- NetSight OneView > Identity and Access > OneView Group Read Access

Use Case 3: Limited Read-Only Access

To provide limited read-only access to only ExtremeCloud IQ - Site Engine reporting and wireless data, configure user membership in an authorization group assigned the following capabilities:

- NetSight OneView > Access OneView
- NetSight OneView > Access OneView Reports
- NetSight Console > Wireless Manager > Launch

Use Case 4: End-System Information, Read-Only Access

To provide read-only access to ExtremeCloud IQ - Site Engine end-system information, configure user membership in an authorization group assigned the following capabilities:

- NetSight OneView > Access OneView
- NetSight OneView > Identity and Access > OneView End-Systems Read Access

Use Case 5: End-System Information, Read/Write Access

To provide read/write access to ExtremeCloud IQ - Site Engine end-system information, configure user membership in an authorization group assigned the following capabilities:

- NetSight OneView > Access OneView
- NetSight OneView > Identity and Access > OneView End-Systems Read/Write Access

Browser Requirements

The following web browsers are supported:

- Microsoft Edge
- Mozilla Firefox 34 and later
- Google Chrome 33.0 and later

Browsers must have JavaScript enabled in order for the web-based views to function.

While it is not required that cookies are enabled, impaired functionality results if they are not. This includes (but is not limited to) the ability to generate PDFs and persist table configurations such as filters, sorting, and column selections.

Screen Resolution

For optimum display of graphs and tables, ExtremeCloud IQ - Site Engine is best viewed on a system with a minimum screen resolution of 1280x1024.

Enable Report Data Collection

To view ExtremeCloud IQ - Site Engine reporting data, you must enable statistics collection for your network devices. You must be a member of an authorization group that has been assigned the NetSight OneView > Access NetSight OneView and Administration capability to enable data collection. Data collection is only available with the NMS license and above.

Enable Device Statistics Collection

To view ExtremeCloud IQ - Site Engine device reports, you must enable statistics collection for your network devices from either ExtremeCloud IQ - Site Engine Devices, or the Console device tree or **Device Properties** tab. Statistics can be collected in a historical or threshold alarms collection mode.

- **Historical Mode** — Device and physical port statistics are saved to the database and aggregated over time, and are then used in ExtremeCloud IQ - Site Engine reports. The device statistics are also used for active threshold alarms configured in the

Console Alarms Manager.

NOTE: Enabling Historical Device Statistics Collection may use substantial disk space.

- **Threshold Alarms Mode (formerly Monitor Mode)** — Device statistics are saved to a Threshold Alarms cache for one hour and then dropped. These statistics are used for active threshold alarms, configured in the Console Alarms Manager, but not for ExtremeCloud IQ - Site Engine reporting.

NOTE: The Threshold Alarms mode option is not available if you have disabled Threshold Alarms Collection in the OneView Collector Advanced Settings window in Administration > Options.

If you are enabling statistics collection on an ExtremeControl engine, Application Detection engine, or ExtremeWireless Controller, read through the following notes:

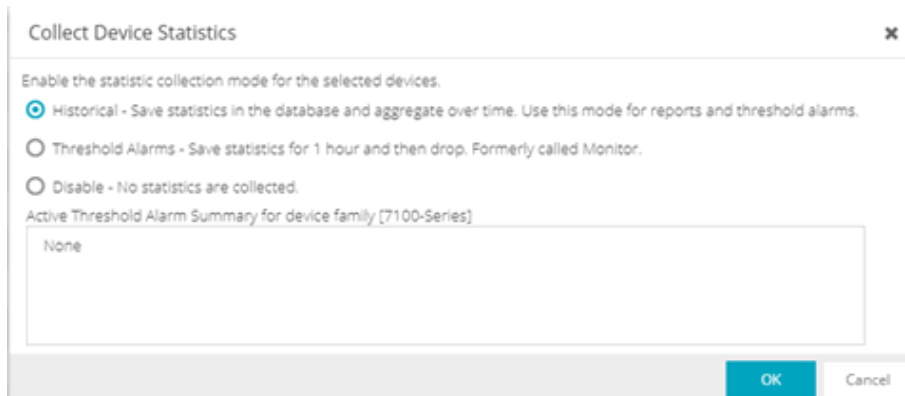
- **ExtremeControl Engine**
When collecting statistics on an ExtremeControl engine, the engine must be added to ExtremeCloud IQ - Site Engine to collect all engine statistics. In addition, Threshold Alarms mode is not supported on ExtremeControl engines.
- **Application Detection Engine**
When collecting statistics on an Application Detection engine, the engine must be added to the Analytics > Configuration > ExtremeAnalytics Engines table in order for ExtremeCloud IQ - Site Engine to collect all Application Detection statistics. In addition, Threshold Alarms mode is not supported on Application Detection engines.
- **ExtremeWireless Controller**
Wireless Controller [statistics collection](#) is configured separately from other devices.

Enabling Device Statistics Collection

Use the following steps to enable device statistics collection.

1. You can enable statistics collection from either ExtremeCloud IQ - Site Engine or Console:
 - In the **Network** tab, right-click one or more devices (multiple devices must be in the same device family) and select **Device > Collect Device Statistics**. You can also click the **Menu** icon (☰) in the upper left corner of the **Network** tab and select **Device > Collect Device Statistics**.

- In the Console device tree or **Device Properties** tab, right-click one or more devices (multiple devices must be in the same device family) and select OneView > Collect Device Statistics.
2. From the Collect Device Statistics window, select the statistic collection mode you want to use: **Historical**, **Threshold Alarms (formerly Monitor)**, or **Disable**.



All active threshold alarms configured in the ExtremeCloud IQ - Site Engine **Alarms and Events** tab (for the selected device family) that use the collected statistics display in the Active Threshold Alarms Summary box. If the selected devices do not match any active threshold alarms, this box is blank. To reduce unnecessary statistic collection, do not enable Threshold Alarms mode on devices that do not match any active threshold alarms.

TIP: A summary event is generated daily in the **Alarms and Events > Events** tab that shows the number of device with statistic collection enabled where corresponding threshold alarms are not configured.

3. Click **OK**. ExtremeCloud IQ - Site Engine begins collecting statistics for the selected devices.

Enable Interface Statistics Collection

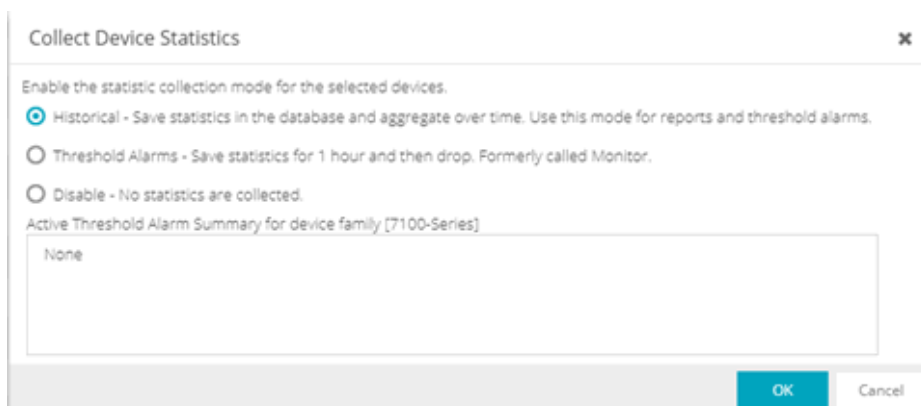
To view ExtremeCloud IQ - Site Engine interface reports, you must enable statistics collection for your device interfaces from either the ExtremeCloud IQ - Site Engine **Network** tab, or the **Console Port Properties** tab or Interface Summary FlexView. Statistics can be collected in a historical collection mode or a threshold alarms collection mode.

- Historical Mode — Interface statistics are saved to the database and aggregated over time, used in ExtremeCloud IQ - Site Engine reports. The interface statistics are also used for active threshold alarms configured in the **Alarms and Events** tab.
- Threshold Alarms Mode (formerly Monitor Mode) — Interface statistics are saved for one hour and then dropped. These statistics are used for active threshold alarms configured in the Console Alarms Manager, but not for ExtremeCloud IQ - Site Engine reporting. (Note that the Threshold Alarms mode option is not available if you have disabled Threshold Alarms Collection in the OneView Collector Advanced Settings window in the **Administration > Options** tab.)

Enabling Interface Statistics Collection

Use the following steps to enable interface statistics collection.

1. You can enable statistics collection from either ExtremeCloud IQ - Site Engine or Console:
 - On the **Network** tab, click on the device name link to open the Interface Summary FlexView. In the FlexView, right-click on one or more interfaces and select Collect Interface Statistics.
 - On the **Network** tab, right-click on a device and select Port Tree. In the Port Tree, select an interface, right-click and select **Collect Interface Statistics**.
 - In the **Console Port Properties** tab or Interface Summary FlexView, right-click one or more interfaces and select the OneView > Collect Interface Statistics.
2. From the Collect Device Statistics window, select the statistic collection mode you want to use: **Historical**, **Threshold Alarms (formerly Monitor)**, or **Disable**.



All active threshold alarms configured in the ExtremeCloud IQ - Site Engine **Alarms and Events** tab (for the selected device family) that use the collected statistics

display in the Active Threshold Alarm Summary box. If the selected devices do not match any active threshold alarms, this box is blank. To reduce unnecessary statistic collection, do not enable Threshold Alarms mode on devices that do not match any active threshold alarms.

TIP: A summary event is generated daily in the **Alarms and Events > Events** tab that shows the number of device with statistic collection enabled where corresponding threshold alarms are not configured.

3. Click **OK**. ExtremeCloud IQ - Site Engine begins collecting statistics for the selected interfaces.

Enable Wireless Controller Statistics Collection

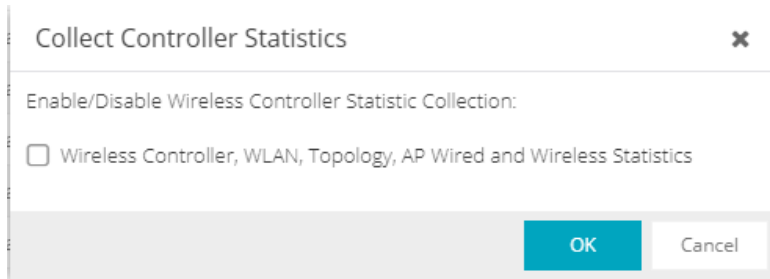
Wireless Controller statistics collection is configured separately from other devices. When you enable Wireless Controller statistics collection, it includes Wireless Controller, WLAN, Topology, and AP wired and wireless statistics, and you also have the option to collect wireless client statistics.

You can enable statistics collection for multiple controllers, however the group cannot contain a mix of devices and wireless controllers. The group must include only controllers.

Enabling Wireless Controller Statistics Collection

Use the following steps to enable wireless controller statistics collection.

1. You can enable statistics collection from either ExtremeCloud IQ - Site Engine or Console:
 - On the **Network** tab, right-click one or more wireless controllers and select **Device > Collect Device Statistics**. You can also click the menu icon (☰) in the upper left corner of the **Network** tab and select **Device > Collect Device Statistics**.
 - In the Console device tree or **Device Properties** tab, right-click one or more wireless controllers and select **OneView > Collect Device Statistics**.
2. From the Collect Controller Statistics window, select the statistics you want to collect.



3. Click **OK**. ExtremeCloud IQ - Site Engine begins collecting statistics for the selected controllers.

Enable Flow Collection

To view ExtremeCloud IQ - Site Engine Flow and Application reports, you must enable NetFlow or application telemetry on the device and enable flow collection for the device interfaces. N-Series, S-Series, and K-Series devices support NetFlow flow collection and ExtremeXOS devices support application telemetry flow collection. You must be a member of an authorization group assigned the NetSight OneView > NetFlow Read/Write Access capability to view NetFlow data or the NetSight OneView > Application Telemetry Read/Write Access capability to view application telemetry data and enable flow collection in ExtremeCloud IQ - Site Engine. Flow collection is only available with the NMS-ADV license.

Enable Flow Collection on a Device

In ExtremeCloud IQ - Site Engine, open the Advanced Configuration panel. Select an ExtremeAnalytics engine and use the **Flow Collection Type** drop-down to select the type of flow collection supported by your device. Use the **Flow Sources** or **Application Telemetry Sources** section of the window (depending on the **Flow Collection Type** selected) to add a device as a flow collection source.

Enable Flow Collection on an Interface

In PortView, you can enable flow collection from the Configure Collection State section of the **Interface Details** tab.

ExtremeCloud IQ - Site Engine Scalability

ExtremeCloud IQ - Site Engine supports reporting on 20,000 objects as determined by the number of devices and interfaces being monitored, along with polling interval and data storage periods. Below are two example network configurations resulting in collected objects under 20,000. For additional information on tuning your deployment, please contact Extreme Networks Support.

Variables		Scenario 1	Scenario 2
Data Retention	Raw Data	7 Days	7 Days
	Hourly Rollups	8 Weeks	8 Weeks
	Daily Rollups	6 Months	6 Months
Polling Interval		15 Minutes	15 Minutes
Devices	Wireless Controllers	5	10
	Wireless APs	1000	2000
	Advanced Switch/Routers	150	50
	Advanced Interfaces	1000	200
	Servers	150	50
Collected Objects		19,450	18,630

ExtremeCloud IQ - Site Engine Timeout

ExtremeCloud IQ - Site Engine automatically times out after a specified amount of time, specified in the **HTTP Session Timeout** section of the Web Server view in the **Administration > Options** tab. A dialog box appears to warn you when you are two minutes from timing out of an ExtremeCloud IQ - Site Engine web page. For additional information, see the Web Server Options Help topic.

NOTE: The ExtremeCloud IQ - Site Engine, ExtremeControl, and ExtremeAnalytics Virtual Engine Installation Guide includes an overview of ExtremeCloud IQ - Site Engine, ExtremeControl, and ExtremeAnalytics [virtual engine deployment requirements](#) and how to deploy a virtual engine on a VMware® and Hyper-V server.

How to Obtain and Apply an ExtremeCompliance License

To use the **Compliance** tab in ExtremeCloud IQ - Site Engine, an additional license is required.

To obtain and apply the license in ExtremeCloud IQ - Site Engine:

1. Contact your sales representative to purchase an ExtremeCompliance license.

An email voucher is generated and sent to you with instructions.

2. Create an Extreme Networks Support Portal account, if necessary.
 - a. Open a browser and go to <https://secure.extremenetworks.com/>.
 - b. Enter your information and click **Create An Account**.

An email is sent to you with instructions to activate your account.

- c. Click the link in your email.

The Portal - Account Activation web page displays.

- d. Enter your **Email Address** and the **Activation Code** included in your activation email, if they do not automatically populate.
- e. Click **Activate**.

3. Access the Extreme Networks Support Portal at <https://extremeportal.force.com/ExtrLicenseLanding>.

4. Enter your **Email** and **Password** and click **Log In**.

5. Click **Generate License**.

The Generate License window displays.

6. Enter your **Voucher ID** from the email voucher sent to you and click **Next**.
7. Select the **Terms and Conditions** checkbox and click **Submit**.

A window displays with your software license key.

8. Copy the license key from the window.

9. Open ExtremeCloud IQ - Site Engine.
10. Access the **Administration** > **Diagnostics** tab.
11. Select **Server** > **Server Licenses** in the left-panel.

The **Server Licenses** panel displays.

12. Click **Add**.

The **Add License** window displays.

13. Paste the license key you copied in Step 9 and click **OK**.
 14. Restart ExtremeCloud IQ - Site Engine.
 15. The **Compliance** tab is now available in the menu, allowing you to use ExtremeCompliance audit functionality.
-

Related Information

For information on related tabs:

- [ExtremeCompliance Overview](#)
- [Diagnostics](#)

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.

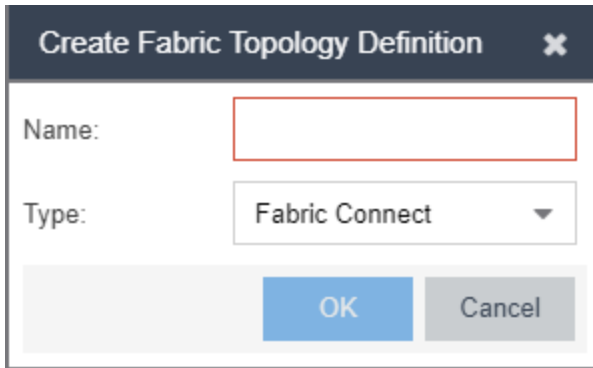
Create a Topology Definition

You can create a [Topology Definition](#) on the **Sites** tab in ExtremeCloud IQ - Site Engine. Once 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 screenshot shows a dialog box titled "Create Fabric Topology Definition". It has a dark header bar with a close button (X). The main area contains two fields: "Name:" with an empty text input field, and "Type:" with a dropdown menu currently set to "Fabric Connect". At the bottom, there are two buttons: "OK" (blue) and "Cancel" (grey).

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

Once 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 screenshot shows the 'Fabric Topology Summary' configuration page for 'topo1'. The interface includes a navigation menu on the left with categories like 'World', 'Fabric', 'XOS-site', 'dvr-site', 'non-dvr-site', 'site1-topo-svcDef', 'Topology Definitions', 'Service Definitions', and 'sd1'. The main content area is divided into three sections:

- Fabric Infrastructure Settings:**
 - IS-IS Manual Area: 49.0000.0000
 - Primary BVLAN: 4051
 - Secondary BVLAN: 4052
- DvR Domain Settings:**

Name	Domain ID
dvr2	2
dvr1	1
- Features:**
 - Multicast
 - IP Shortcuts
 - IPv6 Shortcuts

At the bottom right, there are 'Save' and 'Cancel' buttons.

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 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.

Once the topology definition is created and configured, you can [apply](#) it to a site within your network. Once 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.

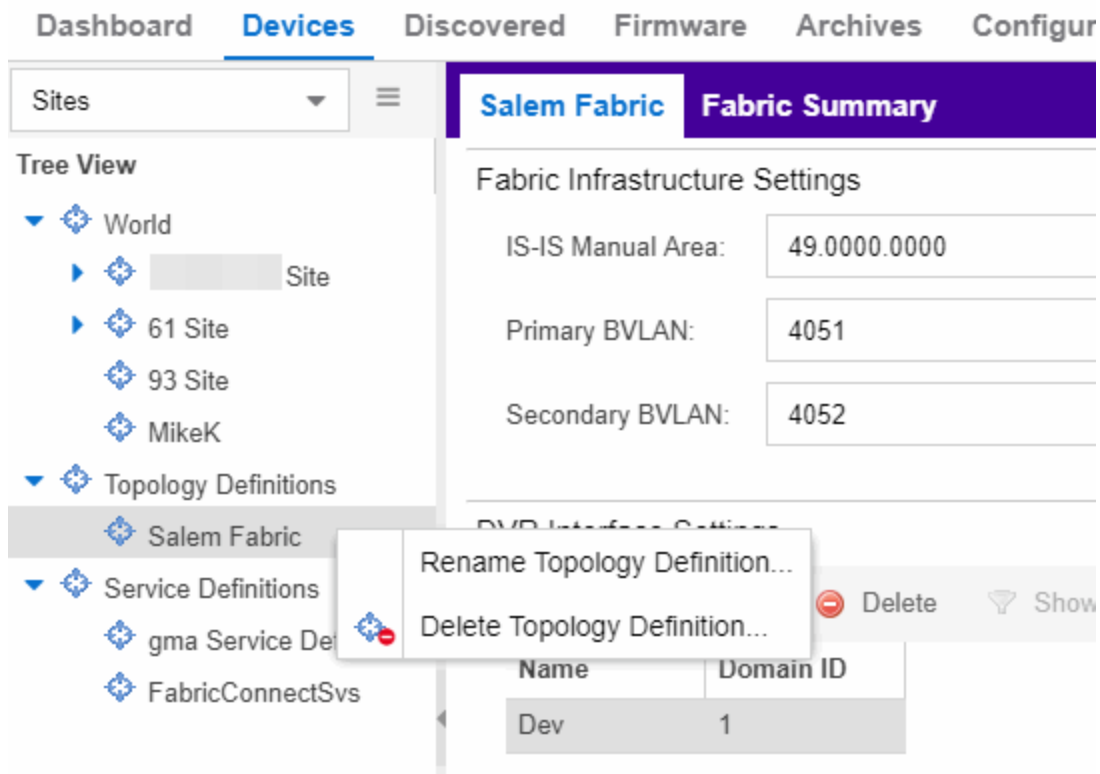
Rename a Topology Definition

Once 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.

- Right-click the topology definition you are renaming.



- Click **Rename Topology Definition**.
- Enter a new name in the **Name** field.
- Click **OK** to change the topology name.

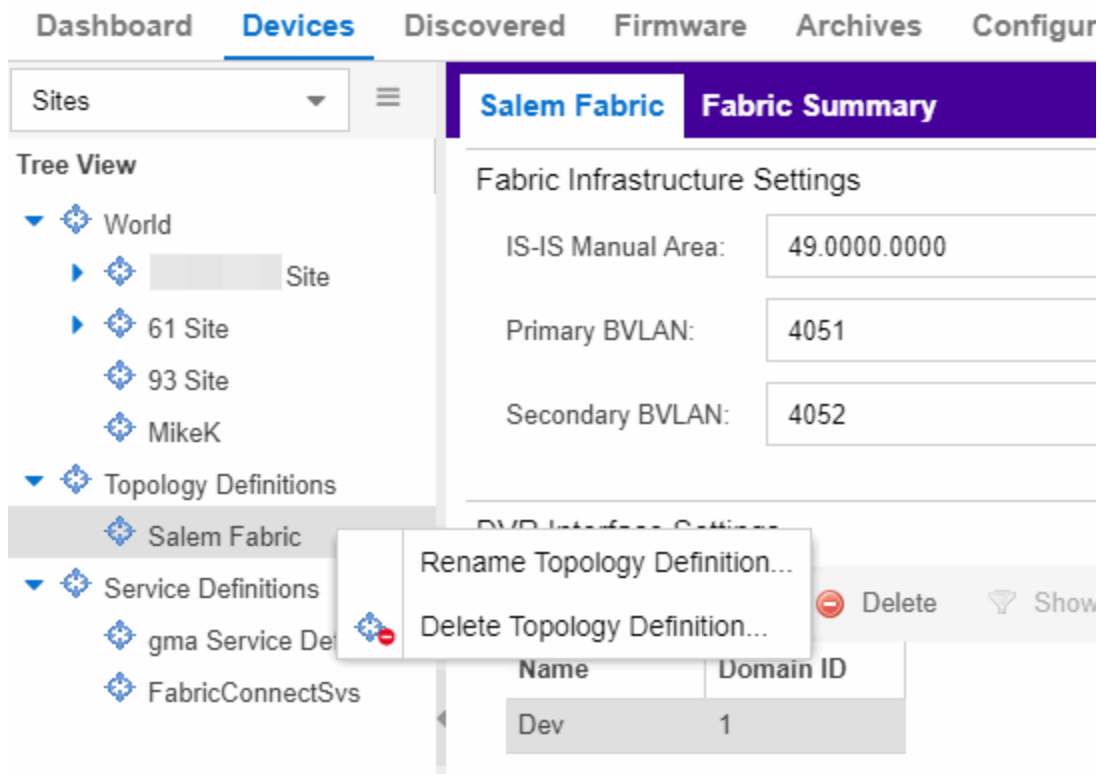
Delete a Topology Definition

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

To delete a topology definition:

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

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



5. Click **Delete Topology Definition**.

6. Click **Yes** to delete the topology definition you selected.

Related Information

For information on related topics:

- [Services](#)
- [Fabric](#)
- [Sites](#)
- [Devices](#)

How to Create a Fabric Service Definition

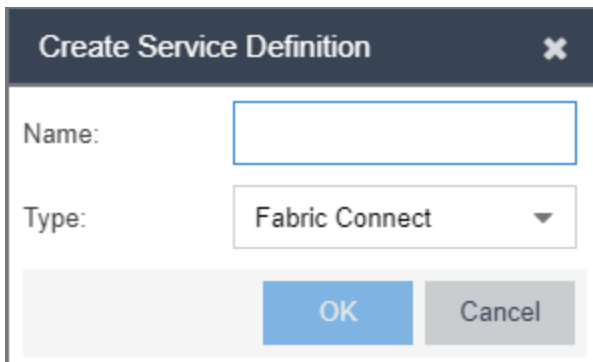
You can create a service definition in the **Sites tab** in ExtremeCloud IQ - Site Engine. Service definitions display information configured in service applications

definitions. Once 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. Click **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. Click **OK** to create the service definition.

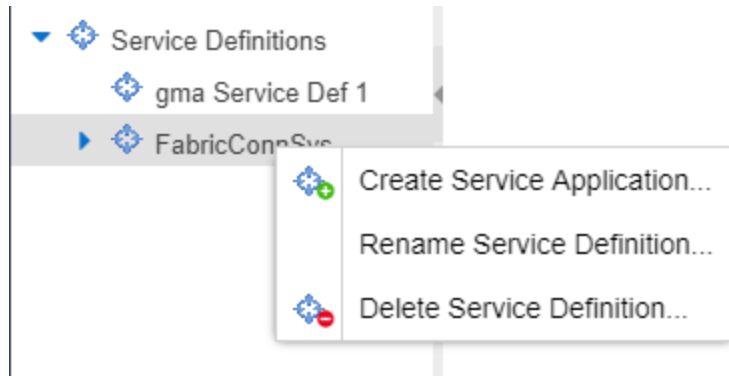
Once the service definition is created and configured, you can [apply](#) it to a site within your network. Once fabric services have been assigned to a site, they cannot be deleted.

Service Definition Panel

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

Rename a Service Definition

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

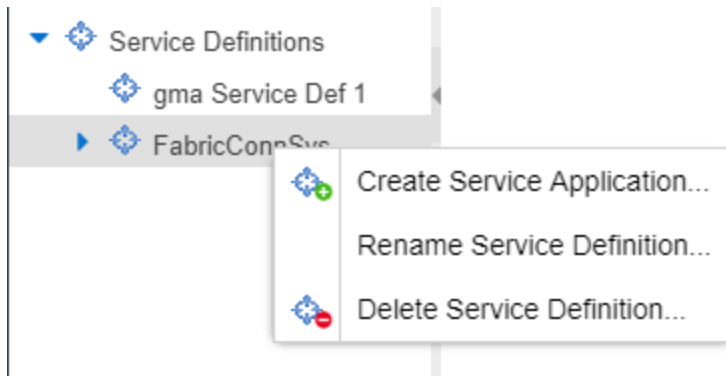


To rename a service definition:

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. Click **Rename Service Definition**.
6. Enter a new name in the **Name** field.
7. Click **OK** to rename the service definition.

Delete a Service Definition

Once 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 once 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. Click **Delete Service Definition**.
6. Click **Yes** to delete a service definition.

Related Information

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 screenshot shows the 'Services' configuration page for 'FabricConnSvsApp'. It features two main sections: 'L2 VSN' and 'L3 VSN'. The 'L2 VSN' section includes a table with columns for Name, Service ID, Flex UNI, VLAN, CVIDs, and Port Template. The 'L3 VSN' section includes a table with columns for Name, Service ID, VRF, Multi Cast, Unicast, and Direct Route. Both sections have 'Add', 'Edit', and 'Delete' buttons, and a 'Show Filters' option. The 'L2 VSN' section also has a 'Service Types' dropdown set to 'All' and a checked 'Extended IGMP Settings' checkbox. At the bottom right, there are 'Save' and 'Cancel' buttons.

The Services tab includes three tabs:

- [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.
- [Service Application Name](#) — Configure the L2 and L3 Virtual Services Networks (VSNs). The **Service Application Name** tab is divided into L2 VPN and L3 VSN tables.

VRF Definition

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

The screenshot shows a configuration window titled "Services" with a sub-tab "Service Summary". The "VRF Definition" tab is active, showing a table with two columns: "Name" and "VRF ID". The table contains one row with "Default" and "0". Above the table are buttons for "Add", "Edit", "Delete", and "Show Filters". At the bottom right are "Save" and "Cancel" buttons.

Name	VRF ID
Default	0

Name

The name of the VRF definition.

VRF ID

The ID number assigned to the VRF definition.

VLAN Definition

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

Services
Service Summary

VRF Definition
VLAN Definition
Topology Service Application

+ Add
 Edit
 Delete
 Show Filters

Name	VID ↑	VRF ID
Default	1	0

<< < | Page of 1 | > >>
 Reset

Save
Cancel

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 VSP 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.

Service Application Name

The **Service Application Name** tab 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.

The screenshot shows a web interface for configuring services. At the top, there is a purple header with 'Services' and 'Service Summary'. Below this, there are tabs for 'VRF Definition', 'VLAN Definition', and 'FabricConnSvsApp'. The main content area is divided into two sections: 'L2 VSN' and 'L3 VSN'. Each section has a toolbar with 'Add', 'Edit', and 'Delete' icons, and a 'Show Filters' button. The 'L2 VSN' section has a 'Service Types' dropdown set to 'All' and a checked 'Extended IGMP Settings' option. Below the toolbars are two tables. The first table, under 'L2 VSN', has columns for Name, Service ID, Flex UNI, VLAN, CVIDs, and Port Template. The second table, under 'L3 VSN', has columns for Name, Service ID, VRF, Multi Cast, Unicast, and Direct Route. At the bottom right, there are 'Save' and 'Cancel' buttons.

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.

Flex UNI

Indicates that the fabric service is using the User-Network-Interface (UNI).

The following interface types are available:

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

VLAN

The VLAN assigned to the fabric service.

CVIDs

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

Port Template

Use the drop-down list to determine the purpose of the port:

- **Access** — Select this option if the port connects to user end-systems.
- **Interswitch** — You can also manually select this option if the port is used to connect to other switches. This option is selected by default if the port detects neighboring switches that are configurable.
- **Management** — Select this option if the port is used to manage network traffic with ExtremeCloud IQ - Site Engine.
- **AP** — Select this option if the port is used to connect with a networking device that allows a Wi-Fi device to connect to a wired network.
- **Phone** — Select this option if the port is used to connect to a telephone.
- **Router** — Select this option if the port is used to connect to a router.

- **Printer** — Select this option if the port is used to connect to a printer.
- **Security** — Select this option if the port is used to connect to a device or devices that have been configured with security or advanced security settings.
- **IoT** — Select this option if the port is used to connect to an additional wireless "smart" device.
- **Other** — Select this option if the port is used to connect to any other device.

DVR Enable

Select to enable distributed virtual routing.

IMPORTANT: A device on which you enable DVR Leaf mode does not support all ExtremeCloud IQ - Site Engine features. DVR Leaf mode is a constrained operating mode for the device and previous configurations defined on a device may no longer function properly.

DVR Gateway

Enter the gateway address of the DVR device.

Multicast Snooping

Select to configure the service to listen to Internet Group Management Protocol (IGMP) network traffic. The feature allows a network switch to listen in on the IGMP conversation between hosts and routers.

Multicast Routing

Select to configure the service to distribute data to multiple recipients. Using multicast, a source can send a single copy of data to a single multicast address, which is then distributed to an entire group of recipients.

IGMP Version

The version of IGMP the service is using: Version 1, 2, or 3.

IGMP Querier

Enter the address of the IGMP Querier. Use this feature when there is no multicast router in the VLAN to originate the queries.

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.

Related Information

For information on related topics:

- [Service Summary](#)
- [Fabric](#)
- [Sites](#)

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 VSP 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

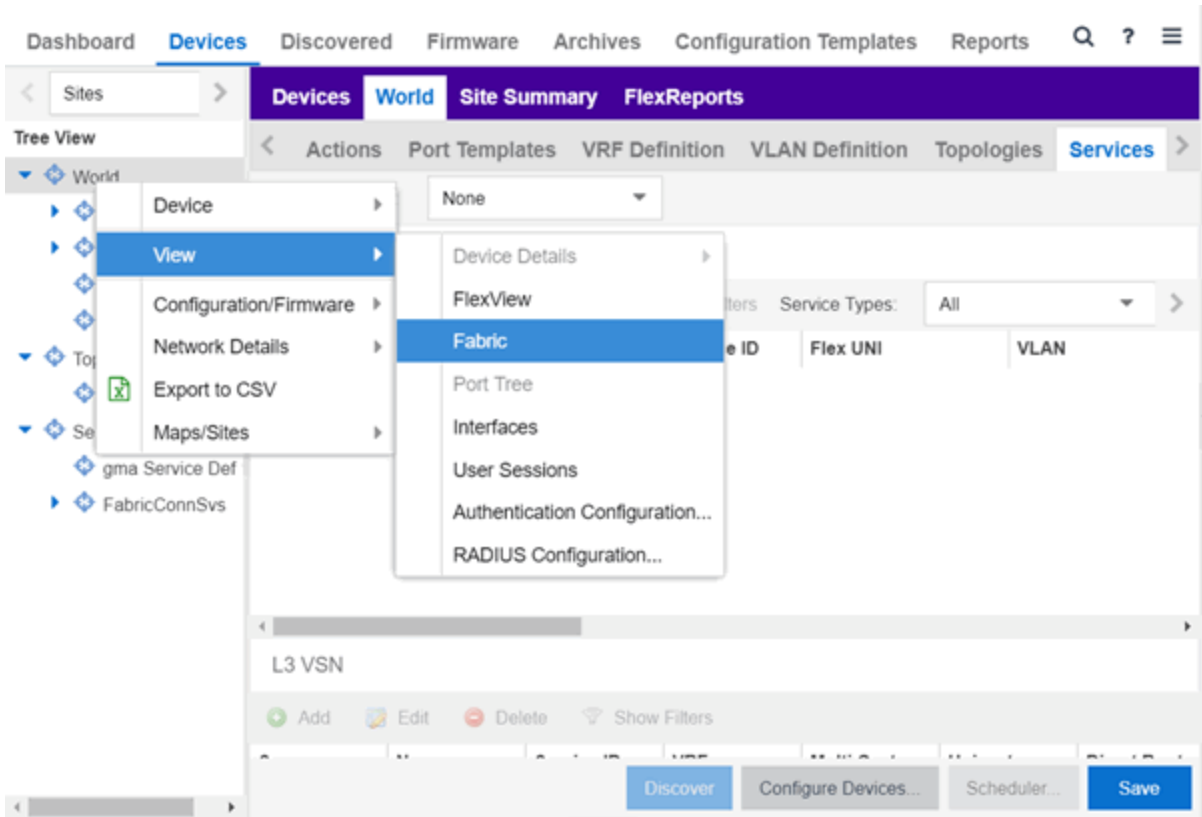
For minimum requirements, see ExtremeCloud IQ - Site Engine Configuration and Requirements.

Accessing Fabric in ExtremeCloud IQ - Site Engine

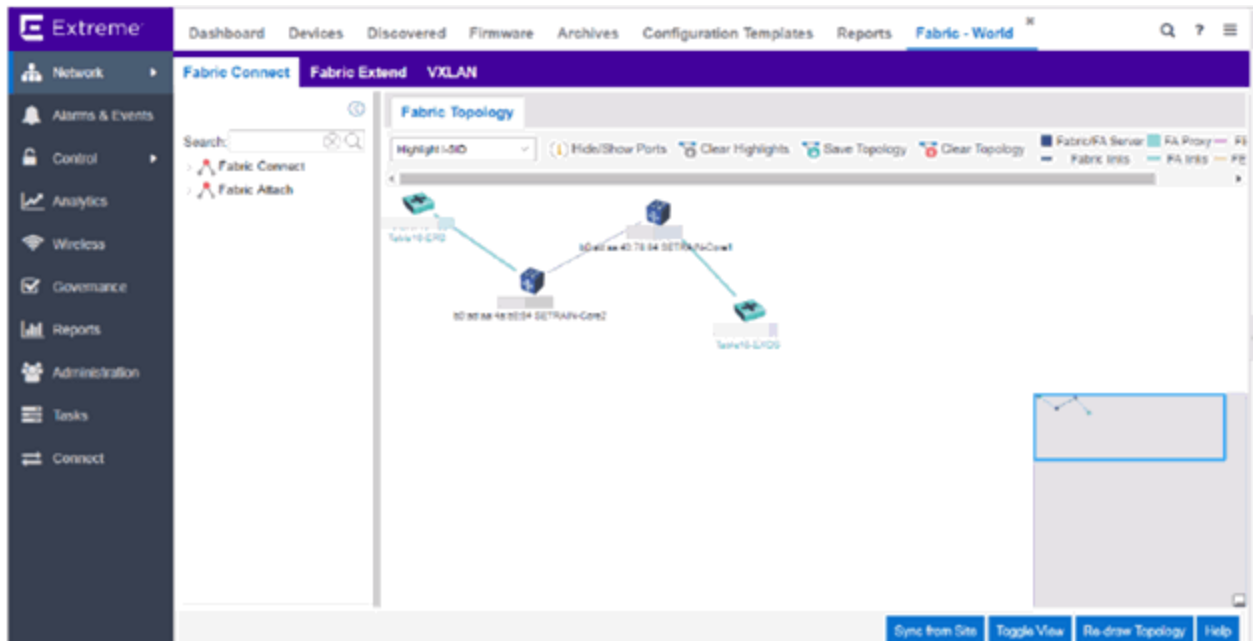
After adding the Fabric Manager engine in ExtremeCloud IQ - Site Engine, view the fabric topologies configured on your devices on the **Fabric** tab.

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 **View > Fabric** from the menu.



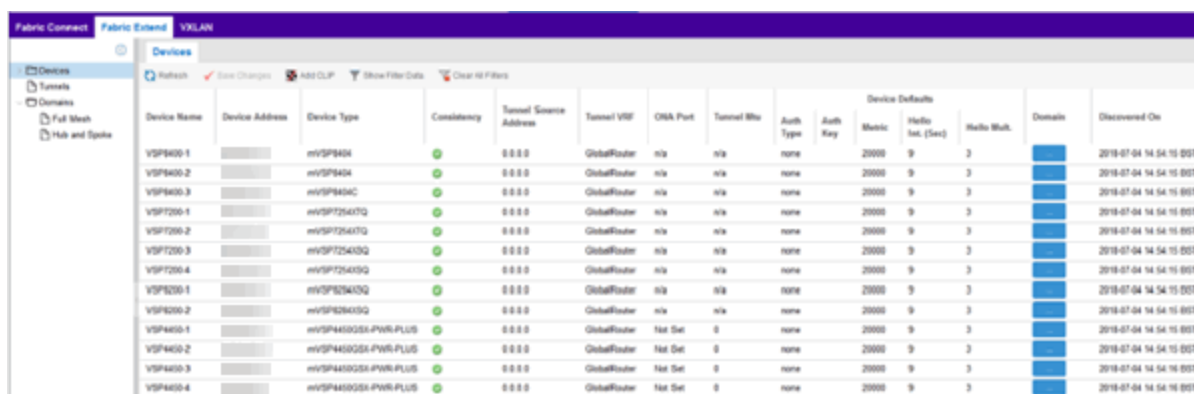
The Fabric tab opens.



Fabric Tab

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

- Fabric Connect – Displays the fabric topologies configured on your fabric-enabled devices.
- Fabric Extend – Allows you to extend fabric functionality to include Layer 2 and Layer 3 core networks.



Device Name	Device Address	Device Type	Consistency	Tunnel Source Address	Tunnel VRF	ONA Port	Tunnel Mtu	Auth Type	Auth Key	Device Defaults	Domain	Discovered On	
										Metric	Hello Int. (Sec)	Hello Mult.	
VSP400-1		svVSP400	Consistent	0.0.0.0	GlobalRouter	v1a	v1a	none		20000	9	3	2019-07-04 14:54:15 BST
VSP400-2		svVSP400	Consistent	0.0.0.0	GlobalRouter	v1a	v1a	none		20000	9	3	2019-07-04 14:54:15 BST
VSP400-3		svVSP400	Consistent	0.0.0.0	GlobalRouter	v1a	v1a	none		20000	9	3	2019-07-04 14:54:15 BST
VSP7200-1		svVSP7200	Consistent	0.0.0.0	GlobalRouter	v1a	v1a	none		20000	9	3	2019-07-04 14:54:15 BST
VSP7200-2		svVSP7200	Consistent	0.0.0.0	GlobalRouter	v1a	v1a	none		20000	9	3	2019-07-04 14:54:15 BST
VSP7200-3		svVSP7200	Consistent	0.0.0.0	GlobalRouter	v1a	v1a	none		20000	9	3	2019-07-04 14:54:15 BST
VSP7200-4		svVSP7200	Consistent	0.0.0.0	GlobalRouter	v1a	v1a	none		20000	9	3	2019-07-04 14:54:15 BST
VSP9200-1		svVSP9200	Consistent	0.0.0.0	GlobalRouter	v1a	v1a	none		20000	9	3	2019-07-04 14:54:15 BST
VSP9200-2		svVSP9200	Consistent	0.0.0.0	GlobalRouter	v1a	v1a	none		20000	9	3	2019-07-04 14:54:15 BST
VSP4400-1		svVSP4400-PLUS	Consistent	0.0.0.0	GlobalRouter	Net Set	0	none		20000	9	3	2019-07-04 14:54:15 BST
VSP4400-2		svVSP4400-PLUS	Consistent	0.0.0.0	GlobalRouter	Net Set	0	none		20000	9	3	2019-07-04 14:54:15 BST
VSP4400-3		svVSP4400-PLUS	Consistent	0.0.0.0	GlobalRouter	Net Set	0	none		20000	9	3	2019-07-04 14:54:15 BST
VSP4400-4		svVSP4400-PLUS	Consistent	0.0.0.0	GlobalRouter	Net Set	0	none		20000	9	3	2019-07-04 14:54:15 BST

- VXLAN – Allows you to configure a Virtual Extensible LAN (VXLAN) to tunnel Layer 2 traffic over a Layer 3 network in the fabric topologies you configure.

Related Information

For information on related topics:

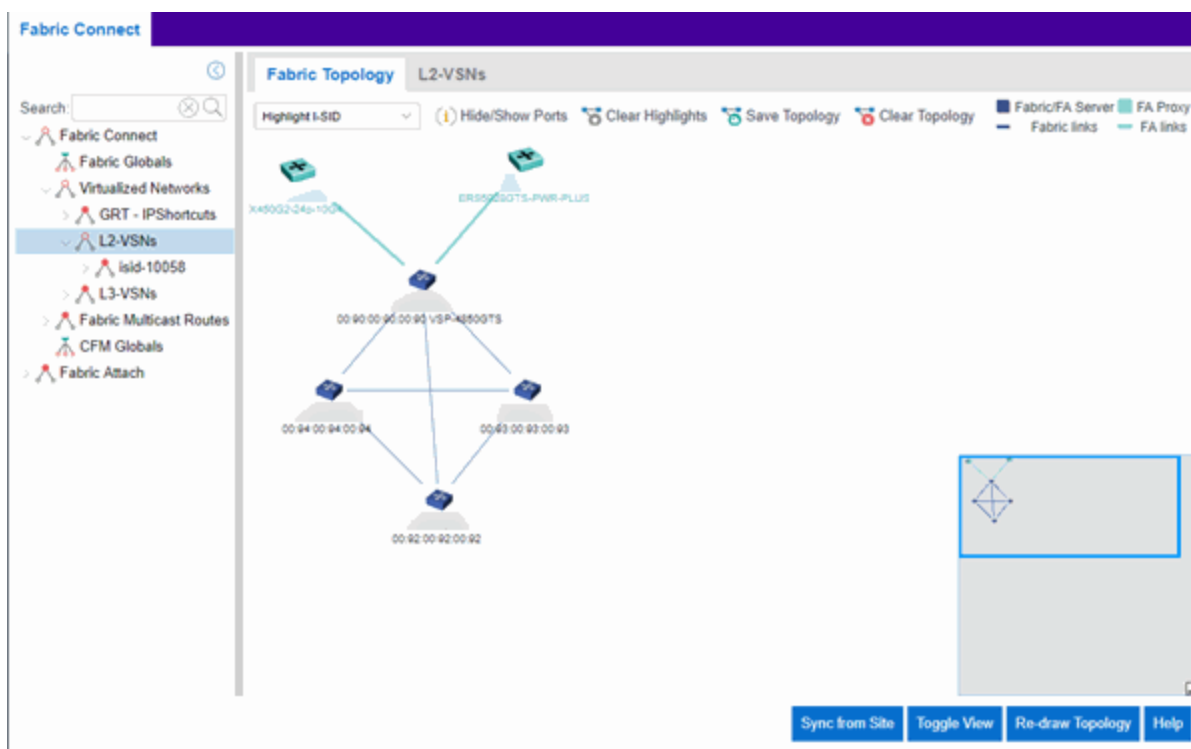
- [Services](#)
- [Service Summary](#)
- [Fabric Connect](#)
- [Fabric Assist](#)
- [Sites](#)
- [Devices](#)

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 and configure 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.



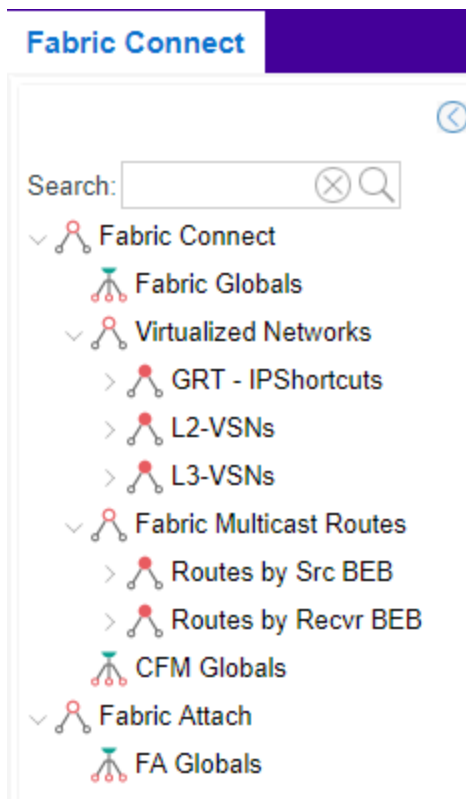
The Fabric Connect tab is divided into two sections: the [left-panel tree](#) view and a Fabric Topology [right-panel map](#) view.

Left-Panel Tree

Beginning in version 21.04.10, 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.

The screenshot shows the 'Fabric Connect' interface with the 'L2-VSNs' tab selected. The left-hand navigation tree includes 'Fabric Connect', 'Fabric Globals', 'Virtualized Networks', 'GRT - IPShortcuts', 'L2-VSNs', 'L3-VSNs', 'BGP-VPNs', 'Fabric Multicast Routes', 'CFM Globals', and 'Fabric Attach'. The main panel displays a table of L2-VSNs with the following data:

SysName	IPAddress	I-SID	UNIType
SETRAIN-Core1		12930	C-VLAN UNI
SETRAIN-Core1		12420	C-VLAN UNI
SETRAIN-Core1		121220	C-VLAN UNI
SETRAIN-Core1		12810	C-VLAN UNI
SETRAIN-Core1		121610	C-VLAN UNI, Flex UNI
SETRAIN-Core2		121610	Flex UNI
SETRAIN-Core1		12430	C-VLAN UNI
SETRAIN-Core1		121230	C-VLAN UNI
SETRAIN-Core1		12820	C-VLAN UNI
Table16-ERS		121620	C-VLAN UNI
SETRAIN-Core1		121620	C-VLAN UNI, Flex UNI
SETRAIN-Core2		121620	Flex UNI
SETRAIN-Core1		12310	C-VLAN UNI
SETRAIN-Core1		121110	C-VLAN UNI
SETRAIN-Core1		12830	C-VLAN UNI
SETRAIN-Core1		121630	C-VLAN UNI, Flex UNI
SETRAIN-Core1		12320	C-VLAN UNI

53 Rows

Buttons: Sync from Side, Toggle View, Re-draw Topology, Help

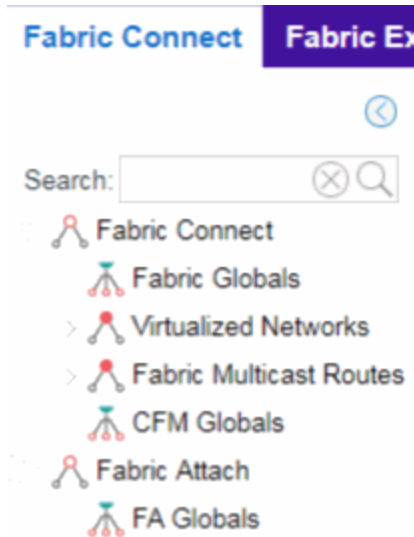
Select the **Toggle View** button to display Fabric Connect fabric services for individual devices.

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:

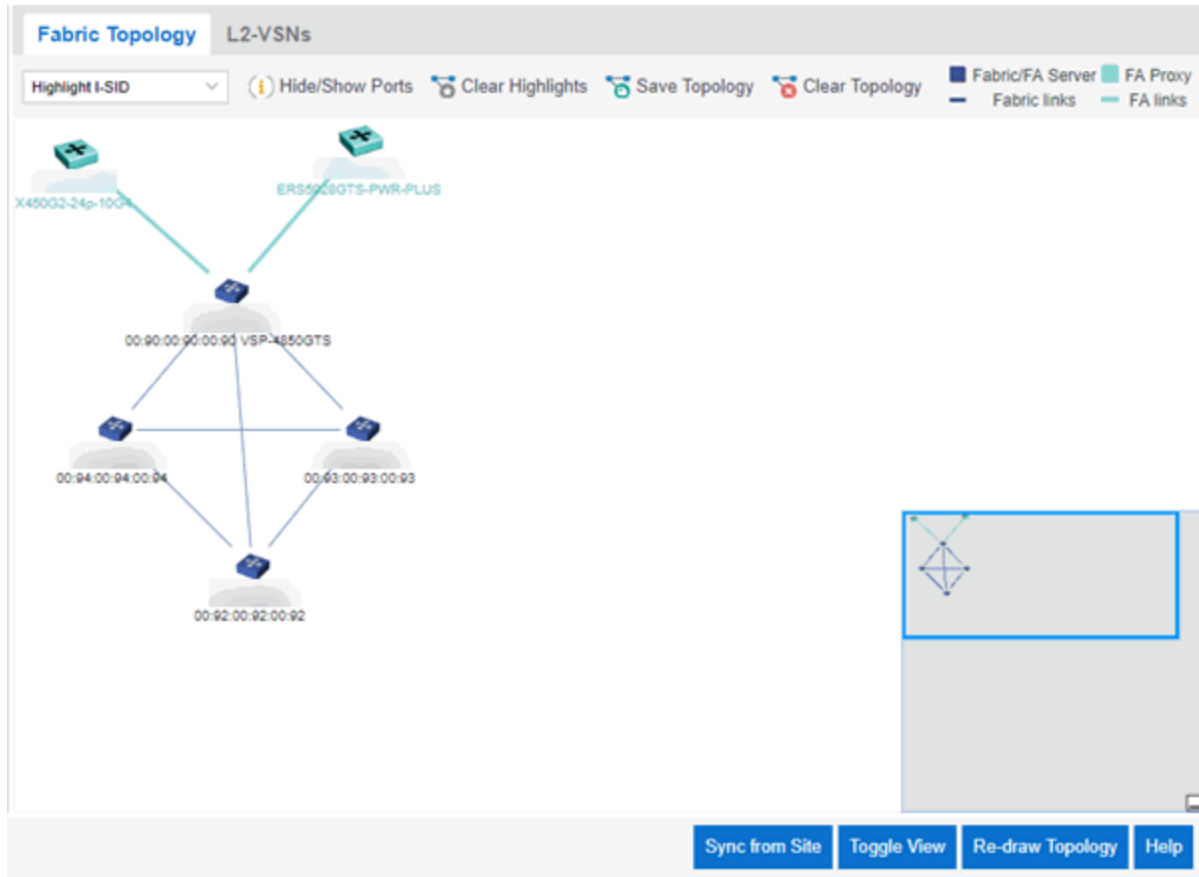
FA Server — for VOSS, ERS 49xx v5.9.2 and later, ERS 4850 v5.9.2 and later, and ERS 59xx series devices; FA Proxy (client proxy) — for ERS 35xx, ERS 48xx, ERS 49xx, ERS 55xx, ERS 56xx, ERS 59xx, and VSP 70xx series devices; FA Standalone Proxy (client proxy) — for ERS 35xx, ERS 48xx, ERS 55xx, ERS 56xx,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

Related Information

For information on related topics:

- [Services](#)
- [Service Summary](#)
- [Sites](#)
- [Devices](#)
- [Fabric Assist](#)

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](#).

Related Information

For information on related topics:

- [Sites](#)
- [Profiles](#)
- [Add Device](#)
- [Edit Device](#)
- [Devices](#)

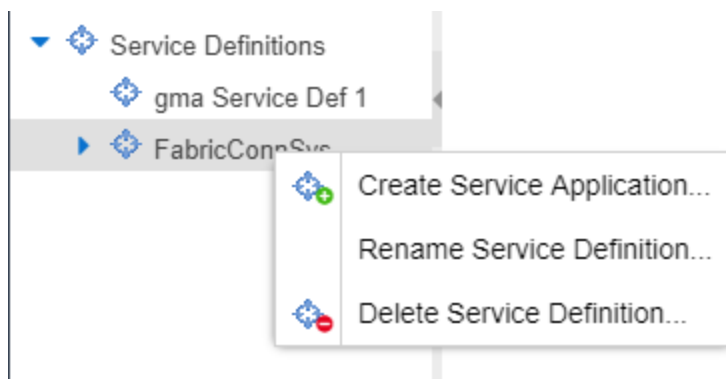
How to Create a Service Application

You can create a service application via the **Sites** tab in ExtremeCloud IQ - Site Engine. Service definitions display information from service applications. Once 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. Click **Create Service Application**.

The **Create Service Application** window opens.

6. Enter a name in the **Name** field.
7. Click **OK**.
8. Click 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. Once the service application is created and configured, you can [apply](#) it to a site within your network. Once services have been assigned to a site, they cannot be deleted.

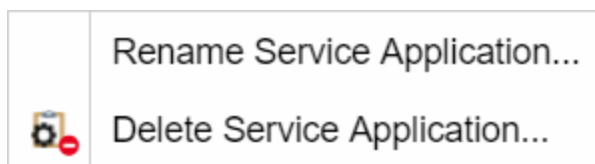
NOTE: A Service Application must have the same fabric type as its associated Service Definition. For example, if a Service Definition is created with Fabric Connect type, it can only have Service Applications of Fabric Connect type. Currently, Fabric Connect is the only fabric type available.

Once 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:

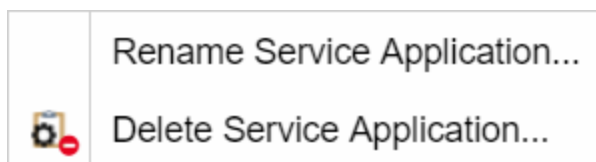
1. Open the **Devices** tab.
2. Select **Sites** from the left-panel tree drop-down list.
3. Expand **Service Definitions** in the left-panel.
4. Right-click the service application you are renaming.



5. Click **Rename Service Application**.
6. Enter a new name in the **Name** field.
7. Click **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. Click **Delete Service Application**.
 6. Click **Yes** to delete the service application.
-

Related Information

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.

The screenshot shows the ExtremeCloud IQ Administration console. The top navigation bar includes tabs for Profiles, Users, Server Information, Certificates, Options, Device Types, Backup/Restore, Diagnostics, and Client API Access. The Profiles tab is active, displaying a table of profiles and a list of CLI Credentials.

Name	SNMP Version	Read Credential	Write Credential	Max Access Credential	Read Security Level
public_v1_Profile	SNMPv1	public_v1	public_v1	public_v1	
EXTR_v1_Profile	SNMPv1	public_v1	private_v1	private_v1	
public_v2_Profile	SNMPv2	public_v2	public_v2	public_v2	
EXTR_v2_Profile	SNMPv2	public_v2	private_v2	private_v2	
snmp_v3_profile	SNMPv3	default_snmp_v3	default_snmp_v3	default_snmp_v3	AuthPriv
VOSS_v1_Profile	SNMPv1	public_v1	private_v1	private_v1	

The CLI Credentials tab is selected, showing a table with the following data:

Description	User Name	Type
Default	admin	Telnet
< No Access >		
Default RWA	rwa	Telnet
Default BOSS ESM	admin	SSH
Default BOSS 4800	RW	Telnet

The **Add CLI Credential** dialog box is open, showing the following fields:


- Description:
- User Name:
- Type:
- Login Password:
- Enable Password:
- Configuration Password:

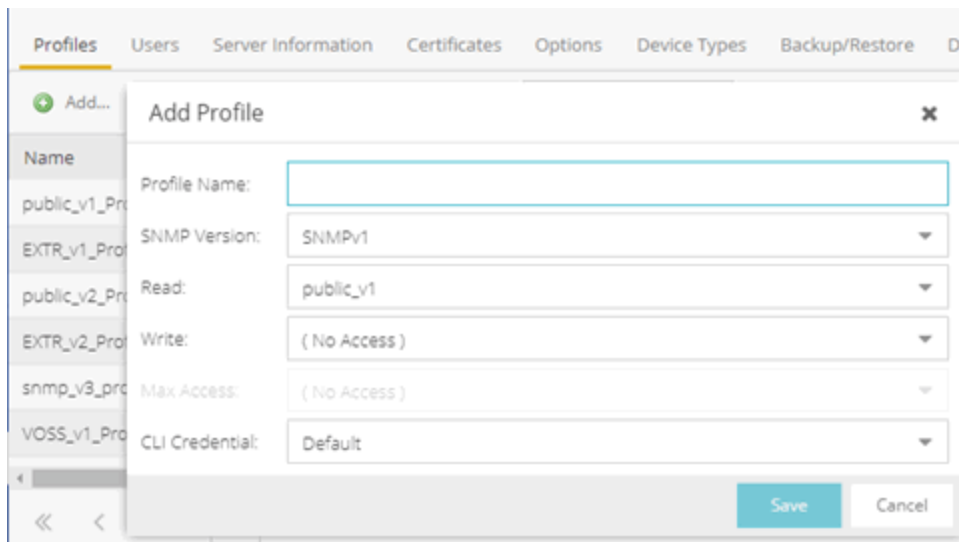
Buttons for Save and Cancel are visible at the bottom of the dialog.

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. Click **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. Click 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, click the **Add Devices** button (the **Add Device** window appears), and click 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**.

Related Information

- [ExtremeCloud IQ - Site Engine Fabric](#)
- [Fabric Connect](#)

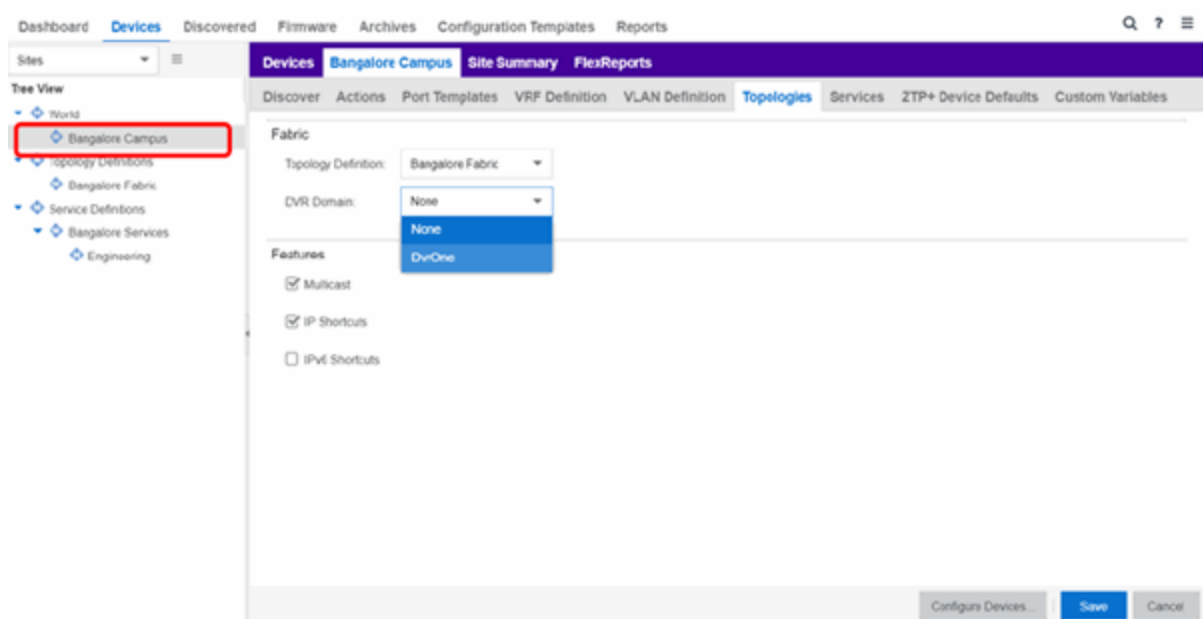
Applying Fabric Services

Once you have created and configured your fabric topology, service and service application services, you can apply them to sites within your network. Once 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.

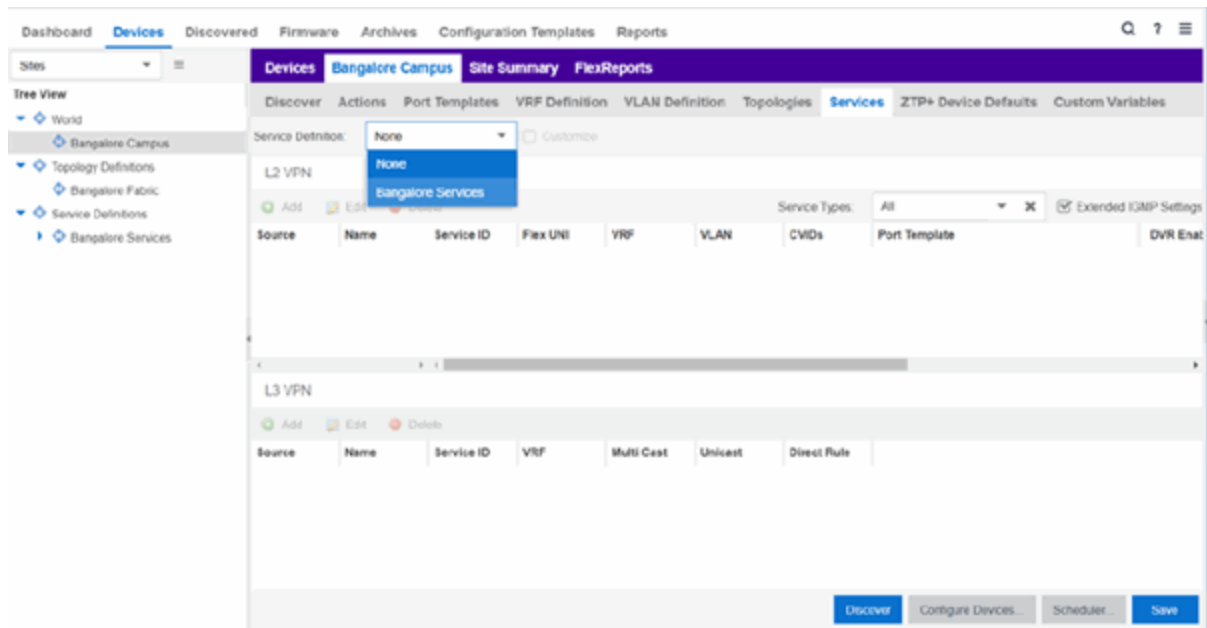


5. Select the **Topologies** tab.
6. Select the topology you want to apply to the site from the **Topology Definition** drop-down list.
7. Select the DVR Domain from the **DVR Domain** drop-down list.
8. Select the check boxes in the **Features** section to include the features you want to assign to the topology.
9. 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. Click a site in the left-panel tree.
4. Click 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

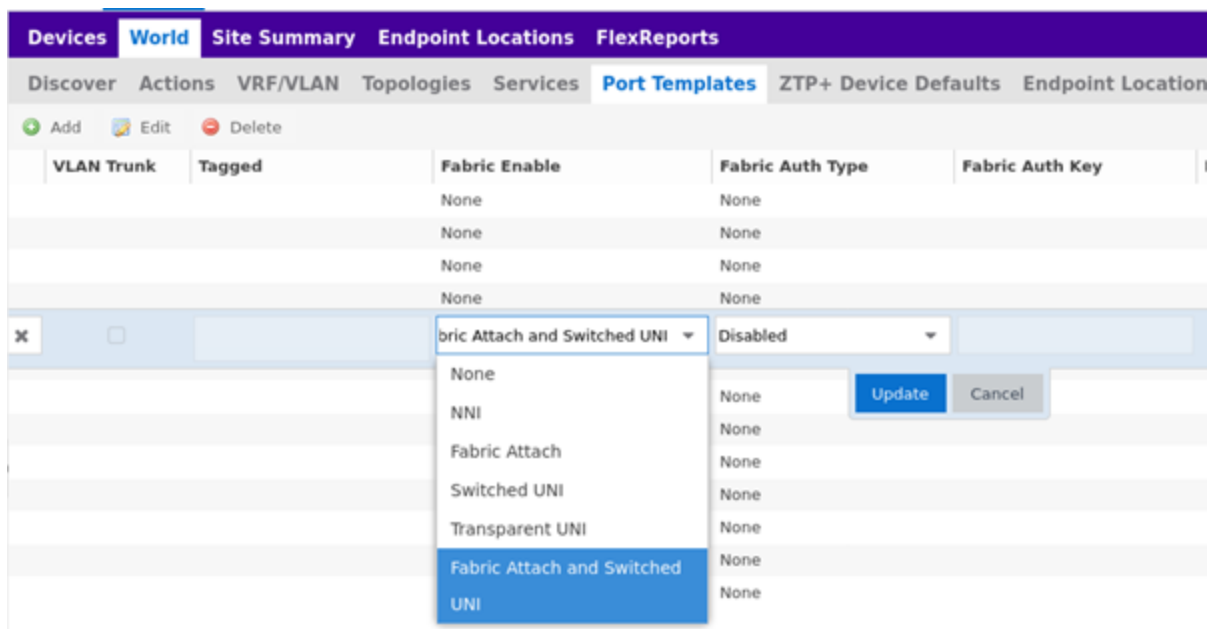
The Port Templates Configuration window enables you to configure ports with a Fabric role. Once complete, you can apply the Port Templates configuration to a device.

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 a port template:

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

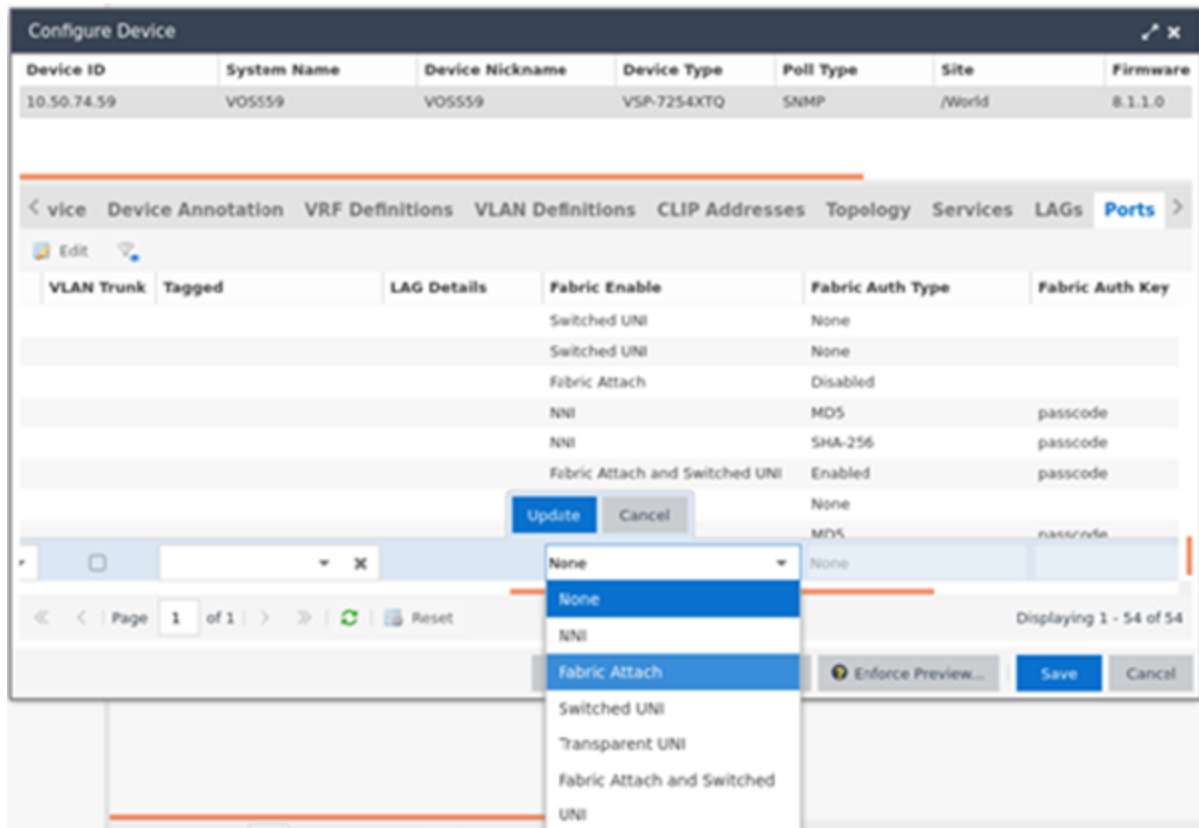
The Port Configuration window enables you to edit the fabric information about the ports on a device.

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.

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 a port template:

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

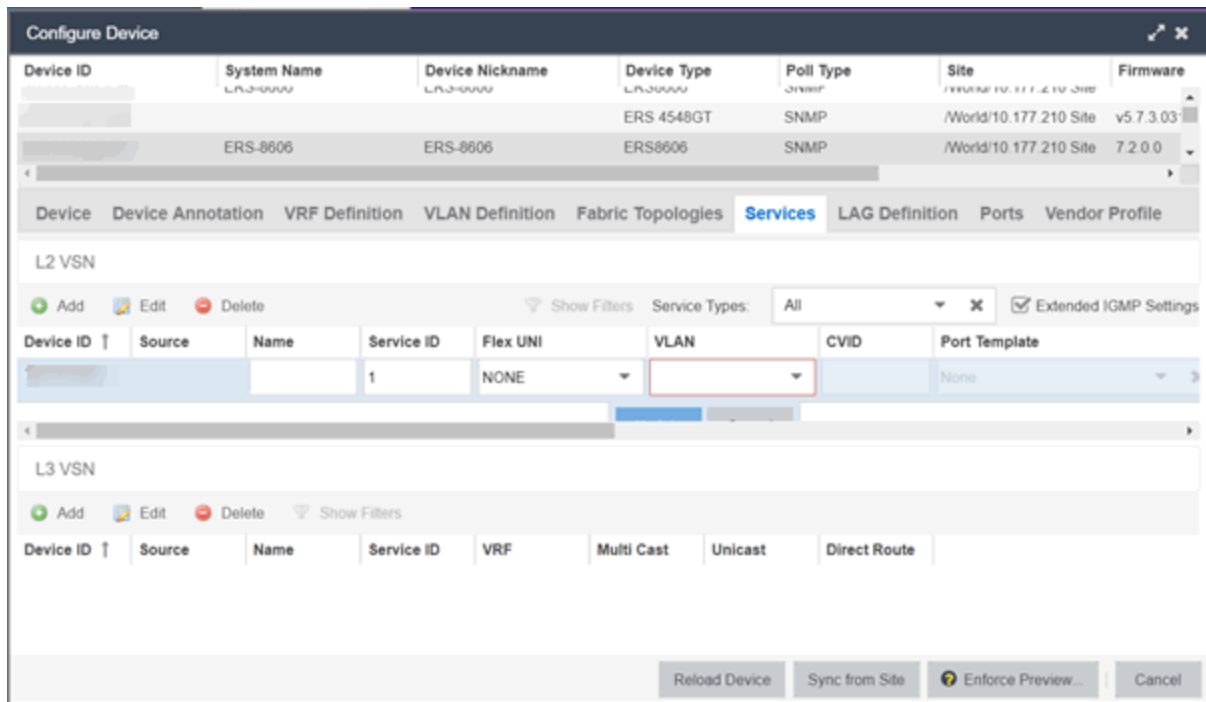
Once you have applied fabric topologies and services to a site, you can also apply the fabric services to devices assigned to that site.



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. Click **Configure Device** from the drop-down list. The **Configure Device** window opens.
5. Click the **Fabric Topologies** tab.
6. Click 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, click 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. Click 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. Click **Configure Device** from the drop-down list. The **Configure Device** window opens.



5. Click the **Services** tab. The service details that you configured to the site display in the L2 VPN and L3 VPN tables.
6. Click 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. Click the Add ( **Add**) button to add an L2 VSN or L3 VSN service to the device.
8. Click the Edit ( **Edit**) button to edit service details that were populated from the site.
9. Click 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. Click **Configure Device** from the drop-down list. The **Configure Device** window opens.
5. Click the **VRF Definition** tab.

The screenshot shows the 'Configure Device' window with the 'VRF Definition' tab selected. The window has a dark header with the title 'Configure Device' and a close button. Below the header is a table with columns: 'Device ID', 'System Name', 'Device Nickname', 'Device Type', and 'Poll Type'. Underneath the table is a navigation bar with tabs: 'Device', 'Device Annotation', 'VRF Definition' (highlighted), 'VLAN Definition', 'Services', and 'Fabric Topologies'. Below the navigation bar are action buttons: 'Add' (with a green plus icon), 'Edit' (with a pencil icon), 'Delete' (with a red minus icon), and 'Show Filters' (with a filter icon). The main area contains a table with columns: 'Device ID ↑', 'Name', and 'VRF ID'. The 'Name' field is empty and has a red border, and the 'VRF ID' field contains the number '1'. Below the table are 'Update' and 'Cancel' buttons. At the bottom of the window are 'Reload Device', 'Sync from Site', 'Enforce Preview...' (with a question mark icon), and 'Cancel' buttons.

The **VRF Definition** 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.

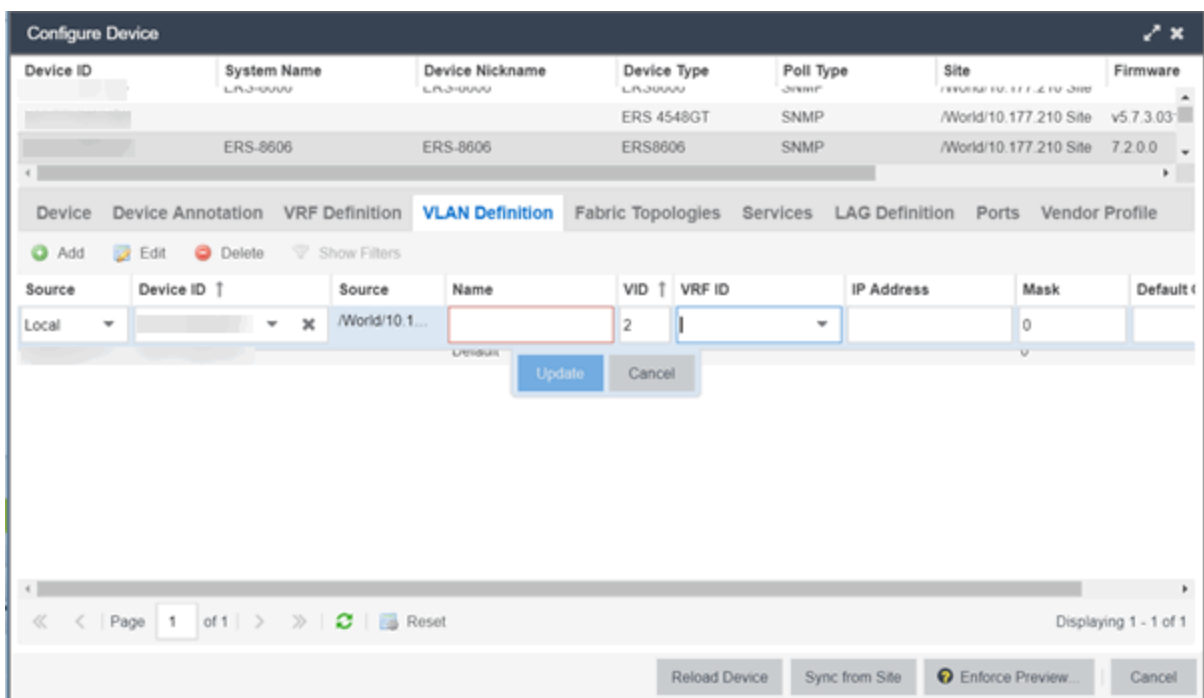
1. Click the Add ( **Add**) button.
2. Enter the name of a VRF in the **Name** field.
3. Enter the ID number in the **VRF ID** field.
4. Click **Update** to add the VRF to the device.
5. Click the **Enforce Preview** button.

You can delete a VRF from the **VRF Definition** tab.


1. Select a VRF in the table.
2. Click the **Delete** ( **Delete**) button.
3. Click **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. Click **Configure Device** from the drop-down list. The **Configure Device** window opens.
5. Click the **VLAN Definition** tab.



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

You can delete a VLAN from the **VLAN Definition** tab.

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

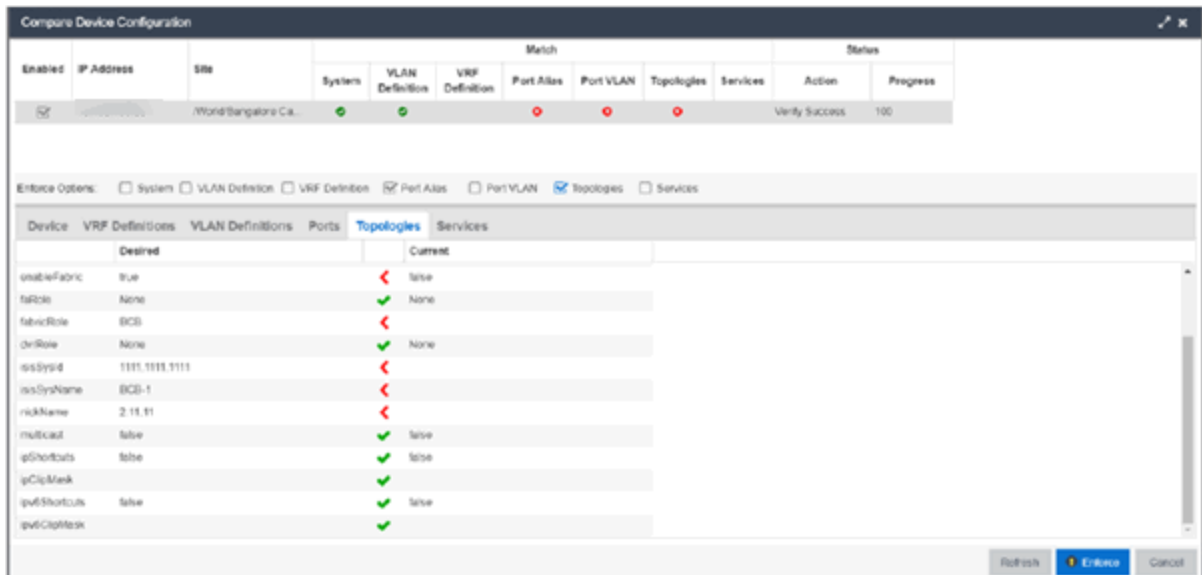
Enforcing the Fabric Configurations

Once you enforce previews on the **Topologies**, **Services**, and **VRF Definitions** 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 Topology

1. Click **Enforce Preview** on the **Topologies** tab in the **Configure Device** window.

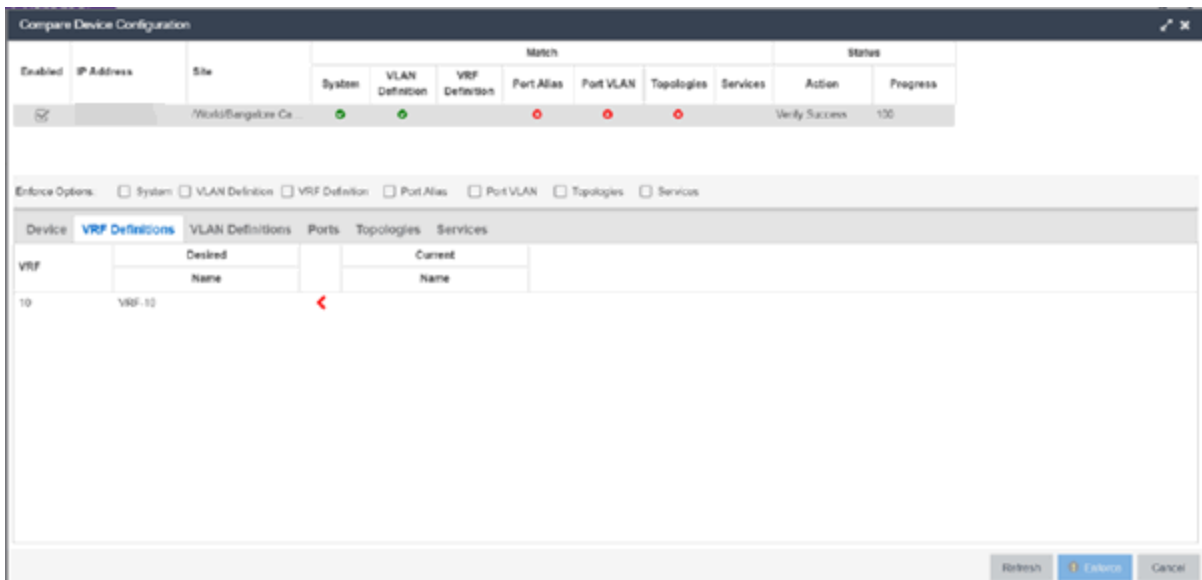
- The **Compare Device** window opens.



- Click the **Topologies Enforce Option**.
- Click **Enforce**.

Enforcing Fabric VRF

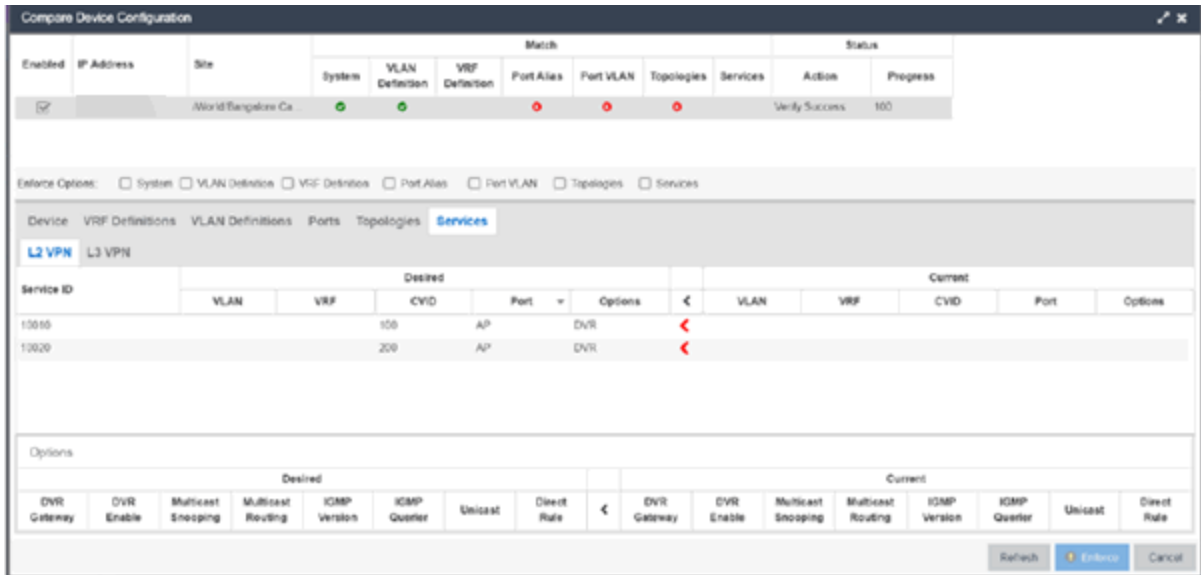
- Click **Enforce Preview** on the **VRF** tab in the **Configure Device** window.
- The **Compare Device** window opens.



3. Click the **VRF Definition** tab.
4. Click **Enforce**.

Enforcing Fabric Services

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

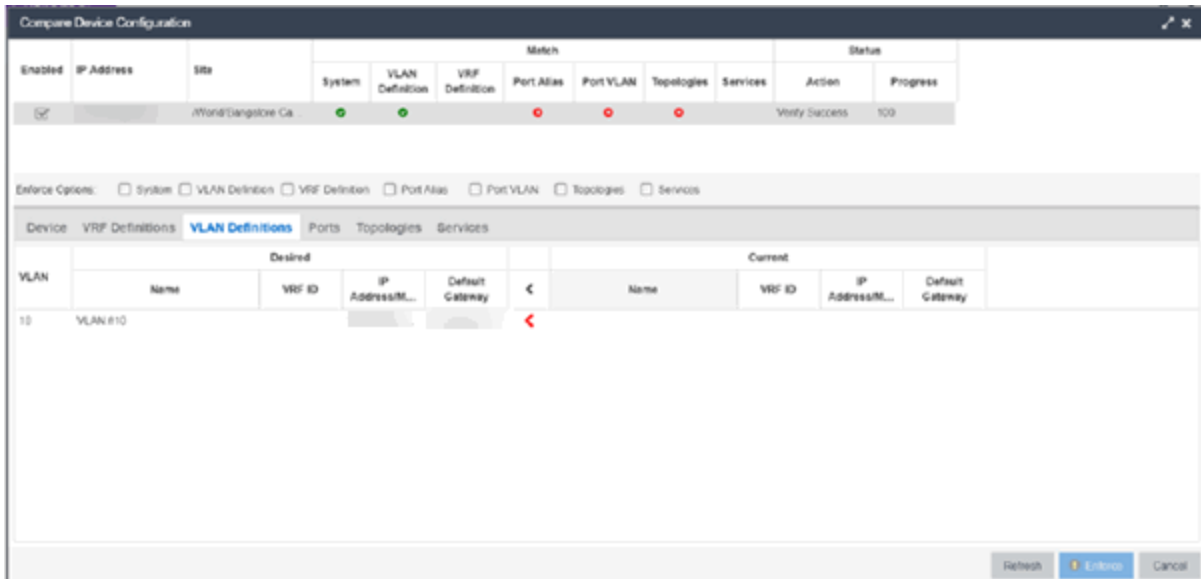


3. Click the **Services Enforce** Option.
4. Click the **L2 VPN** tab.
5. Click **Enforce**.
6. Click the **L3 VPN** tab.
7. Click **Enforce**.

Enforcing Fabric VLAN

1. Click **Enforce Preview** on the **VLAN** tab in the **Configure Device** window.

2. The **Compare Device** window opens.

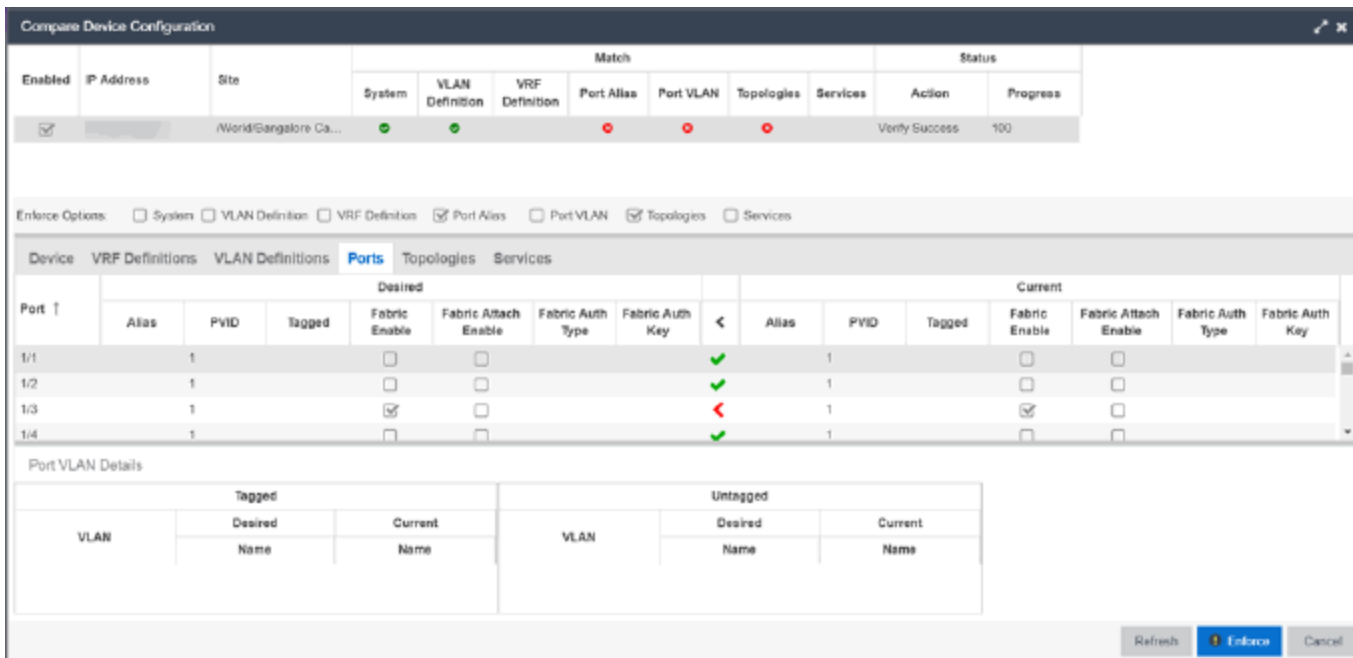


3. Click the VLAN Definition Enforce Option.
4. Click **Enforce**.

Enforcing Fabric Port

1. Click **Enforce Preview** on the **Ports** tab in the **Configure Device** window.

2. The **Compare Device** window opens.



3. Click the Ports Enforce Option.

4. Click **Enforce**.

Related Information

- [Services](#)
- [Fabric](#)
- [Sites](#)
- [Devices](#)

Service Summary

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

Path	Name	Service ID	VRF	VLAN	Sites
<div style="display: flex; justify-content: space-between; align-items: center;"> <input type="text"/> Show Filters </div>					

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.

Related Information

For information on related topics:

- [Services](#)
- [Fabric](#)
- [Sites](#)

Fabric Topology Definition on the Sites Tab

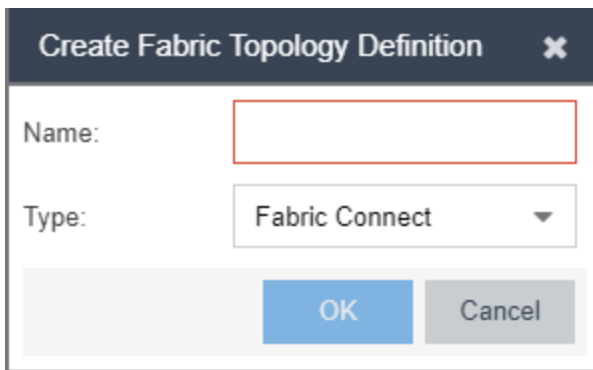
Use the **Fabric Topology Definition** tab to [create](#) a fabric topology definition, [configure](#) fabric topology settings, and [review](#) fabric topology paths and sites. You can also [rename](#) or [delete](#) a fabric topology definition.

Create a Topology Definition

You can create a [Topology Definition](#) on the **Sites** tab in ExtremeCloud IQ - Site Engine. Once 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 screenshot shows a dialog box titled "Create Fabric Topology Definition". It has a dark header bar with a close button (X). The main area contains two labels: "Name:" followed by an empty text input field, and "Type:" followed by a dropdown menu currently showing "Fabric Connect". At the bottom, there are two buttons: "OK" (highlighted in blue) and "Cancel" (greyed out).

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

Once 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 screenshot shows the 'Fabric Topology Summary' configuration page for 'topo1'. The page is divided into three main sections: Fabric Infrastructure Settings, DvR Domain Settings, and Features.

Fabric Infrastructure Settings:

- IS-IS Manual Area: 49.0000.0000
- Primary BVLAN: 4051
- Secondary BVLAN: 4052

DvR Domain Settings:

Buttons: Add, Edit, Delete, Refresh

Name	Domain ID
dvr2	2
dvr1	1

Features:

- Multicast
- IP Shortcuts
- IPv6 Shortcuts

Buttons: Save, Cancel

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 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.

Once the topology definition is created and configured, you can [apply](#) it to a site within your network. Once 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.

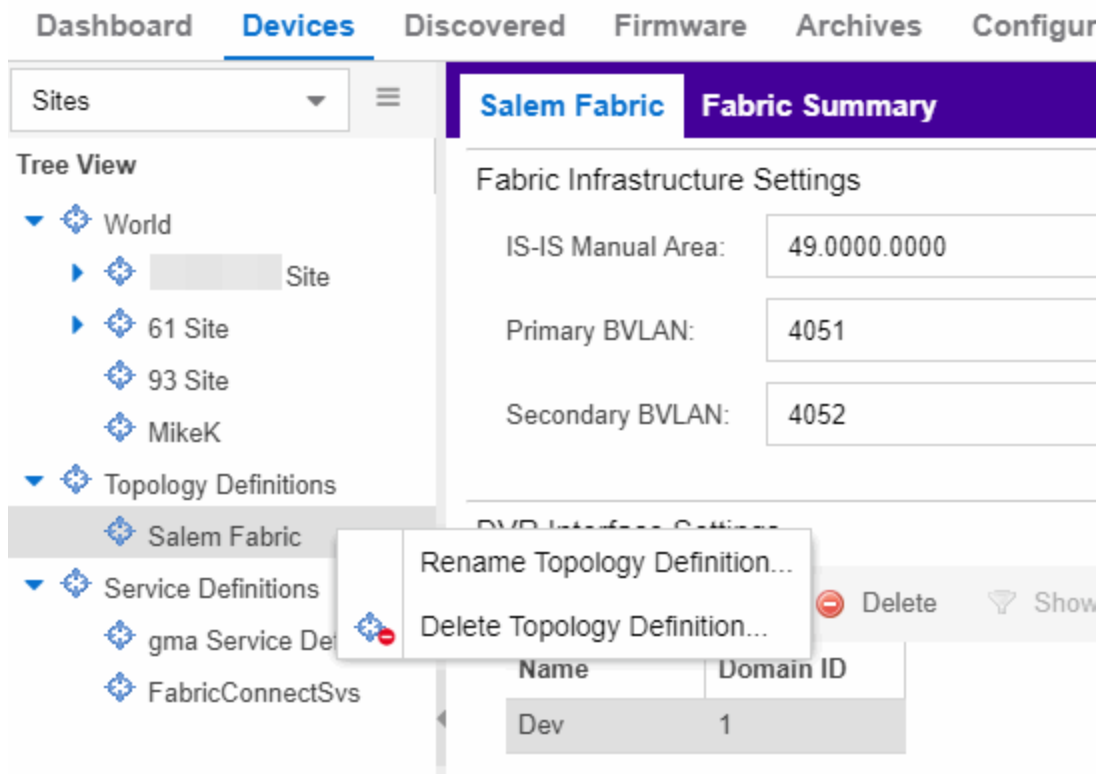
Rename a Topology Definition

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

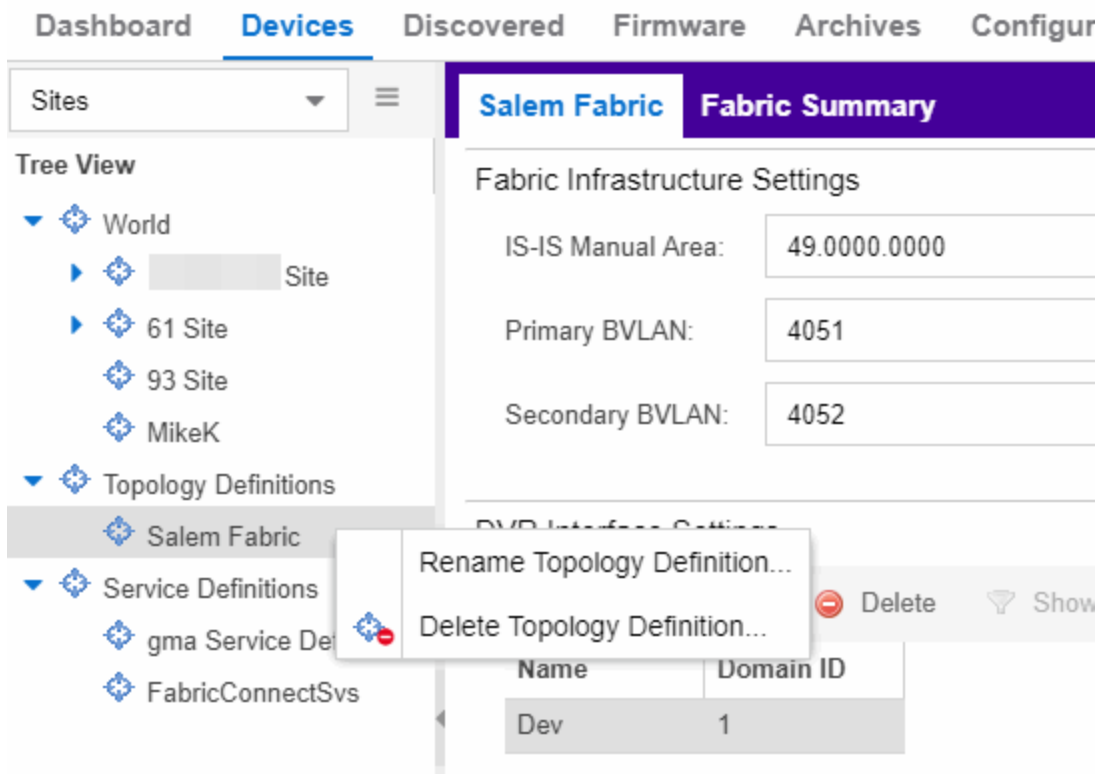
Delete a Topology Definition

Once a topology definition has been created and configured, you can delete it; however, a topology definition cannot be deleted once 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. Click **Delete Topology Definition**.

6. Click **Yes** to delete the topology definition you selected.

Related Information

For information on related topics:

- [Services](#)
- [Fabric](#)
- [Sites](#)
- [Devices](#)

How to Create a Fabric Service Definition

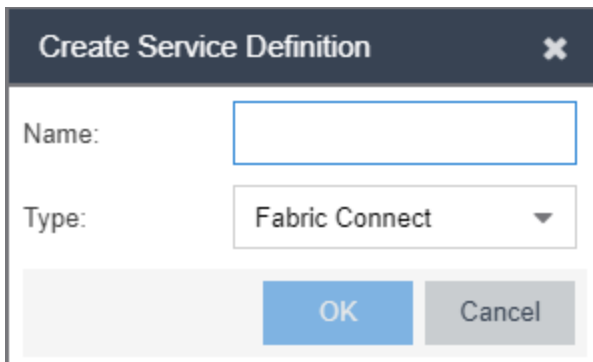
You can create a service definition in the **Sites tab** in ExtremeCloud IQ - Site Engine. Service definitions display information configured in service applications

definitions. Once 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. Click **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. Click **OK** to create the service definition.

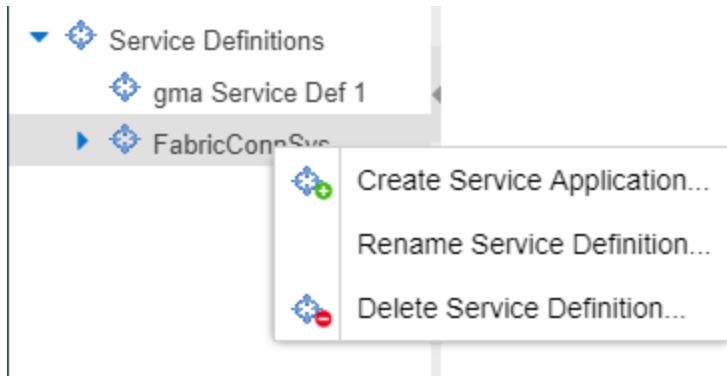
Once the service definition is created and configured, you can [apply](#) it to a site within your network. Once fabric services have been assigned to a site, they cannot be deleted.

Service Definition Panel

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

Rename a Service Definition

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

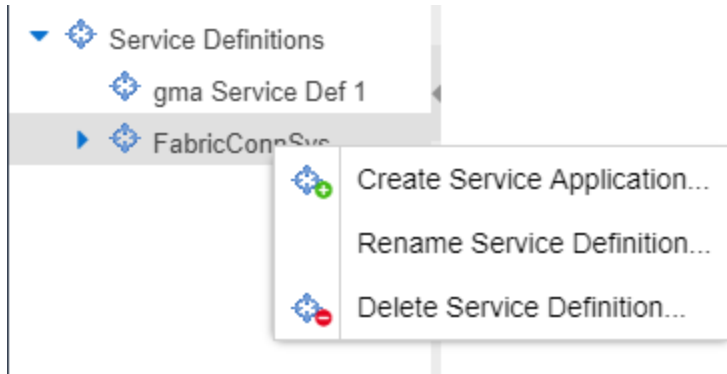


To rename a service definition:

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. Click **Rename Service Definition**.
6. Enter a new name in the **Name** field.
7. Click **OK** to rename the service definition.

Delete a Service Definition

Once 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 once 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. Click **Delete Service Definition**.
6. Click **Yes** to delete a service definition.

Related Information

For information on related topics:

- [Services](#)
- [Fabric](#)
- [Sites](#)
- [Devices](#)

Upgrading Fabric Manager

Use the following procedure to upgrade your version Fabric Manager.

Prerequisites

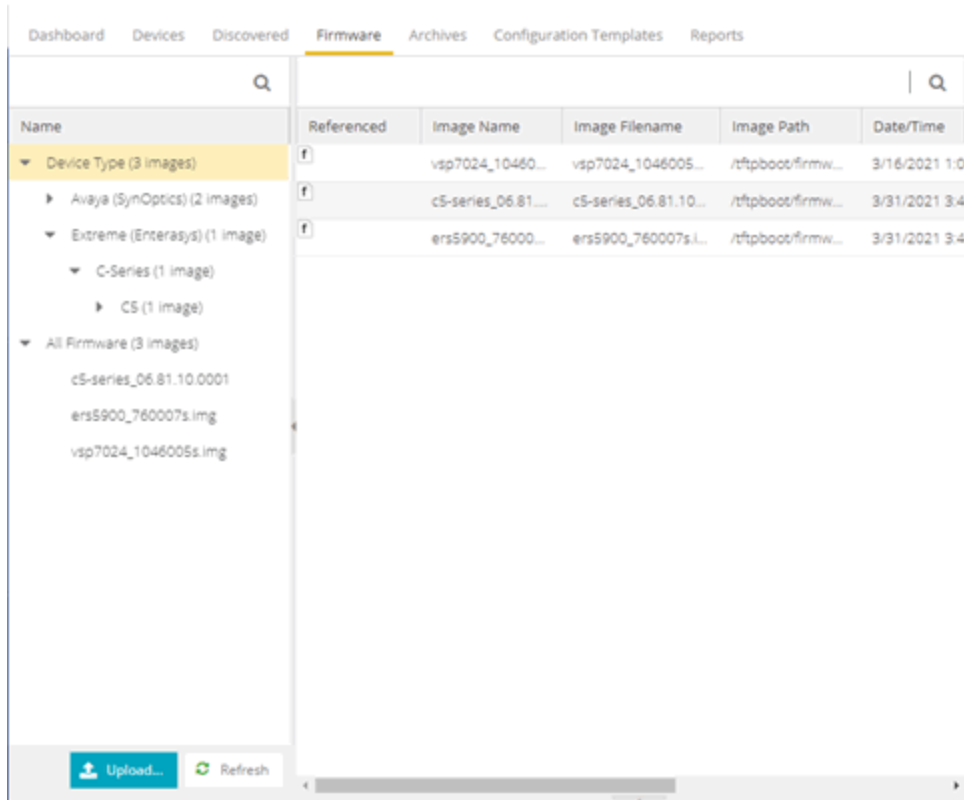
- Upgrade ExtremeCloud IQ - Site Engine to the later version before you upgrade Fabric Manager to the corresponding build number.
- Ensure that both the current and target ExtremeCloud IQ - Site Engine and Fabric Manager build numbers are the same.
- Download the latest upgrade bundle from the Extreme 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

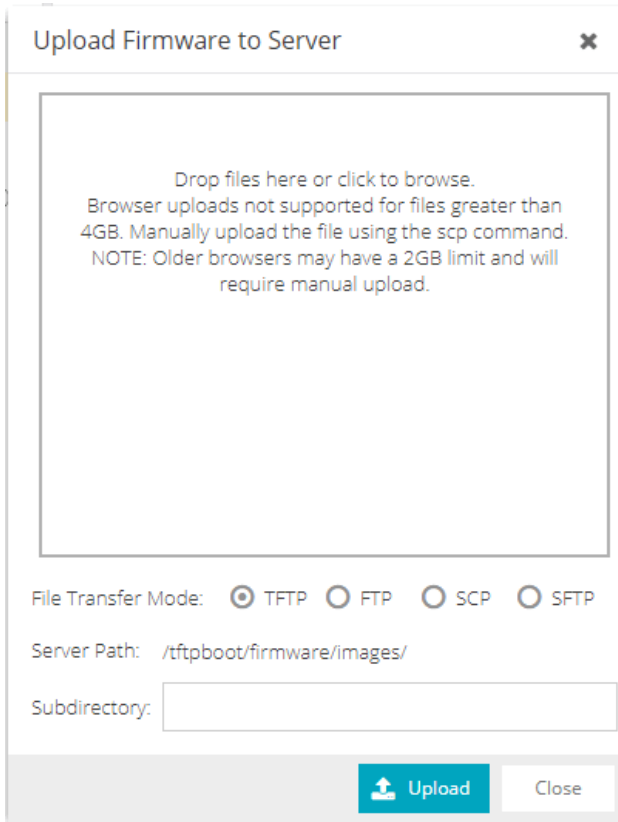
1. Open the **Network** tab in ExtremeCloud IQ - Site Engine.

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**.



Upload Firmware to Server

Drop files here or click to browse.
Browser uploads not supported for files greater than 4GB. Manually upload the file using the scp command.
NOTE: Older browsers may have a 2GB limit and will require manual upload.

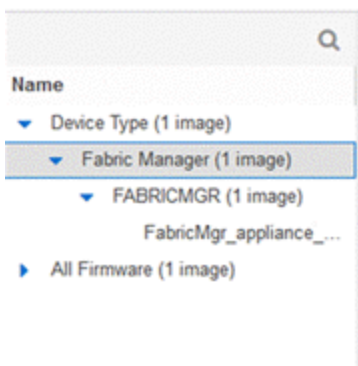
File Transfer Mode: TFTP FTP SCP SFTP

Server Path: /tftpboot/firmware/images/

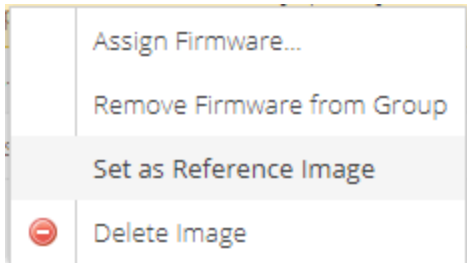
Subdirectory:

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 on the bundle listed on the main panel and select on **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.

Start Time	Type	Target	Result	Progress	Last Time	Message
ZTP+ - Tue Nov 06 2018 10:58:55 GMT-0500 (Eastern Standard Time) ==> Progress: 100% - Success						
Tue Nov 06 2018 10...	ZTP+	VMware-564dca56...	Success	100%	Tue Nov 06 2018 10...	Successfully upgraded FabricMgr_appliance_upgrade_bundle_3.2.1.57.zip
Tue Nov 06 2018 10...	ZTP+	VMware-564dca56...	Success	100%	Tue Nov 06 2018 10...	Successfully upgraded FabricMgr_appliance_upgrade_bundle_3.2.1.57.zip
ZTP+ - Tue Nov 06 2018 10:58:54 GMT-0500 (Eastern Standard Time) ==> Progress: 100% - Success						

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

Start Time	Type	Target	Result	Progress	Last Time	Message
ZTP+ - Tue Nov 06 2018 10:58:50 GMT-0500 (Eastern Standard Time) ==> Progress: 100% - Success						
Tue Nov 06 2018 10...	ZTP+	VMware-564dca56...	Success	100%	Tue Nov 06 2018 10...	Finished without error.
Tue Nov 06 2018 10...	ZTP+	VMware-564dca56...	Success	100%	Tue Nov 06 2018 10...	Finished without error.
ZTP+ - Tue Nov 06 2018 10:58:55 GMT-0500 (Eastern Standard Time) ==> Progress: 100% - Success						

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

Status	Name	Site	IP Address	Status	Details	Device Type	Family	Firmware	Reference
▼	10.54.37.89	World	10.54.37.89	Available	0...	Up 0 Down...			
●	ECA_Router	World	10.54.147.36	Available	39...	Up 2474 Down...	Wireless Co...	54.26.01.0143	
●	SP5A000	World	10.54.37.88	Available	10...	Up 225 Down...	ExtremeNet...	5.8.6.0-0198	
▲	WC16	World	10.54.105.16	Available	88...	Up 2183 Down...	Wireless Co...	10.41.02.0014	
▲	WC193	World	10.54.82.193	Available	10...	Up 2481 Down...	Wireless Co...	10.41.02.0014	
▼	WC225	World	10.54.80.225	Available	10...	Up 2481 Down...	Wireless Co...	10.41.02.0014	
●	fabricmgr	World	10.133.131.104	Available	10...	Up 2803 Down...	FABRICMGR	Fabric Mana...	[Link]

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**.

Related Information

- [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
<p>Error contacting a wireless controller. The controller shows a Warning icon.</p> 	<ol style="list-style-type: none">1. Verify that the Configuration password in the CLI Credential used for this device is properly configured.<ol style="list-style-type: none">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 click 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. Click OK.g. Use this CLI Credential in the controller's Profile.<p>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.</p>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