



Cisco Crosswork Hierarchical Controller 8.0

Analytics Guide

March 2024

Introduction

This document is a how-to-use guide for the analytics applications of Cisco Crosswork Hierarchical Controller.

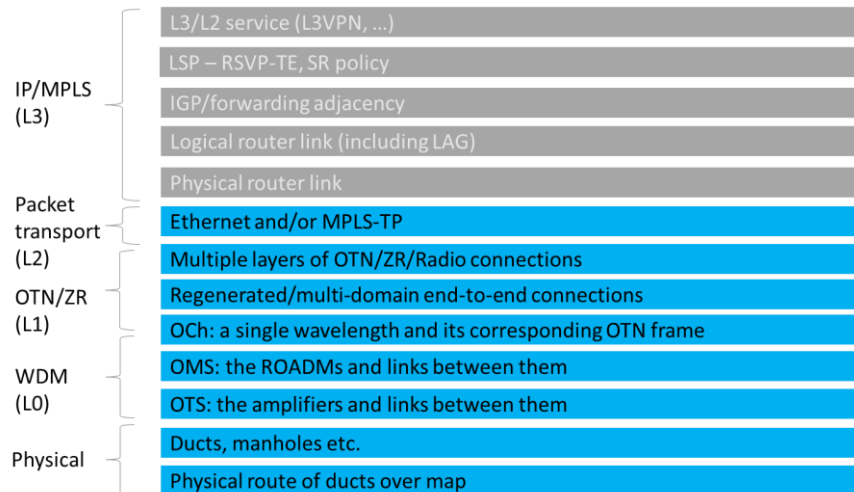
The following table lists the analytics applications. The Legend column indicates if the application falls into one of the following categories:

- **Common:** Common to all layers and multi-layer
- **IP:** Relevant to IP links and services
- **Optical:** Relevant to fibers, optical links, OTN/ETH connections

Table 1. Analytics Applications

Category	Application name	Legend	Description
Analytics	Failure Impact	Common	Enables a user to plan a maintenance event, finding which connections will be impacted by taking resources down and if there is an alternative path. When found, comparing existing and alternative path latency, cost, hops. Supported for OTN, ETH, RSVP-TE tunnels.
	Shared Risk Analysis	Common	Find if there are commonly shared resources (node, site, link, card) between selected group of links in any layer. Group can be selected explicitly or as SHQL rule.

Layers



Terminology

Table 2. Terms

Term	Definition
Adapter	The software used by Crosswork Hierarchical Controller to connect to a device or to the manager, to collect information required by the network model and configure the device.
Agg link	Agg is Link Aggregation Group (LAG) where multiple ETH links are grouped to create higher bandwidth

Term	Definition
	and resilient link.
BGP	Border Gateway Protocol
Circuit E-Line	An Ethernet connection between two ETH client ports on Transponder or Muxponder over OTN signal.
CNC	Crosswork Network Controller.
Device	Optical network element, router, or microwave device.
Device Manager	The application that manages the deployed adapters.
eMBB	Enhanced Mobile Broadband.
ETH chain	A link whose path is a chain of Ethernet links cross-subnet-connected (found using Crosswork Hierarchical Controller cross-mapping algorithm). Eth-chain is a replacement for R_PHYSICAL link in cases where one side of the link is in devices out of the scope discovered by Crosswork Hierarchical Controller.
ETH link	ETH L2 link, spans from one ETH UNI port of an optical device to another, and rides on top of ODU.
Fiber	Chain of fiber segments that spans from one optical device to another.
Fiber segment	Physical fiber line that spans from one passive fiber endpoint (manhole, splice etc.) to another and is used as a segment in a fiber link.
IGP	IGP is the link between two routers that carries IGP protocol messages. The link represents an IGP adjacency.
IP-MPLS	IP multi-protocol label switching.
L3 physical	L3 physical is the physical link connecting two router ports. It may ride on top of an ETH link if the IP link is carried over the optical layer.
L3-VPN	A virtual private network based on L3 routing for control and forwarding.
L3-VPN link	The connection between two sites of a specific L3-VPN (can be a chain of LSP connections or IGP path).
LDP Endpoint	The endpoint of the LDP path (router name). LDP is a signaled path for services between two routers in the MPLS network. The path is signaled by routers using the Label Distribution Protocol.
Logical link, IGP, LSP	Logical link connects VLANs on two IP ports.
LSP	Label Switched Path, used to carry MPLS traffic over a label-based path. LSP is the MPLS tunnel created between two routers over IGP links, with or without TE options.
NMC (OCH-NC, OTSiMC)	NMC is the link between the xPonder facing ports on two ROADMs. This link is the underlay for OCH and it is an overlay on top of OMS links. This is relevant only for disaggregation cases where the ROADM and OT box are separated.
NMS	Network Management System.
OC/OCG	SONET/SDH links that span from one optical device to another and carry SONET/SDH lower bandwidth services, the links ride on top of OCH links and terminate in TDM client ports.
OCH	OCH is a wavelength connection spanning between the client port one OT device (transponder, muxponder, regen) and another. 40 or 80 OCH links can be created on top of OMS links. The client port can be a TDM or ETH port.
ODU	ODU links are sub-signals in OTU links. Each OTU links can carry multiple ODU links, and ODU links can be divided into finer granularity ODU links recursively.

Term	Definition
OSPF	Open Shortest Path First, an Interior Gateway Protocol between routers.
OTN-Line	An OTN connection between two ODU client ports over OTN path.
OTS	OTS is the physical link connecting one line amplifier or ROADM to another. An OTS can be created over a fiber link.
OTU	OTU is the underlay link in OTN layer, used for ODU links. It can ride on top of an OCH.
Packet E-Line	A point-to-point connection between two routers or transponders/muxponders over MPLS-TP or IP-MPLS.
PCC	Path Computation Client. Delegated to controller. Router is responsible for initiating path setup and retains the control on path updates.
PCE	Path Computation Element. Controller-initiated.
Policy	A group of rules and shared risk resource types.
Radio Channel	Multiple radio channels can be on top of radio media, each channel represents a different ETH link with its own rate.
Radio Media	The media layer as a carrier of radio channels.
RD	Route Distinguisher.
RSVP-TE	Resource Reservation Protocol to control traffic engineered paths over MPLS network.
RT	Route Target.
Rule	A group of two or more diverse links/connections.
SCH	A super-channel is an evolution of DWDM in which multiple, coherent optical carriers are combined to create a unified channel of a higher data rate, and which is brought into service in a single operational cycle.
SDN Controller	Software that manages multiple routers or optical network elements.
Shared Risk Resource Type	The type of the resource that the shared risk analysis application checks if objects in the rule share. The types are Link, Device, Shelf, Card, and Port.
SHQL	The Sedona Hierarchical Query Language (SHQL) is used to easily query the model across all dimensions (Vendors, Topologies, Layers, Domains, Status and Time).
SR Policy	Segment Routing Policy. A segment routing path between two nodes, with mapping to the IGP links based on SIDs list.
SRLG	The Shared Risk Link Group are the links or connections that may suffer from a common failure if they share a common risk, such as a device, link or card.
STS	Large and concatenated TDM circuit frame (such as STS-3c) into which ATM cells, IP packets, or Ethernet frames are placed. Rides on top of OC/OCG as optical carrier transmission rates.
uRLLC	Ultra-Reliable Low Latency Communications.
Violation	Any case where a resource, identified by its shared risk resource type, is shared between two links/connections.
VRF	Virtual Routing Function, acts as a router in L3-VPN.
ZR Channel	Multiple ZR channels can be on top of ZR media, each channel represents a different IP link with its own rate.

Term	Definition
ZR Media	The media layer as a carrier of ZR channels, on top of OCH link.

Shared Risk Analysis

This application helps to establish diversity policy rules on predefined links or connection groups or on ad-hoc selected links/connections.

The application identifies any lower layer resources shared by a pair or group of links, or by any connection between selected endpoints. This helps you to ensure that diverse links or connections are not using the same underlying resources.

The LDP Endpoint test looks for the shortest IGP path between the two pairs of routers and then analyses the shared risk between the paths found.

You can define one or more policies and use them for testing. A policy includes the shared risk resource type, the test type and the applicable rules.

- **Shared Risk Resource Type** – The type of resource that according to policy should not be shared by the links/connections paths. One or more of the following resource types can be selected: Device, Shelf, Card, Port, Link, or SRLG.
- **Test scenario** – The test type, either multiple links or a single protected link.
- **Rules** – Groups of links or connections by specific type. Users can select links/connections to a group and give each group a name or use SHQL rule to define the group. The group is retrieved at the time of execution. If there are any network changes, you can use the time machine and network inventory app to identify these changes.

Shared Risk Analysis Tests

To run a test, you can select a policy or ad-hoc select links/connection pairs to check if they share common resources.

Results are displayed as risks, where each row in the results table is a risk found that impacts a pair of links/connection of the selected policy or ad-hoc selection. The results table displays the names of the rules, the links that are at risk, the link type, the number, or resources they share and the total bandwidth at risk.

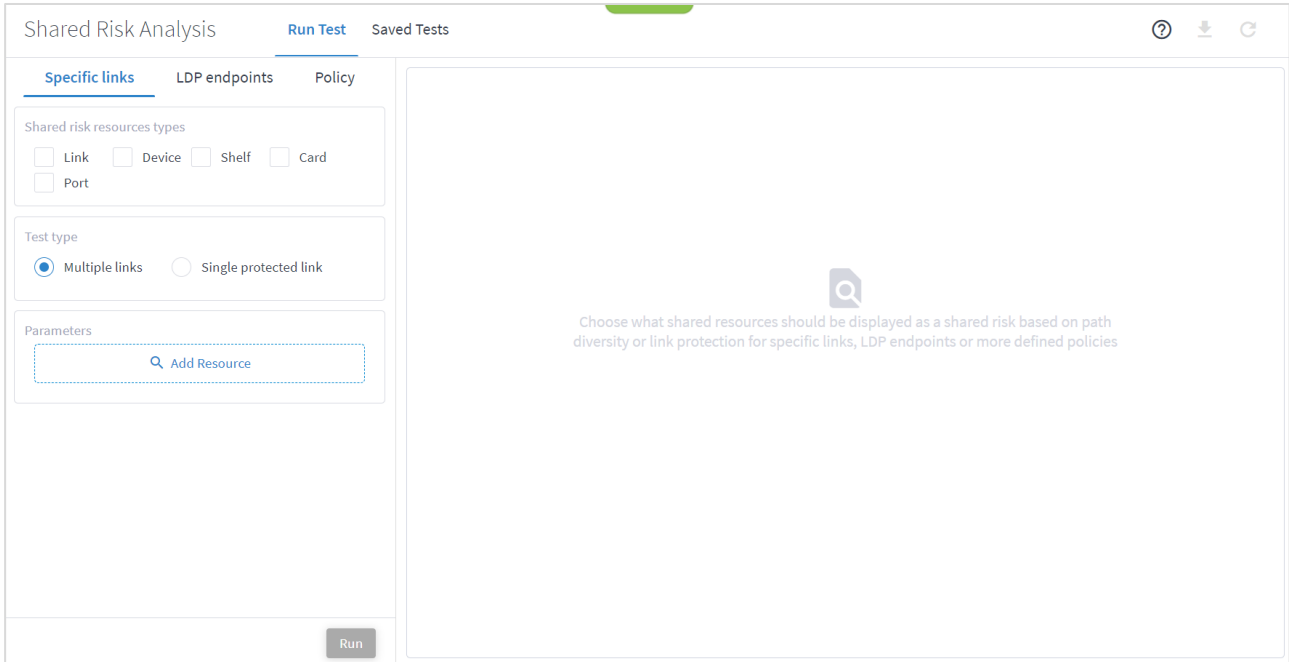
Run Specific Links Test

You can run a test on specific links, checking for shared risk resources of type link, device, shelf, card, and port. You can select whether to check:

- Multiple links
- Single protected link

To run a specific links test:

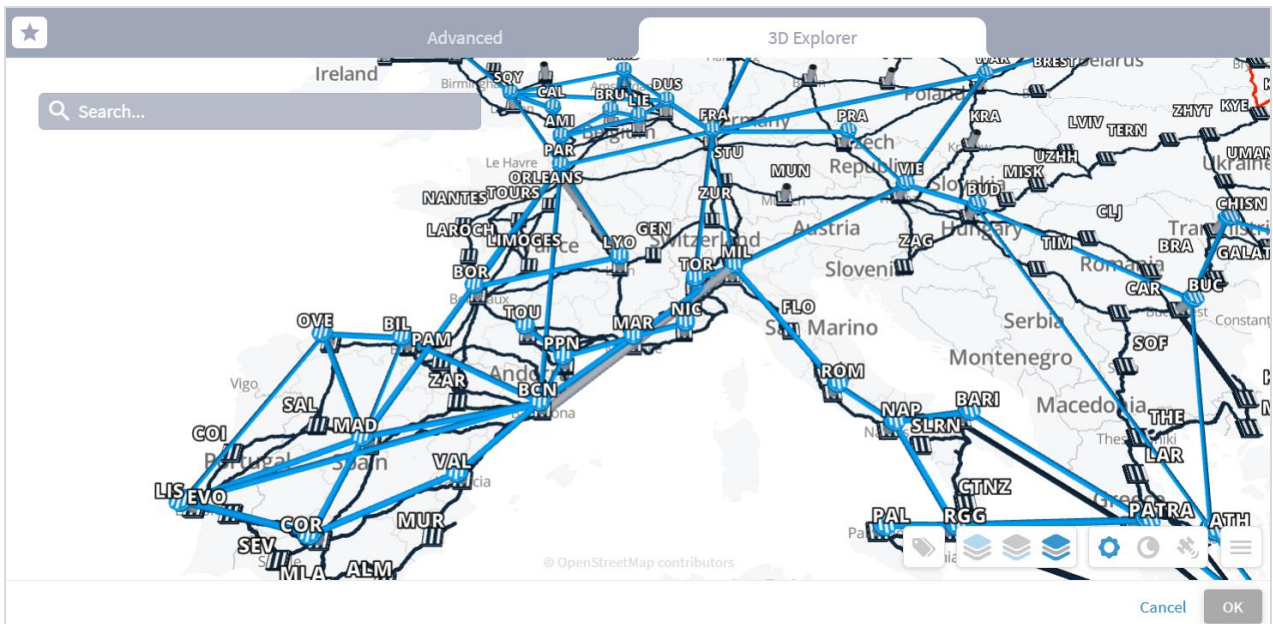
1. In the applications bar in Crosswork Hierarchical Controller, select **Shared Risk Analysis**.



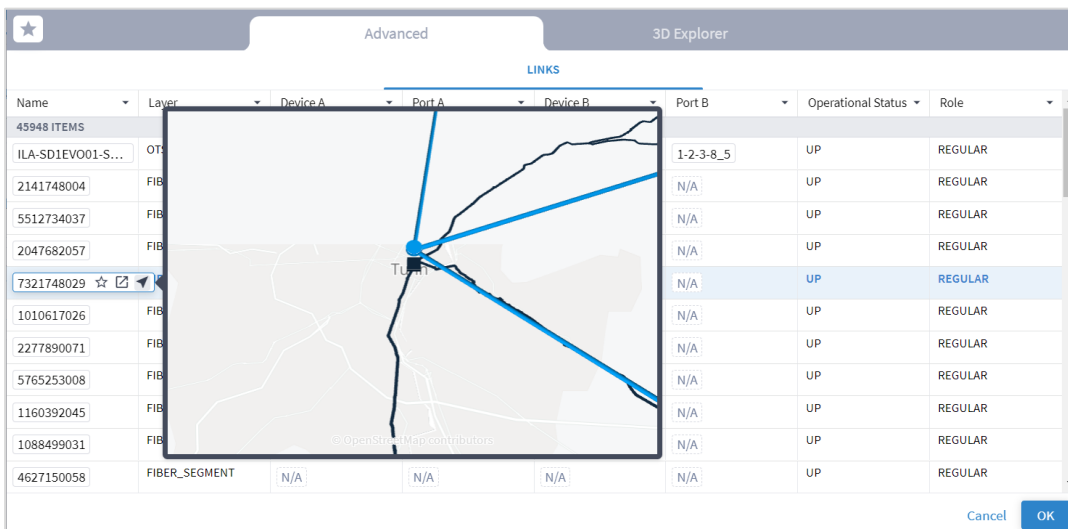
2. Select the required **Shared risk resources types**.
3. Select the **Test type (Multiple links or Single protected link)**.
4. Click **Add Resource** to add a link.

Advanced		3D Explorer					
LINKS							
Name	Layer	Device A	Port A	Device B	Port B	Operational Status	Role
45948 ITEMS							
ILA-SD1EVO01-S...	OTS	ILA-SD1EVO01-S...	1-1-3-8_5	SD1LIS01	1-2-3-8_5	UP	REGULAR
2141748004	FIBER_SEGMENT	N/A	N/A	N/A	N/A	UP	REGULAR
5512734037	FIBER_SEGMENT	N/A	N/A	N/A	N/A	UP	REGULAR
2047682057	FIBER_SEGMENT	N/A	N/A	N/A	N/A	UP	REGULAR
7321748029	FIBER_SEGMENT	N/A	N/A	N/A	N/A	UP	REGULAR
1010617026	FIBER_SEGMENT	N/A	N/A	N/A	N/A	UP	REGULAR
2277890071	FIBER_SEGMENT	N/A	N/A	N/A	N/A	UP	REGULAR
5765253008	FIBER_SEGMENT	N/A	N/A	N/A	N/A	UP	REGULAR
1160392045	FIBER_SEGMENT	N/A	N/A	N/A	N/A	UP	REGULAR
1088499031	FIBER_SEGMENT	N/A	N/A	N/A	N/A	UP	REGULAR
4627150058	FIBER_SEGMENT	N/A	N/A	N/A	N/A	UP	REGULAR

Or select the **3D Explorer** tab.



In the **Advanced** tab, you can select a link and click to view the link in the popup map.



5. Select a link and click **OK**.
6. Add more links (by repeating the steps above for other links to analyze).
7. Click **Run**. In the test results, you see the **VIOLATIONS**.

The screenshot shows the 'Shared Risk Analysis' interface. On the left, there is a configuration panel with sections for 'Specific links', 'LDP endpoints', and 'Policy'. Under 'Specific links', there are checkboxes for 'Link', 'Device', 'Shelf', and 'Card', all of which are checked. Below this is a 'Test type' section with 'Multiple links' selected. A 'Parameters' section contains a search bar and three input fields with IP address ranges: 'cr1.har:cr1.stctopo_lsp_mesh_164250434...', '10.40.0.162 to 10.40.0.161', and '10.40.0.157 to 10.40.0.158'. A 'Run' button is at the bottom of this panel.

The main area displays a table with two tabs: 'VIOLATIONS' and 'CAUSES'. The 'VIOLATIONS' tab is active, showing a table with 3 items. The table has columns for Rule, Link A, Link Type, Link B, Link Type, SRLG Count, and Capacity At Risk [Gbps].

Rule	Link A	Link Type	Link B	Link Type	SRLG Count	Capacity At Risk [Gbps]
	10.40.0.157 to 10.40.0.158	L3 Logical	cr1.har:cr1.stctopo_lsp_mesh_164250434983	LSP	61	
	10.40.0.162 to 10.40.0.161	L3 Logical	10.40.0.157 to 10.40.0.158	L3 Logical	46	
	10.40.0.162 to 10.40.0.161	L3 Logical	cr1.har:cr1.stctopo_lsp_mesh_164250434983	LSP	46	

8. You can select a link and view the link in the popup map and select a row (and click ▶ to expand) in the test results to see more details on the shared resources.

This screenshot shows a detailed view of a link violation. The table from the previous screenshot is partially visible, with one row selected and expanded. A popup window titled 'Shared Resources' is open, showing details for the selected link.

Rule	Link A	Link Type	Link B	Link Type	SRLG Count
	CR2.DUS:CR2.MIL...	LSP	CR2.PAR:CR2.MIL...	LSP	17
	SD1BCN01/2-3-10...	Et...	CR2.DUS:CR2.MIL...	LSP	1
	SD1MIL01/1-16-1...	Et...	CR2.DUS:CR2.MIL...	LSP	1
	SD1BCN01/2-3-10...	Et...	CR2.PAR:CR2.MIL...	LSP	1
	SD1MIL01/1-16-1...	Et...	CR2.PAR:CR2.MIL...	LSP	1
	SD1MIL01/1-16-1...	Et...	SD1BCN01/2-3-10...	Et...	1

The 'Shared Resources' popup window shows the following details:

- CR2.DUS:CR2.MIL:lsp_0-**
- CR2.PAR:CR2.MIL:lsp_0**
- Inventory (15)**
 - Optical Node: ILA-SD1MIL01-SD1ZUR01-0
 - Optical Node: ILA-SD1MIL01-SD1ZUR01-2
 - Optical Node: ILA-SD1FRA01-SD1STU01-1
 - Optical Node: ILA-SD1STU01-SD1ZUR01-1
 - Optical Node: ILA-SD1FRA01-SD1STU01-0
 - Optical Node: SD1MIL01
 - Optical Node: SD1FRA01
 - Optical Node: SD1ZUR01
 - Optical Node: SD1STU01
 - Router: CR2.MIL
 - Router: CR1.FRA
 - Router: CR2.FRA
 - Optical Node: ILA-SD1MIL01-SD1ZUR01-3
 - Optical Node: ILA-SD1MIL01-SD1ZUR01-1
 - Optical Node: ILA-SD1STU01-SD1ZUR01-0
- IGP (2)**
 - 10.40.0.146 to 10.40.0.145
 - 10.40.0.161 to 10.40.0.162

Rule	Link A	Link B	Link Type	Link Type	SRL	Col
6 ITEMS						
	CR2.DUS:CR2.MI...	LSP	CR2.PAR:CR2.MIL...	LSP	17	

Shared Resources

CR2.DUS:CR2.MIL:lsp_0-
CR2.PAR:CR2.MIL:lsp_0

Inventory (15)

- Node: ILA-SD1MIL01-SD1ZUR01-0
- Node: ILA-SD1MIL01-SD1ZUR01-2
- Node: ILA-SD1FRA01-SD1STU01-1
- Node: ILA-SD1STU01-SD1ZUR01-1
- Node: ILA-SD1FRA01-SD1STU01-0
- Node: SD1MIL01
- Node: SD1FRA01
- Node: SD1ZUR01
- Node: SD1STU01
- CR2.MIL
- CR1.FRA
- CR2.FRA
- Node: ILA-SD1MIL01-SD1ZUR01-3
- Node: ILA-SD1MIL01-SD1ZUR01-1
- Node: ILA-SD1STU01-SD1ZUR01-0

146 to 10.40.0.145
161 to 10.40.0.162

Note: For a single protected link, the Link B and Link Type columns are empty, and the **Capacity At Risk** column is likely to be N/A.

- To view the causes, select the **CAUSES** tab.

Shared Risk Analysis

Specific links | LDP endpoints | Policy

Shared risk resources types

Link Device Shelf Card
 Port

Test type

Multiple links Single protected link

Parameters

cr1.harcr1.stctopo_lsp_mesh_164250434...
10.40.0.162 to 10.40.0.161
10.40.0.157 to 10.40.0.158

VIOLATIONS		CAUSES
Resource Name	Number Of Violations	
6 ITEMS		
ILA-wdmjR01-wdmnia01-0/1-2-1	3	
wdmnia01/1-2-9	1	
10.40.0.157 to 10.40.0.158	1	
ILA-wdmjR01-wdmnia01-5	3	
ILA-wdmjR01-wdmnia01-3/Shelf-1	3	
ILA-wdmjR01-wdmnia01-6/1-2-2	3	
Card-1/2 at ILA-wdmjR01-wdmnia01-4	3	
Card-1/2 at ILA-wdmjR01-wdmnia01-3	3	
ILA-wdmjR01-wdmnia01-1/1-2-1	3	
Card-1/2 at wdmnia01	3	
ILA-wdmjR01-wdmnia01-5/1-2-2	3	
cr1.mia/0-1-7	1	
wdmnia01/1-2-8	1	
Card-1/2 at wdmjR01	3	
wdmnia01/1-2-10	1	
Card-1 at cr1.mia	1	
Card-1/2 at ILA-wdmjR01-wdmnia01-2	3	
wdmnia01	3	
wdmjR01/Shelf-1	3	
ILA-wdmjR01-wdmnia01-2	3	
ILA-wdmjR01-wdmnia01-1/1-2-2	3	
ILA-wdmjR01-wdmnia01-0/1-2-2	3	
wdmjR01/1-2-7	1	

10. (Optional) For multiple links, to remove a link from the test, select and click **Run**.

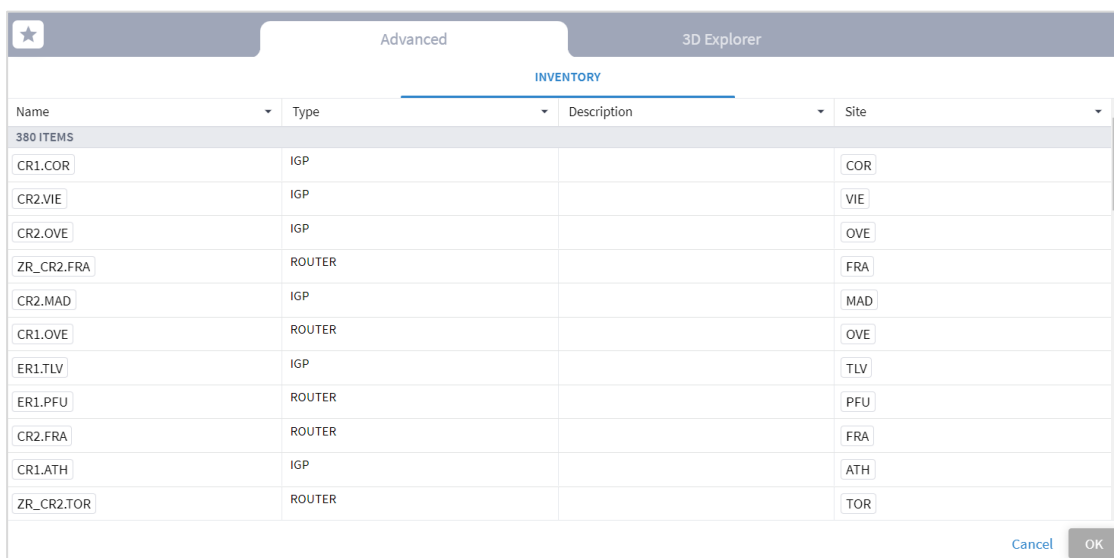
Run LDP Endpoints Test

You can run a test on two pairs of routers acting as LDP endpoints, checking for shared risk resources of type link, device, shelf, card, and port. You need to select two endpoint device pairs.

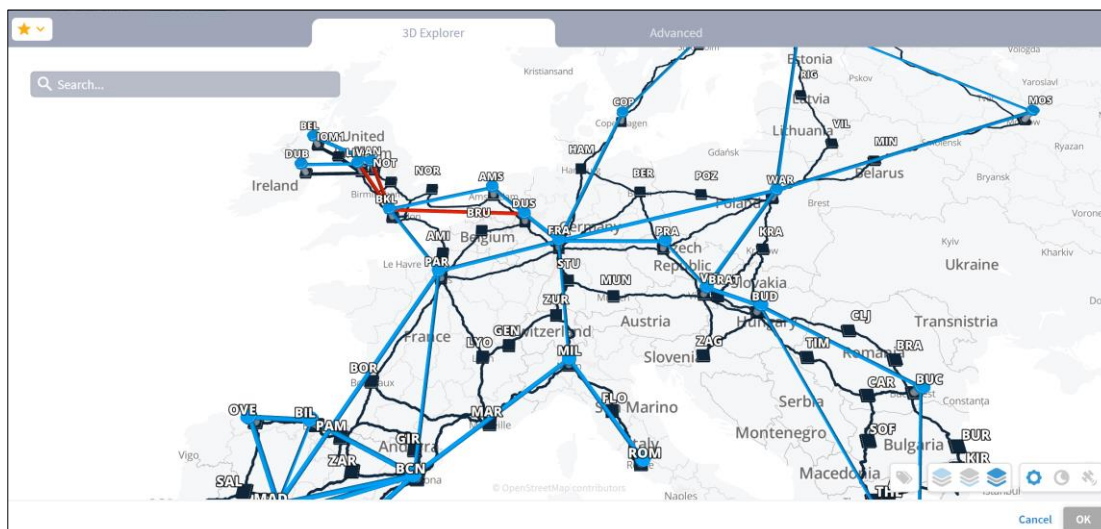
This test looks for the shortest IGP path between the two pairs of routers and then analyses the shared risk.

To run LDP endpoints test:

1. In the applications bar in Crosswork Hierarchical Controller, select **Shared Risk Analysis**.
2. Select the **LDP endpoints** tab.
3. Select the required **Shared risk resource types**.
4. Click to add an endpoint.



Or select the **3D Explorer** tab.



5. Select an endpoint.
6. Click **OK**.
7. Add more endpoints.
8. Click **Run**.

Shared Risk Analysis Live

Specific links **LDP endpoints** Policy

Shared risk resources types

Link Device Shelf Card

Port

Parameters

Endpoint devices pair #1

Select a Device:

Select a Device:

Endpoint devices pair #2

Select a Device:

Select a Device:

Run

Rule	Link A	Link Type	Link B	Link Type	SRLG Count	Capacit At Risk [GBps]
14 ITEMS						
	10.40.0.193 to 10.40.0.194	IGP	10.40.0.201 to 10.40.0.202	IGP	14	N/A
	10.40.0.193 to 10.40.0.194	IGP	10.40.0.205 to 10.40.0.206	IGP	1	N/A
	10.40.0.198 to 10.40.0.197	IGP	10.40.0.201 to 10.40.0.202	IGP	1	N/A
	10.40.0.205 to 10.40.0.206	IGP	10.40.0.198 to 10.40.0.197	IGP	1	N/A
	10.40.0.205 to 10.40.0.206	IGP	10.40.0.201 to 10.40.0.202	IGP	2	N/A
	10.40.0.205 to 10.40.0.206	IGP	10.40.0.205 to 10.40.0.206	IGP	8	N/A
	10.40.1.41 to 10.40.1.42	IGP	10.40.0.205 to 10.40.0.206	IGP	1	N/A
	10.40.1.30 to 10.40.1.29	IGP	10.40.0.205 to 10.40.0.206	IGP	1	N/A
	10.40.1.41 to 10.40.1.42	IGP	10.40.0.205 to 10.40.0.206	IGP	1	N/A
	10.40.1.41 to 10.40.1.42	IGP	10.40.1.41 to 10.40.1.42	IGP	3	N/A
	10.40.1.30 to 10.40.1.29	IGP	10.40.1.41 to 10.40.1.42	IGP	1	N/A
	10.40.1.46 to 10.40.1.45	IGP	10.40.0.205 to 10.40.0.206	IGP	1	N/A
	10.40.1.41 to 10.40.1.42	IGP	10.40.1.46 to 10.40.1.45	IGP	1	N/A
	10.40.1.30 to 10.40.1.29	IGP	10.40.1.46 to 10.40.1.45	IGP	2	N/A

9. In the test results, you can select a link and view the link in the popup map and select a row (and click to expand) in the test results to see more details on the shared resources.

Rule	Link A	Link Type	Link B	Link Type	SRLG Count
14 ITEMS					
	10.40.0.193 to 10...	IGP	10.40.0.201 to 10...	IGP	14
	10.40.0.193 to 10...	IGP	10.40.0.205 to 10...	IGP	1
	10.40.0.198 to 10...	IGP	10.40.0.201 to 10...	IGP	1
	10.40.0.205 to 10...	IGP	10.40.0.198 to 10...	IGP	1
	10.40.0.205 to 10...	IGP	10.40.0.201 to 10...	IGP	2
	10.40.0.205 to 10...	IGP	10.40.0.205 to 10...	IGP	8
	10.40.1.41 to 10.4...	IGP	10.40.0.205 to 10...	IGP	1
	10.40.1.30 to 10.4...	IGP	10.40.0.205 to 10...	IGP	1
	10.40.1.41 to 10.4...	IGP	10.40.0.205 to 10...	IGP	1
	10.40.1.41 to 10.4...	IGP	10.40.1.41 to 10.4...	IGP	3
	10.40.1.30 to 10.4...	IGP	10.40.1.41 to 10.4...	IGP	1
	10.40.1.46 to 10.4...	IGP	10.40.0.205 to 10...	IGP	1
	10.40.1.41 to 10.4...	IGP	10.40.1.46 to 10.4...	IGP	1
	10.40.1.30 to 10.4...	IGP	10.40.1.46 to 10.4...	IGP	2

Shared Resources

10.40.0.193 to 10.40.0.194-10.40.0.201 to 10.40.0.202

▼ **Inventory (11)**

- Optical Node: ILA-SD2BRAT01-SD2KRA01-2
- Optical Node: ILA-SD2KRA01-SD2WAR01-2
- Optical Node: ILA-SD2BRAT01-SD2KRA01-3
- Optical Node: ILA-SD2BRAT01-SD2KRA01-1
- Optical Node: ILA-SD2KRA01-SD2WAR01-0
- Optical Node: SD2VIE01
- Optical Node: SD2KRA01
- Optical Node: SD2BRAT01
- Optical Node: SD2WAR01
- Optical Node: ILA-SD2BRAT01-SD2KRA01-0
- Optical Node: ILA-SD2KRA01-SD2WAR01-1

▼ **OMS (3)**


- SD2KRA01/OMS-1-0-4 to SD2WAR01/OMS-1-0-8
- SD2BRAT01/OMS-1-0-4 to SD2VIE01/OMS-1-0-5
- SD2BRAT01/OMS-1-0-6 to SD2KRA01/OMS-1-0-6

Export Test Results

The tabular test results can be exported into a CSV file for offline analysis.

	A	B	C	D	E	F	G	H	I
1	Rule	Link A	Link A Type	Link B	Link B Type	SRLG	SRLG Type		
2		SD1FRA01/2-4-100-2 to SD1PRA01/1-5-100-2	Ethernet	SD1FRA01/2-1-100-2 to SD1PAR01/1-13-100-2	Ethernet	Optical Node: SD1FRA01	Optical Node		
3		SD1FRA01/2-5-100-2 to SD1PRA01/1-6-100-2	Ethernet	SD1FRA01/2-1-100-2 to SD1PAR01/1-13-100-2	Ethernet	Optical Node: SD1FRA01	Optical Node		
4		SD1FRA01/2-5-100-2 to SD1PRA01/1-6-100-2	Ethernet	SD1FRA01/2-4-100-2 to SD1PRA01/1-5-100-2	Ethernet	Optical Node: ILA-SD1FRA01-SD1PRA01-0	Optical Node		
5									
6									
7									

To export the test results:

1. In the applications bar in Crosswork Hierarchical Controller, select **Shared Risk Analysis**.
2. Run the required test.
3. Click . The file is downloaded automatically.

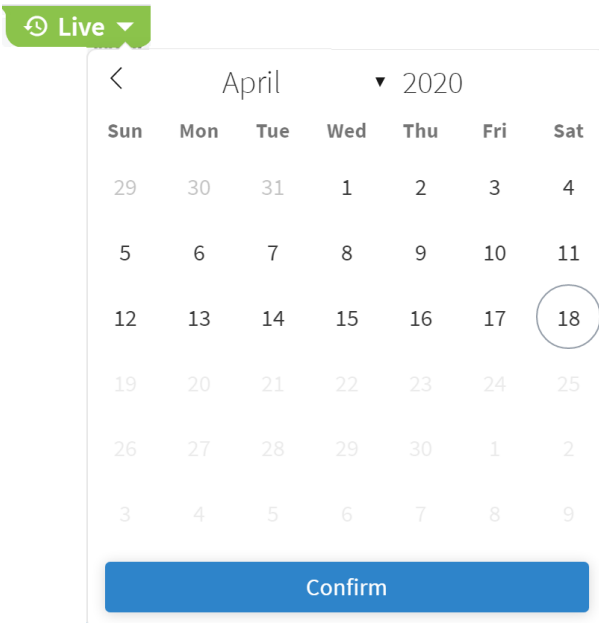
Use Time Machine

The time machine provides a snapshot of the state of the network as it was at a date in the past. In this mode, all applications reflect data and analysis that apply to this point in time.

You can use the time machine to execute the tests on the model as at a date in the past.

To change the model date:

1. In the applications bar in Crosswork Hierarchical Controller, select **Shared Risk Analysis**.
2. Click **Live**, select a date and click **Confirm**.



3. Run the required test.

Share Risk Analysis Policies

You can define one or more policies and use them for testing. A policy includes the shared risk resource type and the applicable rules.

- **Shared Risk Resource Type** – The type of resource that according to policy should not be shared by the links/connections paths. The following resource types can be selected: Device, Shelf, Card, Port, Link, or SRLG.
- **Test type**– Either test multiple links or a single protected link.
- **Rules** – Groups of links or connections by specific type. You can select links/connections to a group and give each group a name.

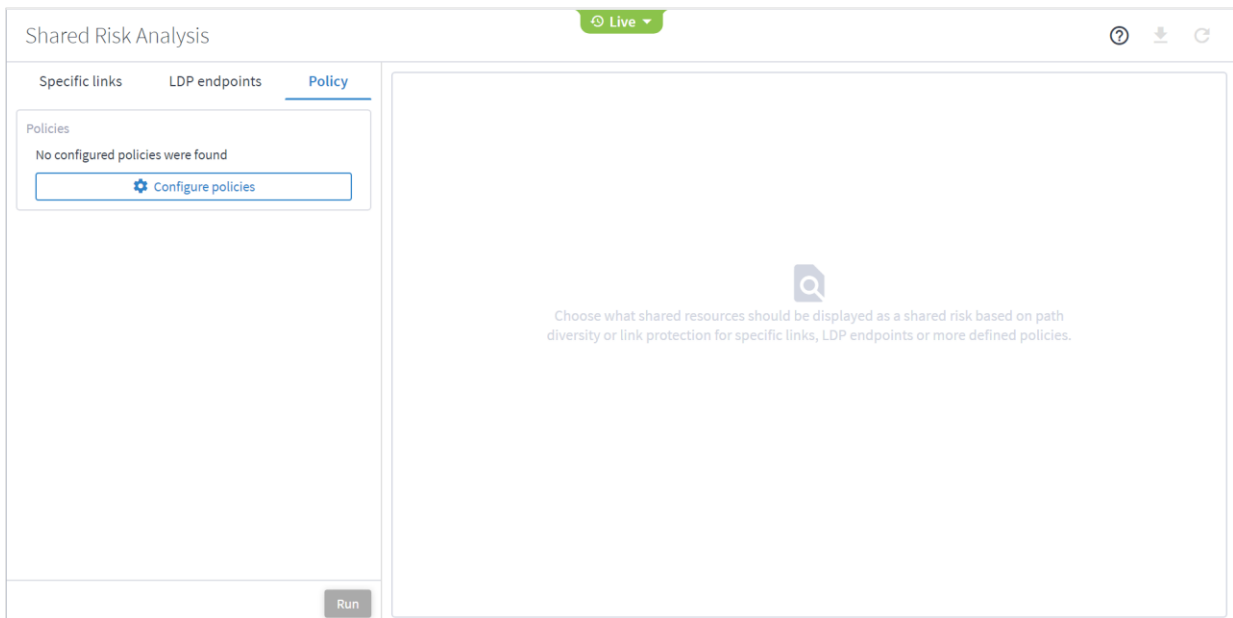
Add Policy

You can add a policy, and then add rules to it. You must add at least one rule to save a new policy.

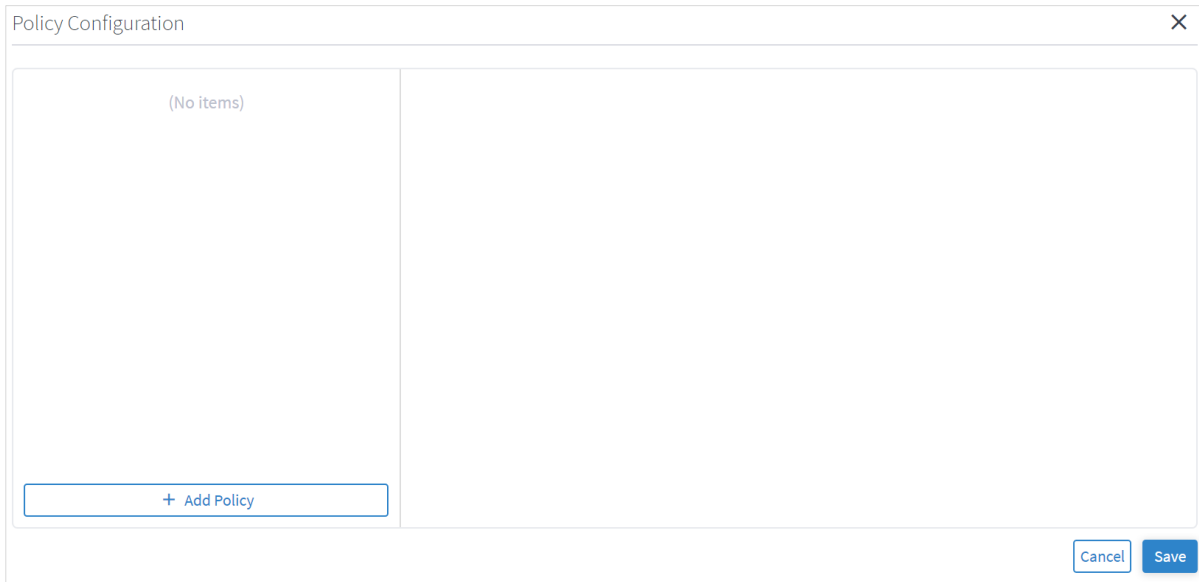
You can add a rule to an existing policy. Alternatively, you can add rules using the Shared Risk API and SHQL query (see [Add Rules using the Shared Risk API](#)).

To add a policy:

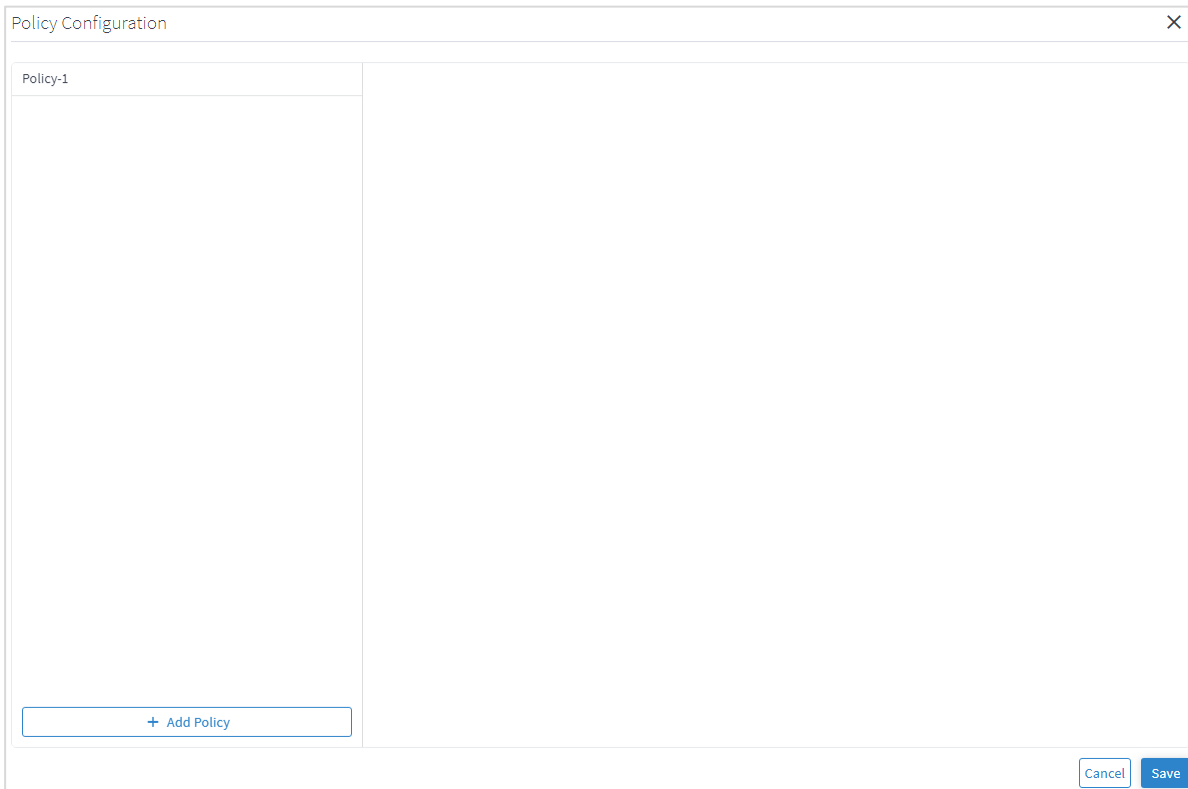
1. In the applications bar in Crosswork Hierarchical Controller, select **Shared Risk Analysis**.
2. Select the Policy tab.



3. Click  **Configure Policies**.





4. In the **Policy Configuration** window, click **Add Policy**.



5. Select the policy.


The screenshot shows the 'Policy Configuration' window with 'Policy-1' selected in the left sidebar. The main area displays the configuration for 'Policy-1'. At the top right, there is a 'Delete policy' button. Below that, the 'Shared risk resource types' section has five checkboxes: Link, Device, Shelf, Card, and Port, all of which are currently unchecked. The 'Test type' section has two radio buttons: 'Multiple links' (which is selected) and 'Single protected link'. Below this is a 'Rules' section with a '+ Add Rule' button. At the bottom left of the window is a '+ Add Policy' button, and at the bottom right are 'Cancel' and 'Save' buttons.

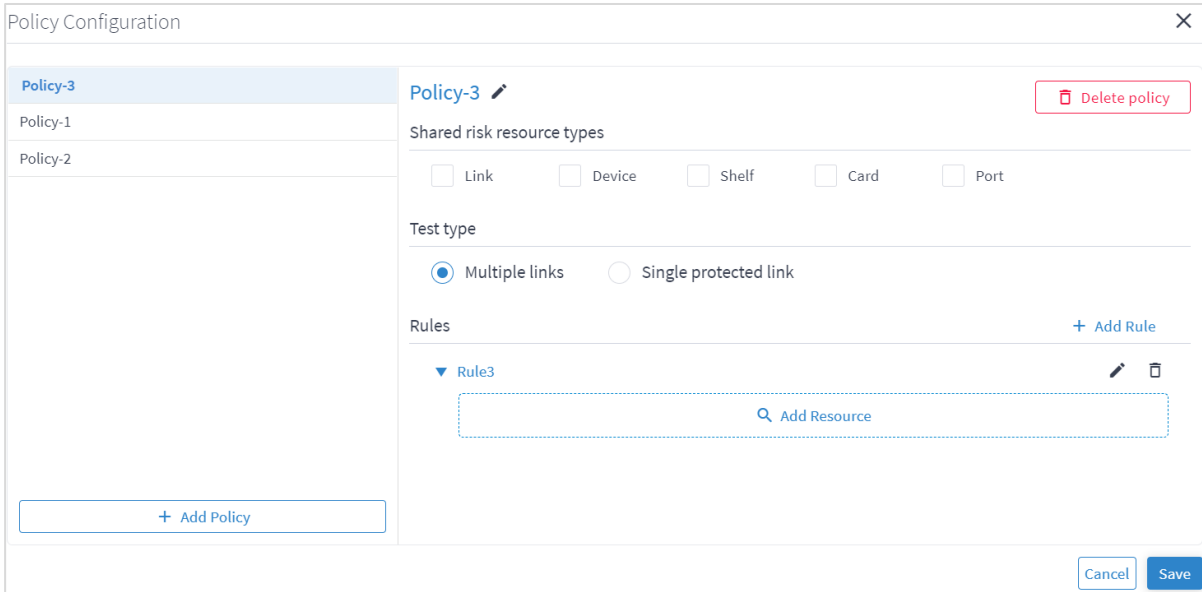
- (Optional) To change the policy name, select the new policy, click , modify the policy name and then click .
- Select the required **Shared risk resource types**.
- Select whether you want to test **Multiple links** or **Single protected link**.
- Click **Add Rule**.

The screenshot shows the 'Policy Configuration' window with 'Policy-3' selected in the left sidebar. The main area displays the configuration for 'Policy-3'. At the top right, there is a 'Delete policy' button. Below that, the 'Shared risk resource types' section has five checkboxes: Link, Device, Shelf, Card, and Port, all of which are currently unchecked. The 'Test type' section has two radio buttons: 'Multiple links' (which is selected) and 'Single protected link'. Below this is a 'Rules' section with a '+ Add Rule' button. A rule has been added, showing a text input field with 'Rule name', a close button (x), a checkmark (✓), and a trash icon. At the bottom left of the window is a '+ Add Policy' button, and at the bottom right are 'Cancel' and 'Save' buttons.

10. Enter a rule **Name**.

11. Click .

12. Click  to expand the rule.




Policy Configuration

Policy-3

Policy-1

Policy-2

Policy-3  Delete policy



Shared risk resource types

Link Device Shelf Card Port

Test type

Multiple links Single protected link

Rules + Add Rule

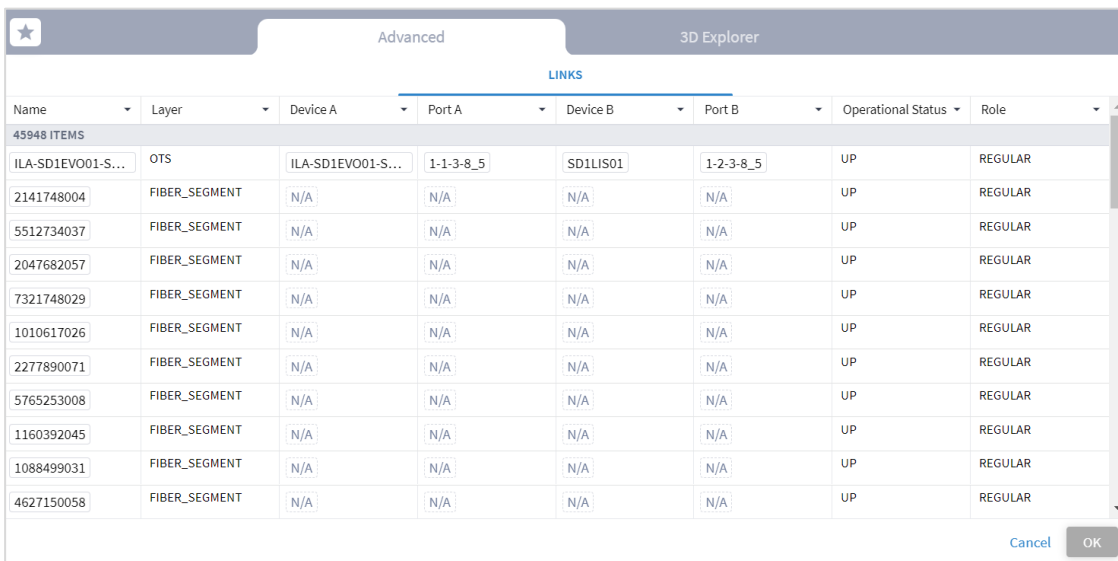
▼ Rule3  

Add Resource

+ Add Policy

Cancel Save

13. Click **Add Resource** to add a resource.



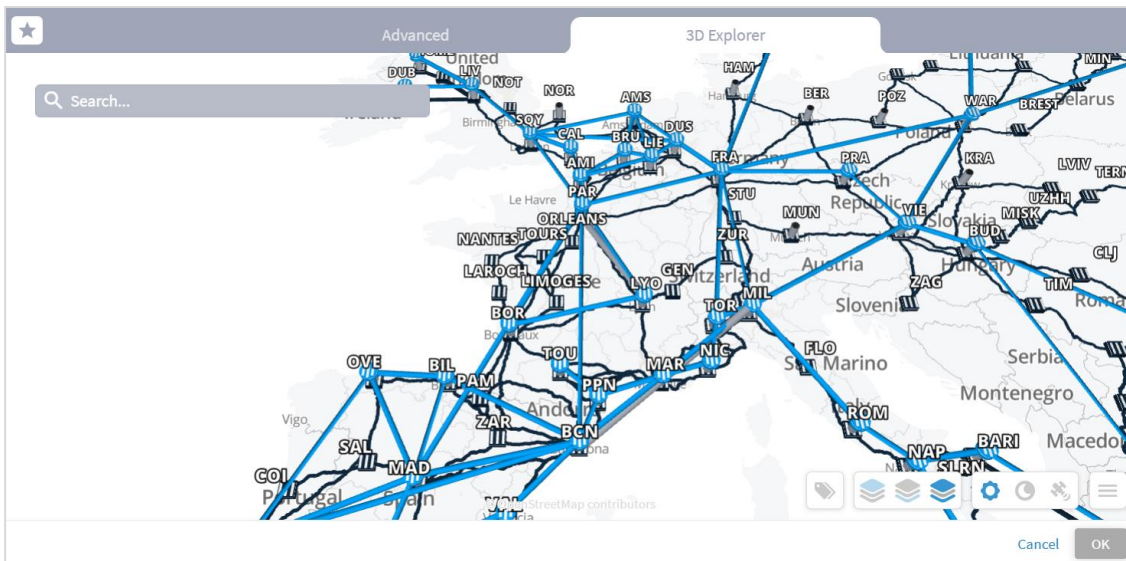
Advanced 3D Explorer

LINKS

Name	Layer	Device A	Port A	Device B	Port B	Operational Status	Role
ILA-SD1EVO01-S...	OTS	ILA-SD1EVO01-S...	1-1-3-8_5	SD1LIS01	1-2-3-8_5	UP	REGULAR
2141748004	FIBER_SEGMENT	N/A	N/A	N/A	N/A	UP	REGULAR
5512734037	FIBER_SEGMENT	N/A	N/A	N/A	N/A	UP	REGULAR
2047682057	FIBER_SEGMENT	N/A	N/A	N/A	N/A	UP	REGULAR
7321748029	FIBER_SEGMENT	N/A	N/A	N/A	N/A	UP	REGULAR
1010617026	FIBER_SEGMENT	N/A	N/A	N/A	N/A	UP	REGULAR
2277890071	FIBER_SEGMENT	N/A	N/A	N/A	N/A	UP	REGULAR
5765253008	FIBER_SEGMENT	N/A	N/A	N/A	N/A	UP	REGULAR
1160392045	FIBER_SEGMENT	N/A	N/A	N/A	N/A	UP	REGULAR
1088499031	FIBER_SEGMENT	N/A	N/A	N/A	N/A	UP	REGULAR
4627150058	FIBER_SEGMENT	N/A	N/A	N/A	N/A	UP	REGULAR

Cancel OK

Or select the **3D Explorer** tab.



In the **Advanced** tab, you can select a link and view the link in the popup map.



14. Select a link and click **OK**.

The screenshot shows the 'Policy Configuration' window. On the left, a list of policies includes 'Policy-2', 'Policy-1', and 'Policy-bla' (which is selected). Below this list is a '+ Add Policy' button. The main area is titled 'Policy-bla' and contains several sections: 'Shared risk resource types' with checkboxes for 'Link', 'Device' (checked), 'Shelf', 'Card', and 'Port'; 'Test type' with radio buttons for 'Multiple links' (selected) and 'Single protected link'; and 'Rules' with a '+ Add Rule' button. Under the 'Rules' section, there is a dropdown menu showing 'qw' and a search box labeled 'Add Resource' with a magnifying glass icon. Below the search box, the value '1010617026' is displayed with a trash icon to its right. At the bottom right of the window are 'Cancel' and 'Save' buttons.

15. If required, add more links to the rule.

16. Click **Save**.

Add Rules using the Shared Risk API

You can add a rule to an existing policy using the Policy API. This enables you to add rules using both GUIDs and/or an SHQL query. For more details, see the *Crosswork Hierarchical Controller NBI and SHQL Guide*.



To add a rule using APIs:

1. Get a list of the policies. See [Get Policies](#).
2. Add a rule to a policy. See [Add a Rule to a Policy](#).
3. You can view the SHQL query in the rule in the Policy Configuration window. See [Edit Policy](#).

Remove Rules

You can remove a rule from a policy.


To remove a rule from a policy:

1. In the applications bar in Crosswork Hierarchical Controller, select **Shared Risk Analysis**.
2. Select the **Policy** tab.
3. Click  **Configure Policies**.
4. Select the required policy.
5. In the **Rules** area, click .
6. Click **Save**.

Edit Policy

You can edit a policy.


To edit a policy:

1. In the applications bar in Crosswork Hierarchical Controller, select **Shared Risk Analysis**.
2. Select the **Policy** tab.
3. Click  **Configure Policies**.
4. Select the required policy.
5. Modify the policy.
6. Click **Save**.

Delete Policy

You can delete a policy.

To delete a policy:

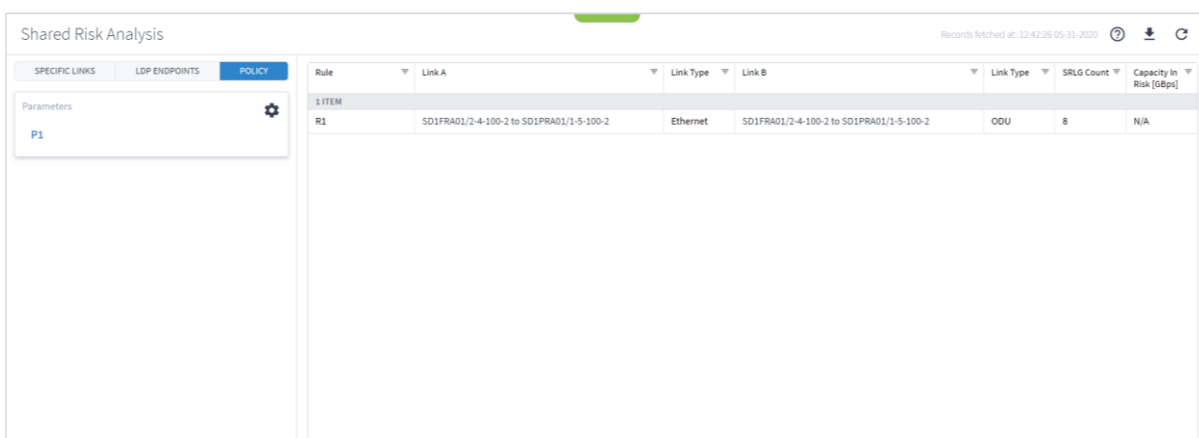
1. In the applications bar in Crosswork Hierarchical Controller, select **Shared Risk Analysis**.
2. Select the **Policy** tab.
3. Click  **Configure Policies**.
4. Select the required policy.
5. Click **Delete policy**.
6. Click **Save**.

Run Policy Test

You can run a test on a policy, checking for shared risk resources of type link, device, shelf, card, and port. Each policy includes one or more rules.

To run a policy test:

1. In the applications bar in Crosswork Hierarchical Controller, select **Shared Risk Analysis**.
2. Select the **Policy** tab.
3. Select the required policy.
4. Click **Run**.



Shared Risk Analysis Records fetched at: 12:42:26 05-31-2020

Rule	Link A	Link Type	Link B	Link Type	SRLG Count	Capacity In Risk [Gbps]
1 ITEM						
R1	SD1FRA01/2-4-100-2 to SD1PRA01/1-5-100-2	Ethernet	SD1FRA01/2-4-100-2 to SD1PRA01/1-5-100-2	ODU	8	N/A

Parameters: P1

5. In the test results, you can select a link and view the link in the popup map and select a row (and click to expand) in the test results to see more details on the shared resources.

The screenshot displays the 'Shared Risk Analysis' interface. At the top, there are tabs for 'SPECIFIC LINKS', 'LDP ENDPOINTS', and 'POLICY'. Below the tabs, there is a table with columns: Rule, Link A, Link Type, Link B, Link Type, SRLG Count, and Capacity In Risk [OBps]. The table contains one row with the following data:

Rule	Link A	Link Type	Link B	Link Type	SRLG Count	Capacity In Risk [OBps]
R1	SD1FRA01/2-4-100-2 to SD1PRA01/1-5-100-2	Ethernet	SD1FRA01/2-4-100-2 to SD1PRA01/1-5-100-2	ODU	8	N/A

Below the table, a popup map is displayed, showing a network topology with various nodes and links. The map includes labels for cities like Amsterdam (AMS), Paris (PAR), London (LON), and others. A red line highlights a specific link between nodes.

Shared Risk API

Crosswork Hierarchical Controller provides APIs to administer shared risk policies and rules.

You can access the Shared Risk API using Swagger: <https://<host>/api/v2/apps/srlg-app/rest/doc>

The APIs include:

- Get a specific policy
- Get all policies
- Create a policy
- Delete a policy
- Change the shared risk type of the policy
- Change a policy type
- Add a new rule to a policy
- Update the rule resources
- Delete a rule from a policy

Get Policies

Use this API to get the list of all the policies. This returns a list of all the policies and their rules.

Request Method

GET

Request URL

`https://example-host/api/v2/apps/srlg-app/rest/policy`

Request Parameters

None

Response Example

```
{
  "name": "policy-1",
  "shared_risk_types": [
    "Link",
    "Port",
    "Card",
    "Shelf",
    "Device"
  ],
  "policy_type": "MULTIPLE-LINKS",
  "rules": [
    {
      "name": "rule-1",
      "resources": [
        "LI/eth/000fc44c94a1f2cd/51308dfd752c1574/df753d953c1e1c8f/f8e7b20537ce03b7"
      ]
    },
    {
      "name": "rule99",
      "resources": [
        "inventory[.name=\"CR1.PAR\"]|port|link[.layer=\"R_LOGICAL\"]"
      ]
    }
  ],
  "name": "test",
  "shared_risk_types": [
    "Link",
    "Device",
    "Shelf",
```

```
    "Port",
    "Card"
  ],
  "policy_type": "MULTIPLE-LINKS",
  "rules": [
    {
      "name": "rule001",
      "resources": [
        "inventory[.name=\"ILA-SD1EVO01-SD1SEV01-1\"]|port|link[.layer=\"R_LOGICAL\"]"
      ]
    }
  ],
  {
    "name": "policy-3",
    "shared_risk_types": [
      "Link"
    ],
    "policy_type": "SINGLE-PROTECTED",
    "rules": [
      {
        "name": "rule-99",
        "resources": [
          "link[.layer=\"R_LOGICAL\"]"
        ]
      }
    ]
  }
}
```

Get a Policy

Use this API to retrieve a policy.

Request Method

GET

Request URL

`https:// example-host/api/v2/apps/srlg-app/rest/policy/{policyGuid}`

Request Parameters

Parameter Name	Data Type	Description
policyGuid	string	The policy guid. Use the guid returned by the Get Policies method.

Response Example

```
{
  "name": "policy-1",
  "shared_risk_types": [
    "Link",
    "Port",
    "Card",
    "Shelf",
    "Device"
  ],
  "policy_type": "MULTIPLE-LINKS",
  "rules": [
    {
      "name": "rule-1",
      "resources": [
        "LI/eth/000fc44c94a1f2cd/51308dfd752c1574/df753d953c1e1c8f/f8e7b20537ce03b7"
      ]
    },
    {
      "name": "rule99",
      "resources": [
        "inventory[.name=\"CR1.PAR\"]|port|link[.layer=\"R_LOGICAL\"]"
      ]
    }
  ]
}
```

Create a Policy

Use this API to create a policy.

Request Method

POST

Request URL

`https://example-host/api/v2/apps/srlg-app/rest/policy/{policyGuid}`

Request Parameters

Parameter Name	Data Type	Description
policyGuid	string	The policy guid. Use the guid returned by the Get Policies method.

Request Body

Parameter Name	Data Type	Description
shared_risk_types	string	Link, Port, Card, Shelf, Device
policy_type	string	SINGLE-PROTECTED or MULTIPLE-LINKS.

Request Body Example

```
{
  "shared_risk_types": [
    "Link"
  ],
  "policy_type": "SINGLE-PROTECTED"
```

Response Example

```
201 Successful Operation
```

Delete Policy

Use this API to delete a policy.

Request Method

DELETE

Request URL

`https://example-host/api/v2/apps/srlg-app/rest/policy/{policyGuid}`

Request Parameters

Parameter Name	Data Type	Description
policyGuid	string	The policy guid. Use the guid returned by the Get Policies method.

Response Example

200 Successful

Update Policy Shared Risk Types

Use this API to change the policy shared risk types.

Request Method

PUT

Request URL

`https://example-host/api/v2/apps/srlg-app/rest/policy/{policyGuid}/shared_risk_types`

Request Parameters

Parameter Name	Data Type	Description
policyGuid	string	The policy guid. Use the guid returned by the Get Policies method.

Request Body

Parameter Name	Data Type	Description
shared_risk_types	string	Link, Port, Card, Shelf, Device

Request Body Example

```
{
  "shared_risk_types": [
    "Link"
  ]
}
```

Response Example

200 Successful Operation

Update Policy Type

Use this API to update credentials.

Request Method

PUT

Request URL

`https://example-host/api/v2/apps/srlg-app/rest/policy/{policyGuid}/policy-type`

Request Parameters

Parameter Name	Data Type	Description
policyGuid	string	The policy guid. Use the guid returned by the Get Policies method.

Request Body

Parameter Name	Data Type	Description
policy_type	string	SINGLE-PROTECTED or MULTIPLE-LINKS.

Request Body Example

```
{
  "policy_type": "SINGLE-PROTECTED"
}
```

Response Example

200 Successful Operation

Add a Rule to a Policy

Use this API to add a rule to a policy. You can use an array of GUIDs and/or an SHQL query to create the rule.

Request Method

POST

Request URL

`https://example-host/api/v2/apps/srlg-app/rest/policy/{policyGuid}/rules{ruleName}`

Request Parameters

Parameter Name	Data Type	Description
policyGuid	string	The policy guid. Use the guid returned by the Get Policies method.
ruleName	string	The rule name. Use one of the rule names returned by the Get Policies method.

Request Body

Parameter Name	Data Type	Description
resources	array(string)	A list of GUID links and/or an SHQL query. If you use an SQL query, make sure that the expression is valid and returns a result. See the SQL User Guide. When you pass an SQL query, ensure that you wrap "...." with a pair of \s, for example: "link[.layer=\R_LOGICAL\]"

Request Body Example

```
{
  "resources": [
    "link[.layer=\R_LOGICAL\]"
  ]
}
```

or

```
{
  "resources": [
    "LI/guid1",
    "LI/guid2"
  ]
}
```

or

```
{
  "resources": [
    "inventory[.name=\CR1.PAR\]|port|link[.layer=\R_LOGICAL\]"
  ]
}
```

Response Example

201 Successful Operation

Update a Rule

Use this API to update the rule's resources. You can use an array of GUIDs and/or an SHQL query to create the rule.

Request Method

PUT

Request URL

`https://example-host/api/v2/apps/srlg-app/rest/policy/{policyGuid}/rules{ruleName}`

Request Parameters

Parameter Name	Data Type	Description
policyGuid	string	The policy guid. Use the guid returned by the Get Policies method.
ruleName	string	The rule name. Use one of the rule names returned by the Get Policies method.

Request Body

Parameter Name	Data Type	Description
resources	array(string)	A list of GUID links and/or an SHQL query. If you use an SQL query, make sure that the expression is valid and returns a result. See the SQL User Guide. When you pass an SQL query, ensure that you wrap "...." with a pair of \s, for example: "link[.layer=\R_LOGICAL\]"

Request Body Example

```
{
  "resources": [
    "link[.layer=\R_LOGICAL\]"
  ]
}
```

or

```
{
  "resources": [
    "LI/guid1",
    "LI/guid2"
  ]
}
```

or

```
{
  "resources": [
    "inventory[.name=\CR1.PAR\]|port|link[.layer=\R_LOGICAL\]"
  ]
}
```

Response Example

201 Successful Operation

Delete a Rule from a Policy

Use this API to delete a rule from a policy.

Request Method

DELETE

Request URL

```
https://example-host/api/v2/apps/srlg-app/rest/policy/{policyGuid}
/policy/{policyGuid}/rules/{ruleName}
```

Request Parameters

Parameter Name	Data Type	Description
policyGuid	string	The policy guid. Use the guid returned by the Get Policies method.
ruleName	string	The rule name. Use one of the rule names returned by the Get Policies method.

Response Example

```
200 Successful
```

Failure Impact

The Crosswork Hierarchical Controller Failure Impact application allows simulation of resource failures in a multidomain network, pointing to the specific domain in which the failure originated and the impact on services and network resources.

This application simulates the impact of a failure in a selected resource (link, device or site) on one or more network objects in the network where the application searches for alternative path to links or services (both, customer-based and resource-based) over the selected resource and provides results to show the impact on the services. The alternative path can be minimized by latency, number of hops, or admin costs and it is displayed with a comparison of the current path to the alternative found path.

You can also exclude resources from the calculated alternative path by selecting specific resources (objects such as devices, ports, and links) or by using tags as reference to group of resources.

This solves the failure impact problem by providing detailed results that can be acted on. For example, additional links can be added to vulnerable points, and any required changes can be made to the topology. This results in reduced failure impact and increased network reliability.

Run Failure Impact Test

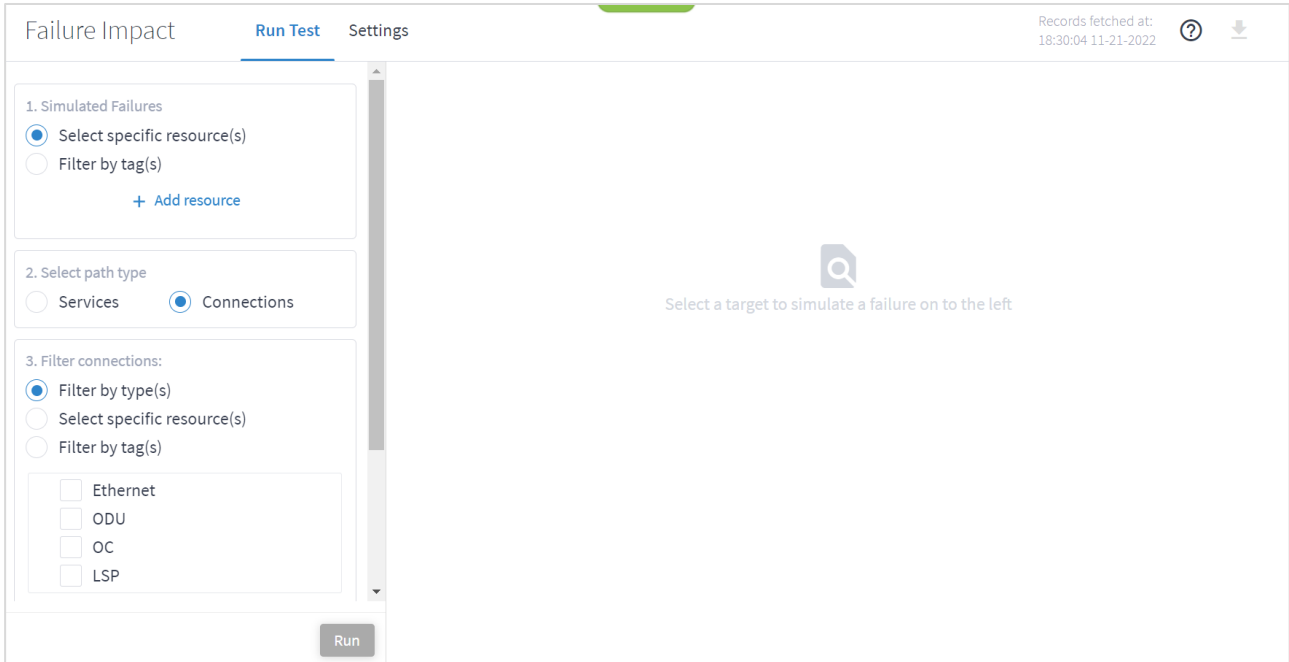
You can run a failure impact test on one or more devices, links and/or sites. The Failure Impact application creates a list of affected services/connections and, if an alternative path exists, the application shows the current and the alternative path for each service/connection.

You can set various options for the test:

- The path optimization criteria (path minimization) can be configured as the number of hops, latency, or admin cost.
- Whether to assess the failure impact by services path or by connections path.
- Depending on the path type selected:
 - Which services to filter by, either E-Line and/or OTN Line or specific services.
 - Which connection type, Ethernet, ODU, OC, and/or LSP, or specific connections.
- Whether to exclude resources from the calculated path(s) selected by:
 - Specific resources selected by the model selector.
 - Use tags.

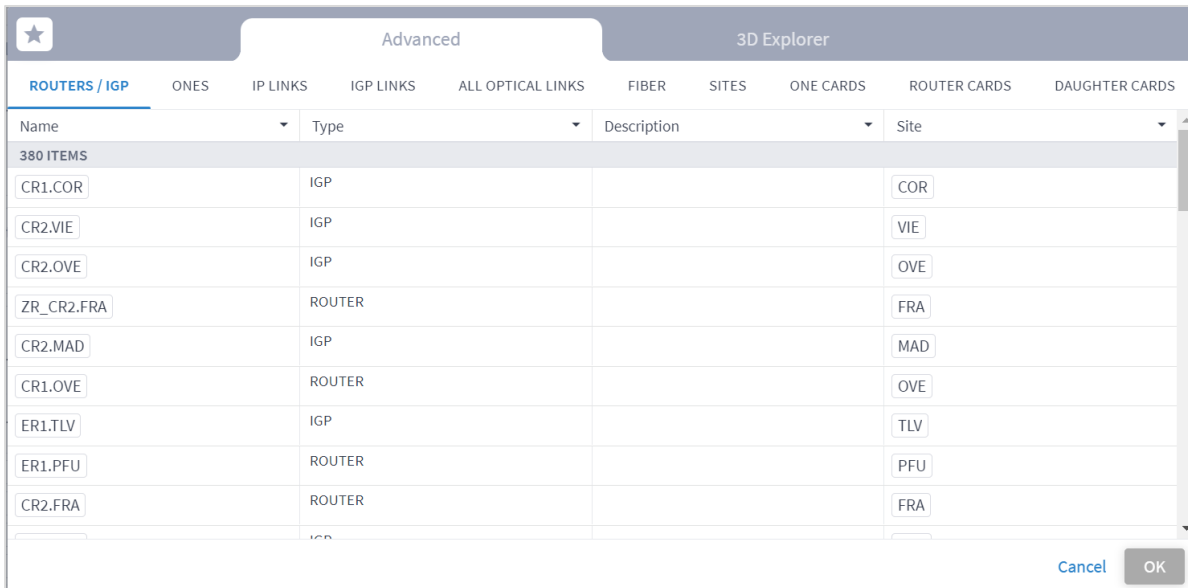
To run a failure impact test:

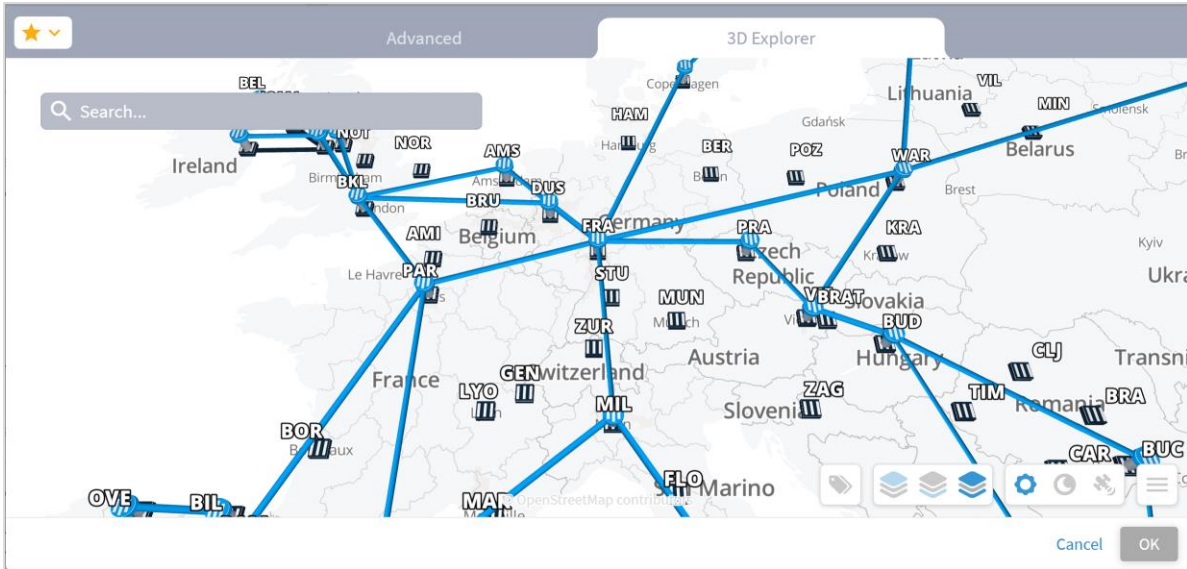
1. In the applications bar, select **Failure Impact**.



2. In the **Simulated Failures** area, do one of the following:

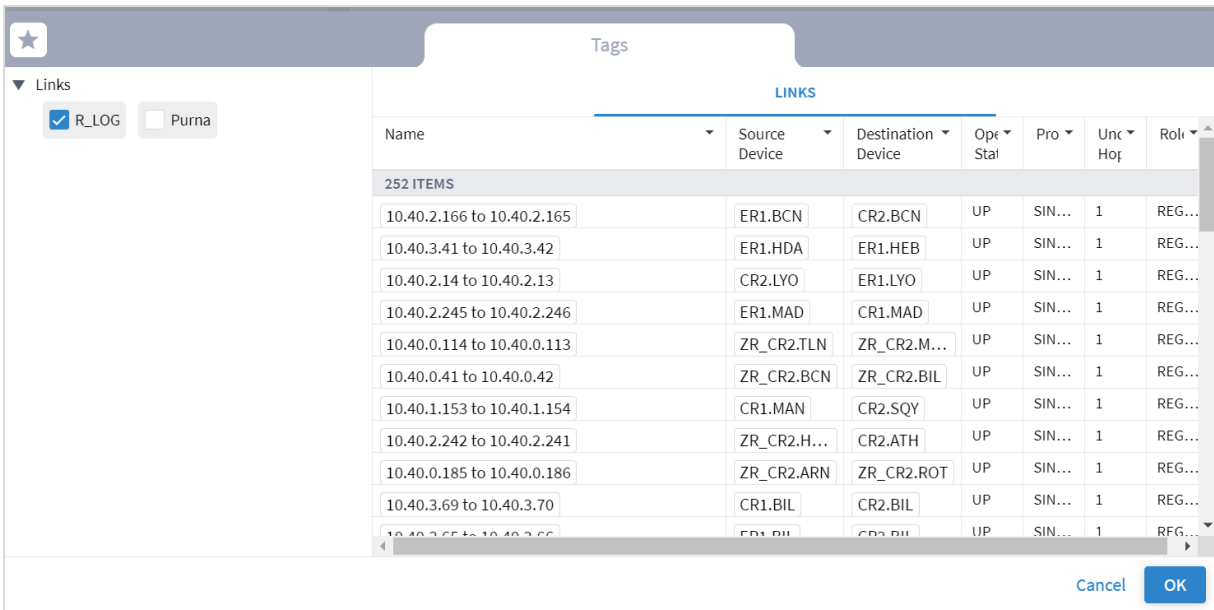
- Choose **Select specific resource(s)** and then click **Add resource**. In the **Advanced** tab, select a resource, or click on the **3D Explorer** tab to select a resource. You can add up to 10 items.





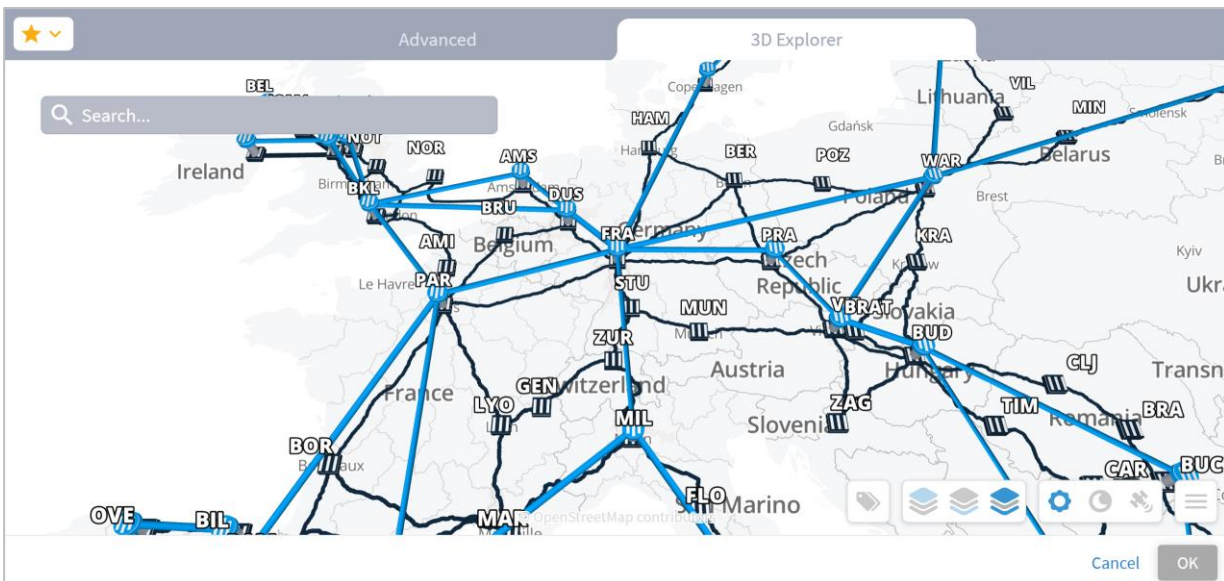
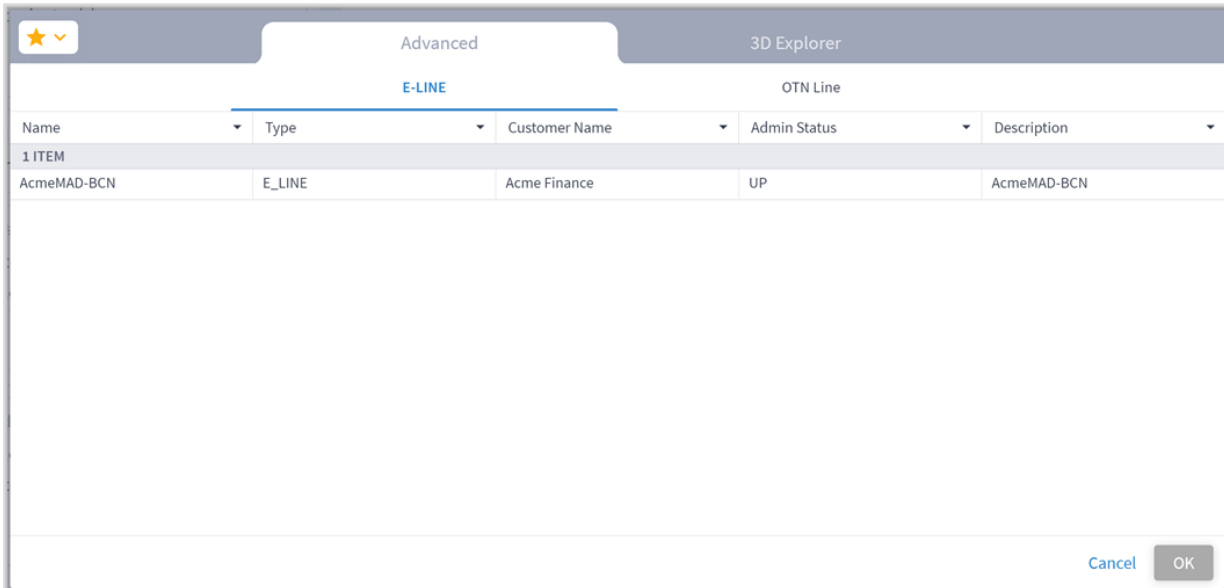
Note: For more information on 3D Explorer, see the *Cisco Crosswork Hierarchical Controller Network Visualization Guide*.

- Choose **Filter by tag(s)** and then click **Add Tags**, then select a tag and click **OK**. Select more tags if required.



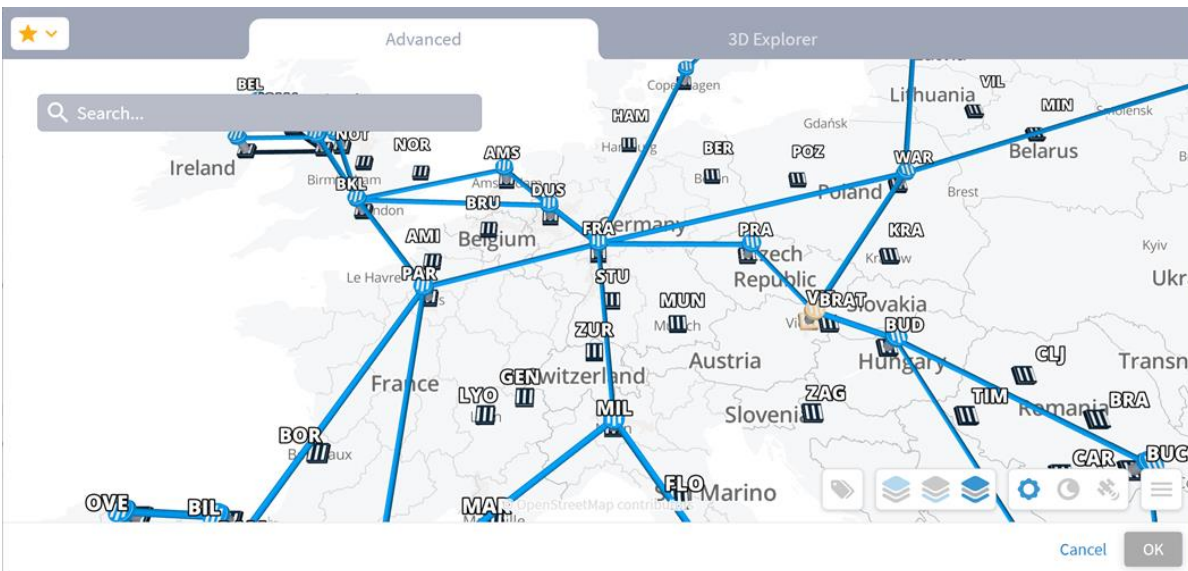
3. Select the **Select path type** (either **Services** or **Connections**).
4. Select the **Filter by type(s)**:
 - For services, **E-LINE** and/or **OTN LINE**.
 - For connections, **Ethernet**, **ODU**, **OC**, and/or **LSP**.

- (Optional) For services, select the **Select specific services** and then click **Add service**. In the **Advanced** tab, select a service, or click on the **3D Explorer** tab to select a service. You can add up to 10 items.



6. (Optional) For connections, select the **Select specific resource(s)** and then click **Add resource**. In the **Advanced** tab, select a resource, or click on the **3D Explorer** tab to select a resource. You can add up to 10 items.

ETHERNET		ODU		OC		LSP	
Name	Layer	Device A	Port A	Device B	Port B	Operational Status	Role
444 ITEMS							
RD_PAR01_AO...	ETH	RD_PAR01_AO...	R-ETH-1-1-21	RD_PRA01_AO...	R-ETH-1-1-13	UP	REGULAR
TenGigE0/0/1/...	ETH	ER1.ONO	TenGigE0/0/1/11	SD1ONO01	1-2-4	UP	CROSS_LINK
ZR_CR2.FRA/F...	ETH	ZR_CR2.FRA	FourHundred...	ZR_CR2.MIL	FourHundred...	UP	REGULAR
TenGigE0/0/1/...	ETH	CR1.MAN	TenGigE0/0/1/13	SD1MAN01	1-5-4	UP	CROSS_LINK
OTN1BOR01/1...	ETH	OTN1BOR01	1-4-4	OTN1PAR01	1-5-4	UP	REGULAR
RD_FRA01_AO...	ETH	RD_FRA01_AO...	R-ETH-1-1-17	RD_BLA01_AO...	R-ETH-1-1-17	UP	REGULAR
SD2MMO01/ET...	ETH	SD2MMO01	ETH-1-1-20	SD2MMO02	ETH-1-1-5	UP	CROSS_SUBNET_...
SD1BCN01/3-6...	ETH	SD1BCN01	3-6-1	SD1CUP01	1-2-1	UP	REGULAR
SD2HERKL01/...	ETH	SD2HERKL01	ETH-1-1-39	SD2TLV01	ETH-1-1-11	UP	REGULAR



7. (Optional) In the **Exclude resources from calculated path(s)** area, and then:
 - Choose **Select specific resource(s)** and then click **Add resource**. In the **Advanced** tab, select a resource, or click on the **3D Explorer** tab to select a resource. You can add up to 10 items.
 - Choose **Filter by tag(s)** and then click **Add tag**, then select a tag, select the required tag value and click OK. Add more tags if required.

8. Click **Run**. The impacted services and connections appear, with the root causes listed in the lower pane.

Impacted services and connections

Failed L1 (OMS) links	Failed L3 (logical) links	Failed ONEs	Failed Routers	LSP connections: Total: 1687		
0	252	0	0	1574	0	1574
				Affected connections	With alt. path(s)	No alt. path(s)

Select a widget above to see its results

9. Select a widget to see its results.


Impacted services and connections

Failed L1 (OMS) links: 0 Failed L3 (logical) links: 252 Failed ONEs: 0 Failed Routers: 0

LSP connections: Total: 1687

1574 Affected connections 0 With alt. path(s) 1574 No alt. path(s)

Name	Device A	Device B	Port A	Port B	Tags	Number Of Upper Links
252 ITEMS						
10.40.1.113 to 1...			TenGigE0/0/1/12	TenGigE0/0/1/11	Links R_LOG Link	25
10.40.1.62 to 10...			FourHundredGig...	FourHundredGig...	Links R_LOG Link	1
10.40.0.185 to 1...			FourHundredGig...	FourHundredGig...	Links R_LOG Link	1
10.40.0.6 to 10.4...			FourHundredGig...	FourHundredGig...	Links R_LOG Link	1
10.40.3.105 to 1...			TenGigE0/0/1/11	TenGigE0/0/1/14	Links R_LOG Link	75
10.40.1.57 to 10...			FourHundredGig...	FourHundredGig...	Links R_LOG Link	1
10.40.1.186 to 1...			10ge-0/1/7	TenGigE0/0/1/11	Links R_LOG Link	1
10.40.3.150 to 1...			HundredGigE0/0...	HundredGigE0/0...	Links R_LOG Link	1
10.40.3.13 to 10...			TenGigE0/0/3/6	TenGigE0/0/1/11	Links R_LOG Link	6
10.40.1.1 to 10.4...			FourHundredGig...	FourHundredGig...	Links R_LOG Link	1
10.40.2.133 to 1...			GigabitEthernet...	TenGigE0/0/1/12	Links R_LOG Link	2
10.40.3.137 to 1...			HundredGigE0/0...	HundredGigE0/0...	Links R_LOG Link	1
10.40.2.57 to 10...			HundredGigE0/0...	HundredGigE0/0...	Links R_LOG Link	2

10. To filter the table, click  and select the required options.

Current Path's Hops Count

Filter

Select All Clear All

4 16

5 8

3 6

6 2

Cancel Apply


Hide Column


Restore All Columns

11. To remove a column, click **Hide Column**.

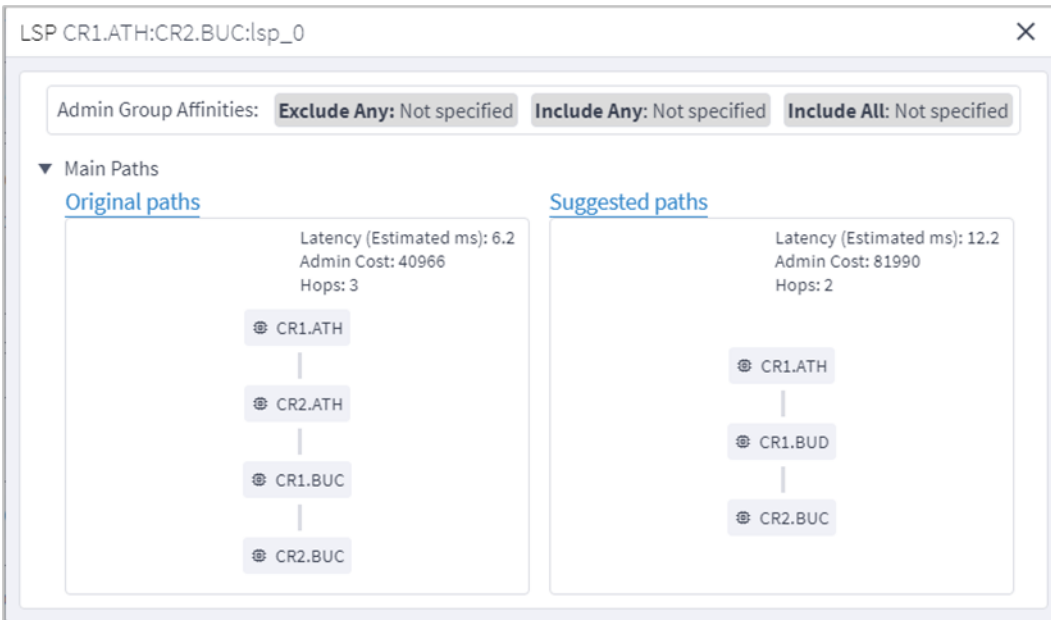
12. To restore all columns, click **Restore All Columns**.

13. To sort the table, click on a column heading.

↓ Connection Type 

↑ Connection Type 

14. Click to select an item in the list. A list of the **Original paths** and **Suggested paths** appears. The simulated failed links show in purple.



15. Click a resource to view the resource in the 3D Explorer map.

Configure the Failure Impact Settings

You can configure various failure impact settings.

When the actual latency of all the links in a path is not known, a fudge factor for optimal paths latency setting is used to set a best guess distance multiplier for the links with missing latency. This multiplier is applied to the geographical distance between the endpoints of the link, and the factored distance is used to estimate the latency of the link.

Note: Setting a high value for the fudge factor means that such a path is only selected if it is significantly shorter than all other alternatives.

The algorithm for computing approximate latency only uses the fudge factor for the links in the path where the distance and latency are missing and is applied as follows:

- Let $L(X,Y)$ be the geographical distance between endpoints X and Y divided by speed of light in fiber.
- For an OTS link between X and Y, if the latency is missing, use $F*L(X,Y)$
- If a higher layer link Z between X and Y has a direct latency value - use it as it is the most accurate value. Otherwise:
 - If Z has a full path - use the sum of latencies of the links along the path (some of which may have been recursively estimated).
 - If Z has a gap in its path between site X and Y - compute the latency of the gap the same way: $F*L(X,Y)$.
 - If Z does not have a path - use $F*L(X,Y)$ for the latency.

To set the failure impact settings:

1. In the applications bar, select **Failure Impact**.
2. Select the **Settings** tab.

Failure Impact Run Test Settings Records fetched at: 18:56:19 11-21-2022

Path Optimization Criteria

Path optimization criteria
Number of Hops

Administratively down objects

Check failure impact on administratively down connections and services
If the above is selected, the optimizer will include administratively down connections in the list of connections it will try to optimize. A connection is considered administratively down if at least one of its endpoints is in admin down state.

Include administratively down links in calculation of alternative path
If the above is selected, then when the optimizer evaluates alternative paths for connections, it will include paths that contain links in administratively down state. A link is considered administratively down if at least one of its endpoints is in admin down state.

Protected Path Diversity Level

Link
 Device
 Site
Select the level in which main and protection paths must be diverse.

Protected Path Diversity Policy

Diversions Policy

3. Select the **Path Optimization Criteria**:
 - **Number of Hops**: Optimize by the number of hops.
 - **Latency [milliseconds]**: Optimize by the latency.
 - **Admin Cost**: Optimize by the admin cost
4. Select how to handle **Administratively down objects**:
 - **Check failure impact on administratively down connections and services**: Select this option to include in recalculation, connections or services that are down (connections and services that at least one of their end ports is administratively down are considered down).
 - **Include administratively down links in calculation of alternative path**: Select this option to include links that are down in the calculation of new alternative paths for impacted connections or services (links with at least one of their end ports administratively down are considered down).
5. Sets the level in which the main and protection paths must be diverse by selecting the **Protected Path Diversity Level (Link, Device, and/or Site)**. The diversity level selected implies the diversity in all layers, down to fiber path. For example, if link is selected, the algorithm checks that no link is shared in all L3 to L1 layers, down to the physical fiber path (if discovered by Crosswork Hierarchical Controller).
6. Select the **Protected Path Diversity Policy**:
 - **Strict**: Only find strictly diverse protection paths.
 - **Best Effort**: Find the “best effort” diverse protection paths. This first tries to optimize the protected path diversity taking devices, sites and links into account. If this fails, it tries to

optimize the protected path diversity taking devices and links into account. If this fails, it tries to optimize for links only. If this fails, the protected path diversity does not take devices, sites or links into account.

7. Set the **Unknown Latency Path** options:

- **Fudge factor for the current paths latency:** This is the fudge factor for the current paths latency. Set this fudge factor to high number means that the estimated latency of some links on the current path will be high, and Crosswork Hierarchical Controller will offer potentially optimal paths even if they are not highly likely to be more optimal.
- **Fudge factor for the optimal paths latency:** This is the fudge factor for optimal paths latency. Setting this fudge factor to a high number means that these links will be selected as an alternative only when there is a high likelihood that such a path is indeed shorter than other alternatives.

8. Click **Save Changes**.


Export Test Results

The tabular test results can be exported into a zip file with one or two CSV files for offline analysis. One file includes the services (if you selected the services path type) and the other includes the connections.

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	
1	Execution Parameter	Value														
2	Time	15:14:26 07-20-2020 UTC														
3	Optimization Goal	NUMBER_OF_HOPS														
4	Optimize down services and resources	TRUE														
5	Include down links in calculation of alternative	TRUE														
6	Latency fudge factor a	3														
7	Latency fudge factor b	2														
8	Protection path diversity level site	FALSE														
9	Protection path diversity level device	FALSE														
10	Protection path diversity level link	FALSE														
11	Protection path diversion policy	Best Effort														
12	Ldp enabled	FALSE														
13	Affected connections	Ethernet														
14	Affected Services	E-Line														
15																
16	Service	Service Ty	Customer	Connector	Connector	Original Pa	Original Pa	Original Pa	Original Pa	Suggested	Suggested	Suggested	Suggested	Hops diff	Latency dif	Adm
17	AcmeMAD-BCN	E-Line	Acme Finar	Acme MAC	Ethernet	Main	3 (Main), 9.2	486	Main	3 (Main), 6.1	486	0.0	-33.7	0.0		

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
1	Execution Parameter	Value													
2	Time	15:14:26 07-20-2020 UTC													
3	Optimization Goal	NUMBER_OF_HOPS													
4	Optimize down services and resources	TRUE													
5	Include down links in calculation of alternative	TRUE													
6	Latency fudge factor a	3													
7	Latency fudge factor b	2													
8	Protection path diversity level site	FALSE													
9	Protection path diversity level device	FALSE													
10	Protection path diversity level link	FALSE													
11	Protection path diversion policy	Best Effort													
12	Ldp enabled	FALSE													
13	Affected connections	Ethernet													
14	Affected Services	E-Line													
15															
16	Connection	Connector	Protected	Original Pa	Original Pa	Original Pa	Original Pa	Suggested	Suggested	Suggested	Suggested	Hops diff	Latency dif	Admin Cos	Comments
17	Acme MAD - BCN	Ethernet	Yes	Main	3 (Main), 9.2	486	Main	3 (Main), 6.1	486	0.0	-33.7	0.0			Protection pa
18	OTN1MAD01/ to OTN1BCN01/	ODU	Yes	Main	3 (Main), 9.2	486	Main	3 (Main), 6.1	486	0.0	-33.7	0.0			Protection pa

To export the test results:

1. In the applications bar, select **Failure Impact**.
2. Run the required test.
3. Click . The file is downloaded automatically

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at <https://www.cisco.com/go/offices>.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: <https://www.cisco.com/go/trademarks>. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)