

Configure Disjoint Layer 2 in Intersight Managed Mode Domain

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Components Used](#)

[Background Information](#)

[Disjoint Layer 2 \(DL2\)](#)

[Network Diagram](#)

[Configure](#)

[Step 1. Create a VLAN Policy that includes all VLANs](#)

[Step 2. Create a Ethernet Network Group Policy](#)

[Step 3. Create a New Ethernet Network Group Policy for the Virtual NICs \(Optional\)](#)

[Step 4. Create or Modify the Port Policy](#)

[Step 5. Assign the VLAN Policy and the Port Policy to the Domain Profile](#)

[Step 6. Assign the Ethernet Group Policy to a LAN Connectivity Policy](#)

[Verify](#)

[Related Information](#)

Introduction

This document describes how to deploy disjoint Layer 2 networks upstream of the Fabric Interconnects while in Intersight Managed Mode.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Basic understanding of Disjoint Layer 2 networks.
- Basic understanding of how to configure a UCS Domain in Intersight Managed Mode.

Components Used

- Intersight Managed Mode
- 6454 Fabric Interconnect
- 4.2.1g Firmware

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

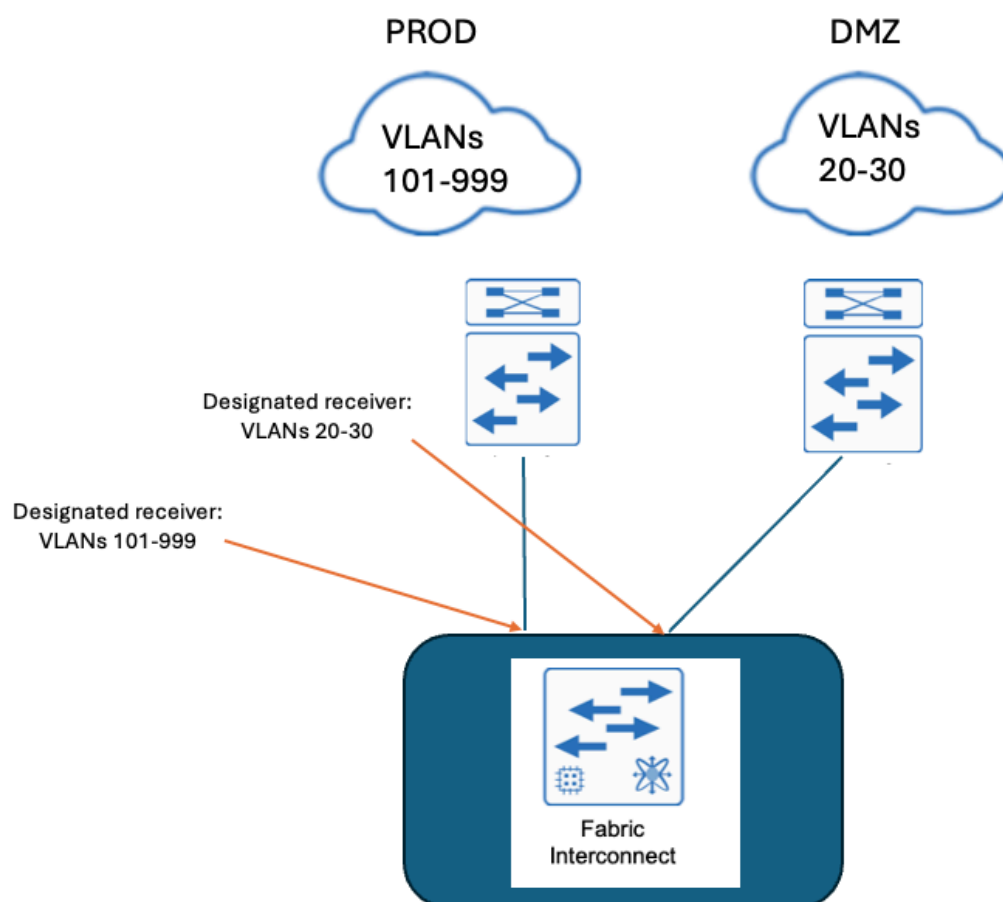
Background Information

Disjoint Layer 2 (DL2)

Disjoint layer-2 networks are required if you have two or more Ethernet clouds that never connect, but must be accessed by servers or virtual machines located in the same Cisco UCS domain.


They are also required in a multi-tenant environment if servers or virtual machines for more than one client are located in the same Cisco UCS domain and they need to access the L2 networks for both clients.

Network Diagram

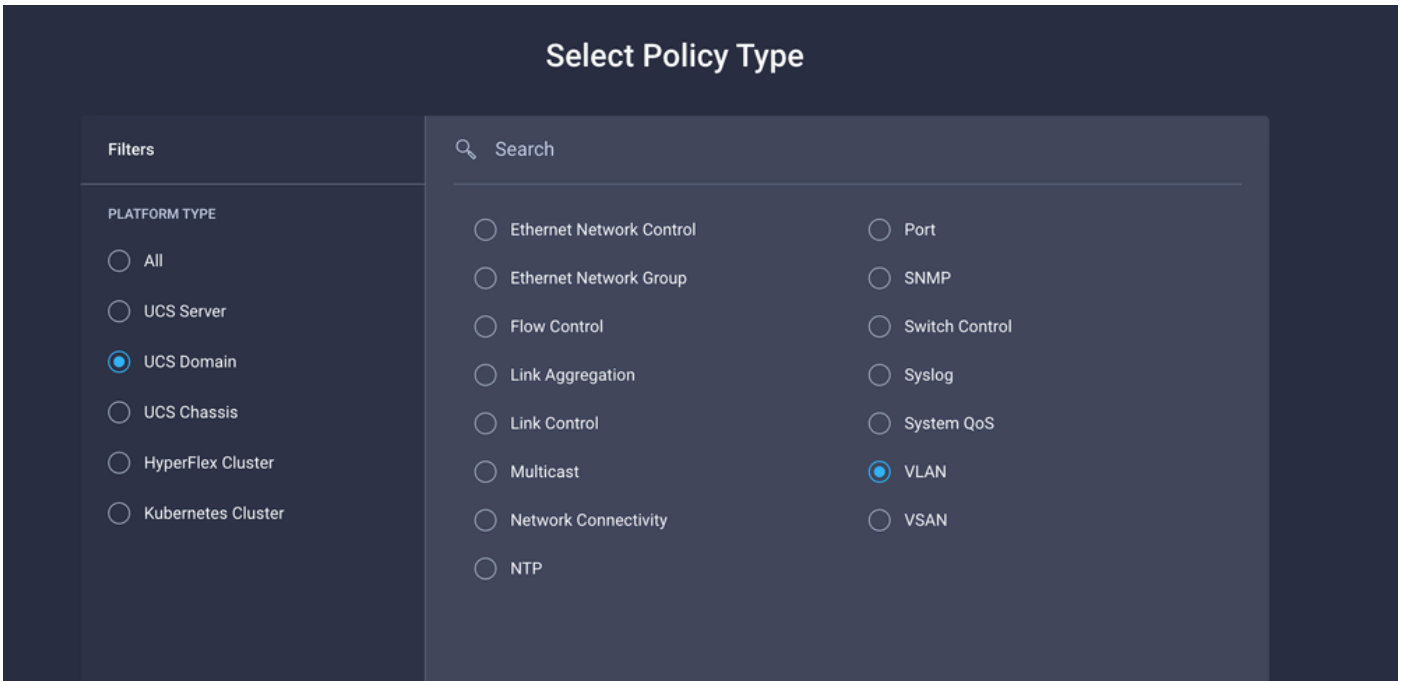


Configure

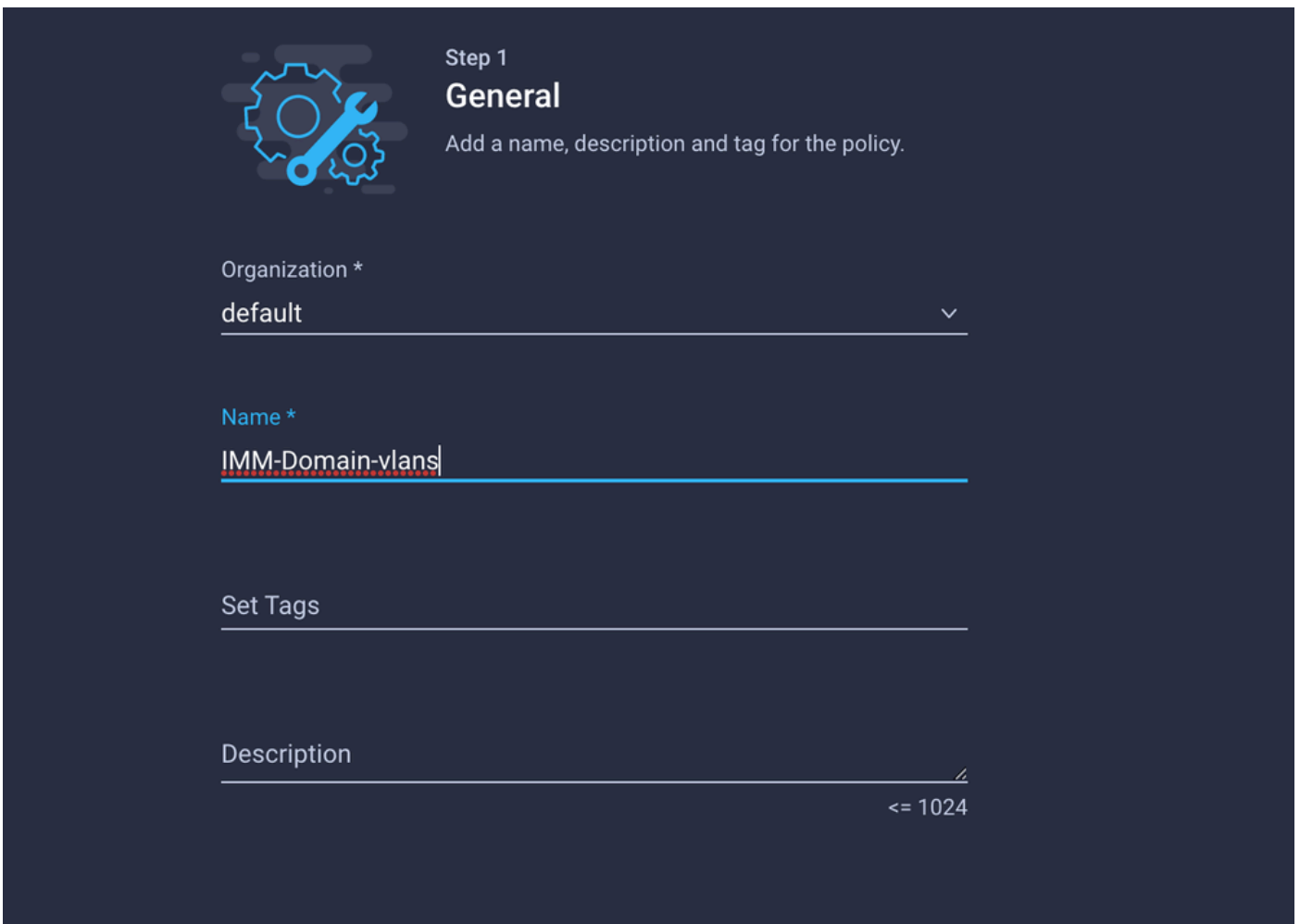
Step 1. Create a VLAN Policy that includes all VLANs

 **Note:** This includes our Production VLANs called PROD and our Demilitarized Zone VLANs called DMZ that are to be present in the environment.

Navigate to **Policies > Create Policy > VLAN**.



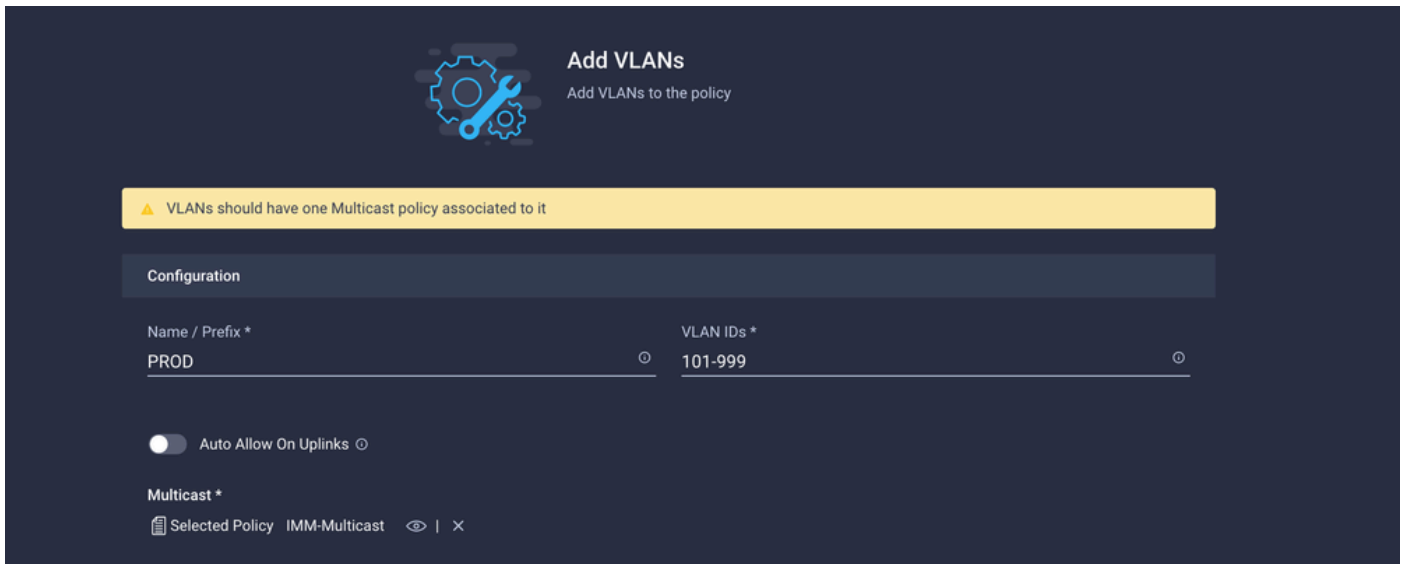
Create a Name and click **Next**.



Click **Add VLANs**.

Now when you add the VLAN or VLAN range for the PROD/DMZ network ensure to leave **Auto Allow on Uplinks** unchecked and add a Multicast policy. This ensures that these VLANs can be disjointed and

assigned to specific ports or port channels later.



Add VLANs
Add VLANs to the policy

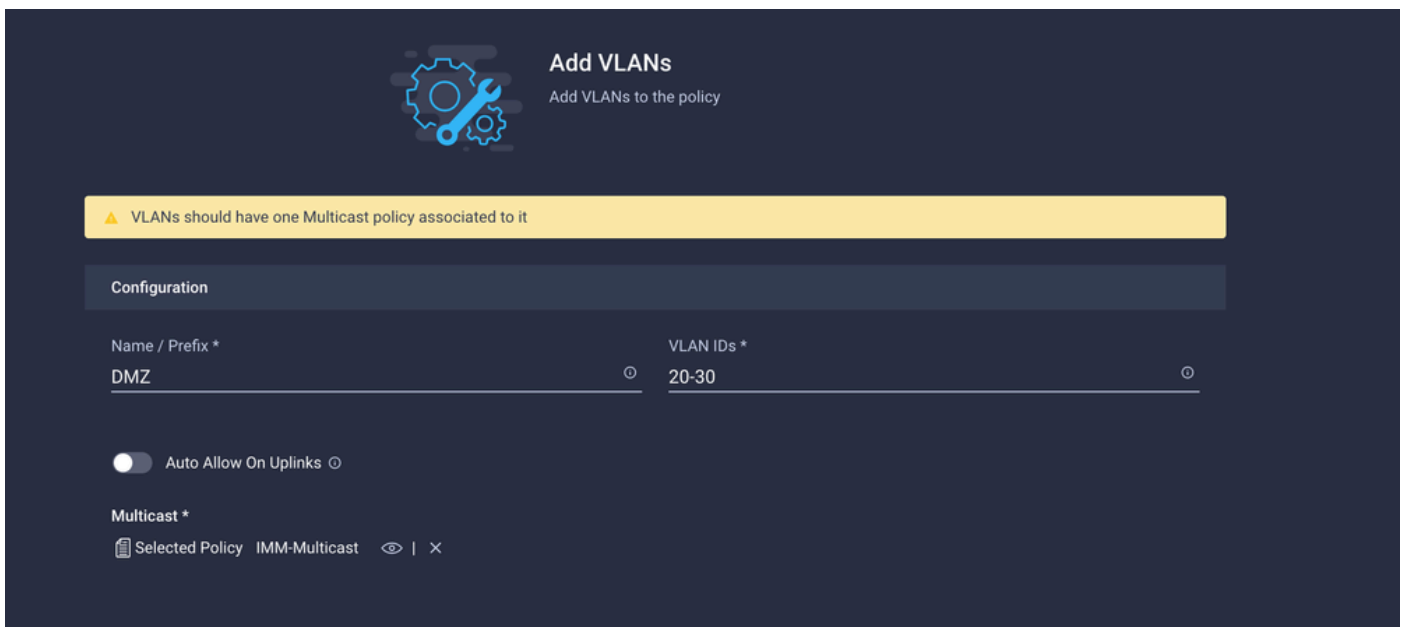
⚠ VLANs should have one Multicast policy associated to it

Configuration

Name / Prefix * VLAN IDs *

Auto Allow On Uplinks

Multicast *
Selected Policy IMM-Multicast



Add VLANs
Add VLANs to the policy

⚠ VLANs should have one Multicast policy associated to it

Configuration

Name / Prefix * VLAN IDs *

Auto Allow On Uplinks

Multicast *
Selected Policy IMM-Multicast

Once finished click **Add** to add the VLANs to the VLAN policy and click **Create**.

Step 2. Create a Ethernet Network Group Policy

This policy is used to assign the group of VLANs to specific Uplinks.

Navigate to **Policies > Create Policy > Ethernet Network Group**.

The first group of VLANs is for the Production Uplink.

Select Policy Type

Filters

PLATFORM TYPE

- All
- UCS Server
- UCS Domain
- UCS Chassis
- HyperFlex Cluster
- Kubernetes Cluster

Search

- Ethernet Network Control
- Ethernet Network Group
- Flow Control
- Link Aggregation
- Link Control
- Multicast
- Network Connectivity
- NTP
- Port
- SNMP
- Switch Control
- Syslog
- System QoS
- VLAN
- VSAN

Create a Name and click **Next**.



Step 1

General

Add a name, description and tag for the policy.

Organization *

default



Name *

Prod-vlans

Set Tags

Description

<= 1024



Step 2

Policy Details

Add policy details

VLAN Settings

Allowed VLANs

101-999



Native VLAN

1



1 - 4093

The second group is for the DMZ Uplink.



Step 1

General

Add a name, description and tag for the policy.

Organization *

default



Name *

DMZ-vlans

Set Tags

Description

<= 1024



Step 2

Policy Details

Add policy details

VLAN Settings

Allowed VLANs

20-30



Native VLAN

1



1 - 4093

Step 3. Create a New Ethernet Network Group Policy for the Virtual NICs (Optional)

This step is optional because the Ethernet Network Group Policies that you have created in Step 2. can also be reused to assign them to the vNICs on a Service Profile.

 **Note:** If the policies are reused then all the VLANs allowed on the Uplink are also allowed on the vNIC. If it is preferred to only allow a subset of VLANs then you need to create a separate policy and allow the preferred VLANs on the vNIC.

Navigate to **Policies > Create Policy > Ethernet Network Group**.

Create a Name and click **Next**.



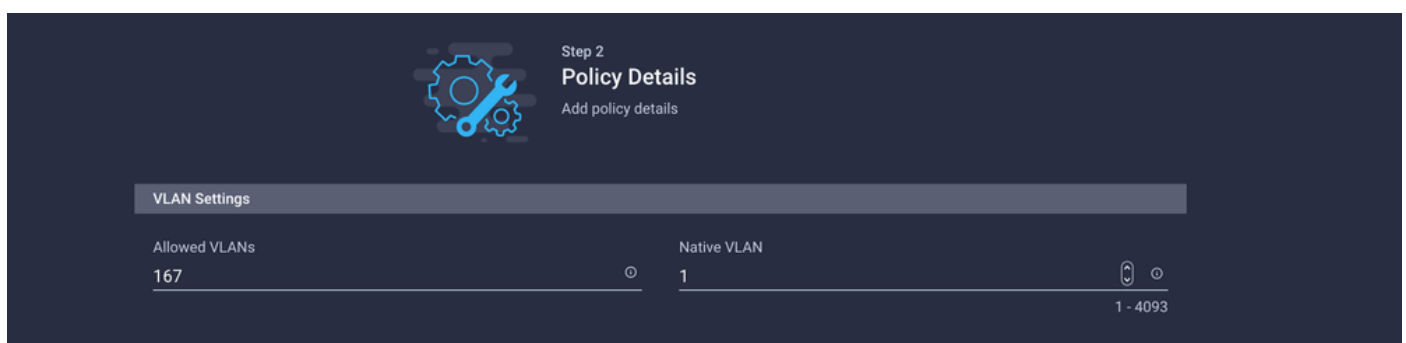
Step 1
General
Add a name, description and tag for the policy.

Organization *
default

Name *
MGMT-VNIC-167

Set Tags

Description
≤ 1024



Step 2
Policy Details
Add policy details

VLAN Settings

Allowed VLANs	Native VLAN
167	1

1 - 4093

Create another Ethernet Network Group for the other DMZ VLAN.



Step 1

General

Add a name, description and tag for the policy.

Organization *

default

Name *

DMZ-VNIC-20

Set Tags

Description

<= 1024



Step 2

Policy Details

Add policy details

VLAN Settings

Allowed VLANs

20



Native VLAN

1



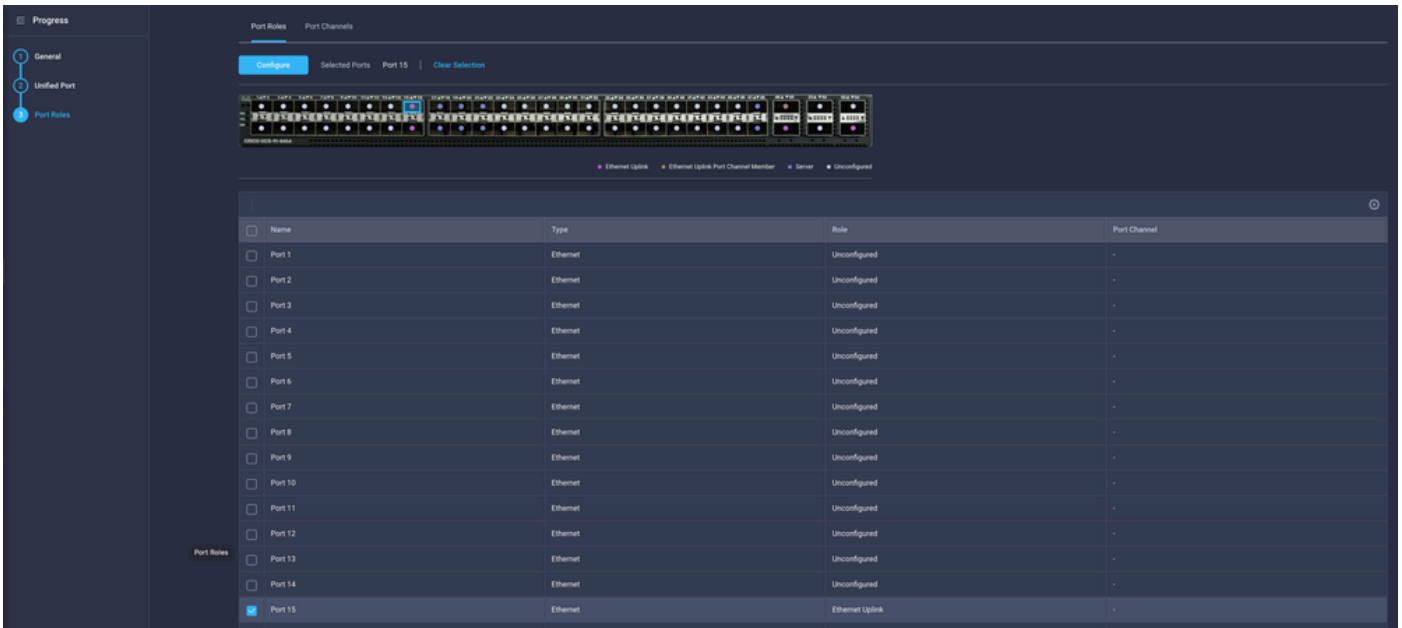
1 - 4093

Step 4. Create or Modify the Port Policy

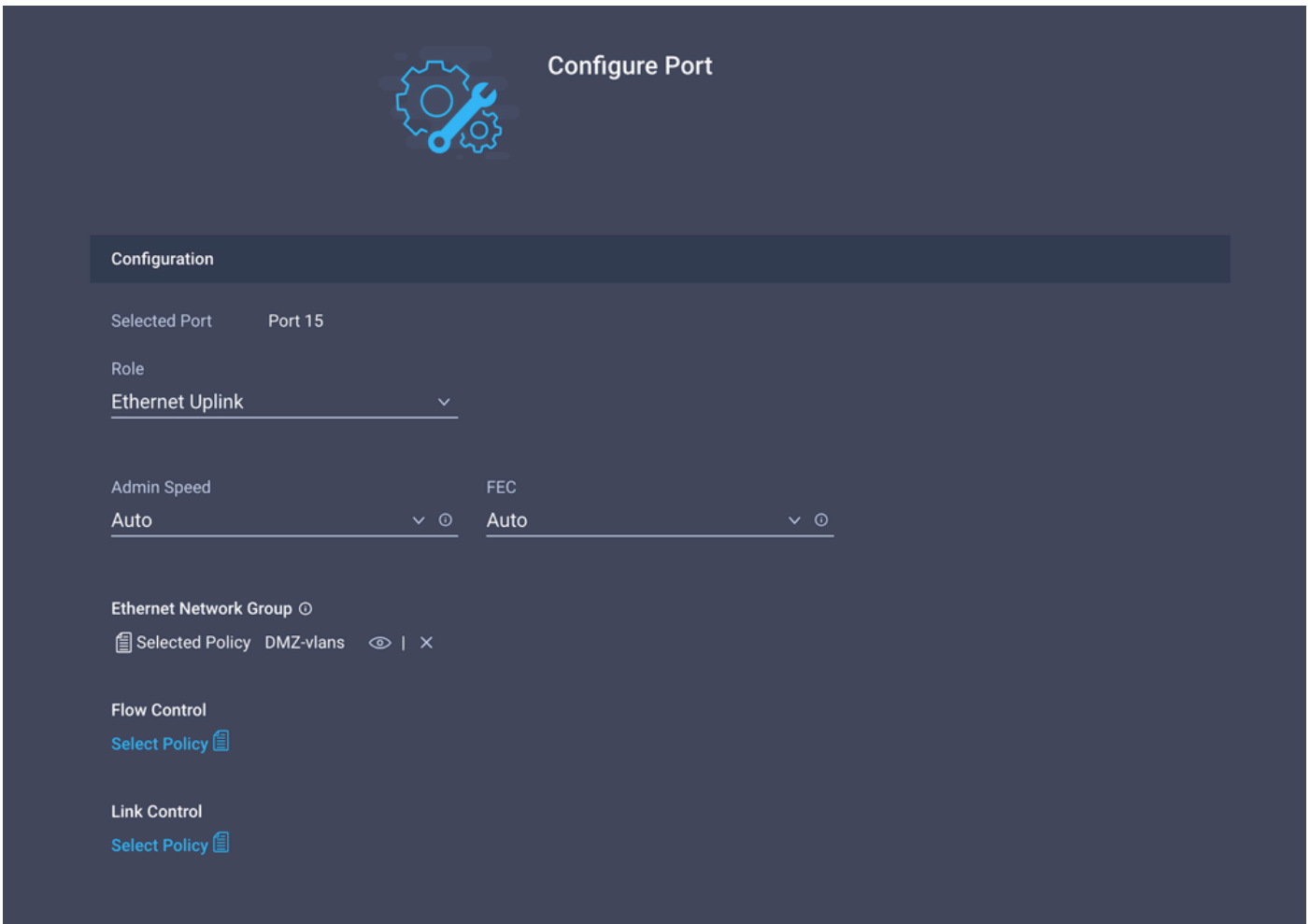
Create a Port Policy or modify the one that already exists, then assign it to the Ethernet Network Group and to the appropriate Uplinks.

Navigate to the **Policies** tab > **Create Policy** > select **Port** > Create a **Name** > **Next**.

Select the **Port** or **Port-channel** and click **Configure**.



Assign the Ethernet Network Group created in Step 2.



Repeat the same process for the other Uplink.

Progress

General
Unified Port
Port Rules

Port Rules Port Channels

Configure Selected Ports Port 16 Clear Selection

Name	Type	Role	Port Channel
<input type="checkbox"/> Port 1	Ethernet	Unconfigured	-
<input type="checkbox"/> Port 2	Ethernet	Unconfigured	-
<input type="checkbox"/> Port 3	Ethernet	Unconfigured	-
<input type="checkbox"/> Port 4	Ethernet	Unconfigured	-
<input type="checkbox"/> Port 5	Ethernet	Unconfigured	-
<input type="checkbox"/> Port 6	Ethernet	Unconfigured	-
<input type="checkbox"/> Port 7	Ethernet	Unconfigured	-
<input type="checkbox"/> Port 8	Ethernet	Unconfigured	-
<input type="checkbox"/> Port 9	Ethernet	Unconfigured	-
<input type="checkbox"/> Port 10	Ethernet	Unconfigured	-
<input type="checkbox"/> Port 11	Ethernet	Unconfigured	-
<input type="checkbox"/> Port 12	Ethernet	Unconfigured	-
<input type="checkbox"/> Port 13	Ethernet	Unconfigured	-
<input type="checkbox"/> Port 14	Ethernet	Unconfigured	-
<input type="checkbox"/> Port 15	Ethernet	Ethernet Uplink	-
<input checked="" type="checkbox"/> Port 16	Ethernet	Ethernet Uplink	-

Configure Port

Configuration

Selected Port Port 16

Role
Ethernet Uplink

Admin Speed Auto FEC Auto

Ethernet Network Group
Selected Policy Prod-vlans

Flow Control
[Select Policy](#)

Link Control
[Select Policy](#)

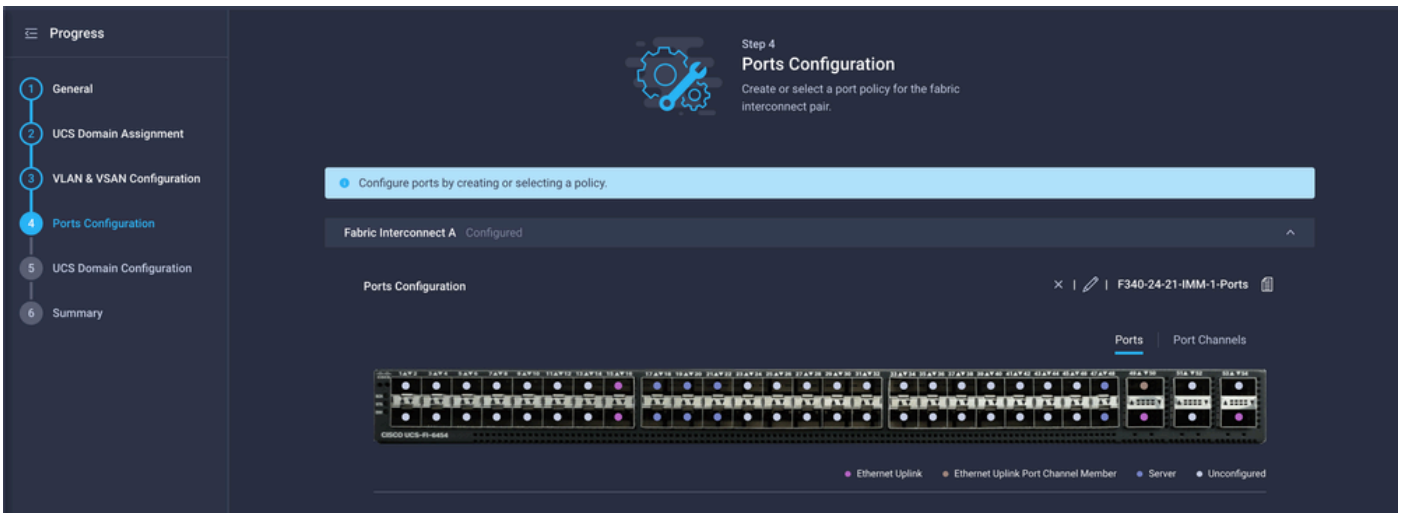
Step 5. Assign the VLAN Policy and the Port Policy to the Domain Profile

Navigate to **Profiles > UCS Domain Profiles** and select the appropriate **Domain Profile**.

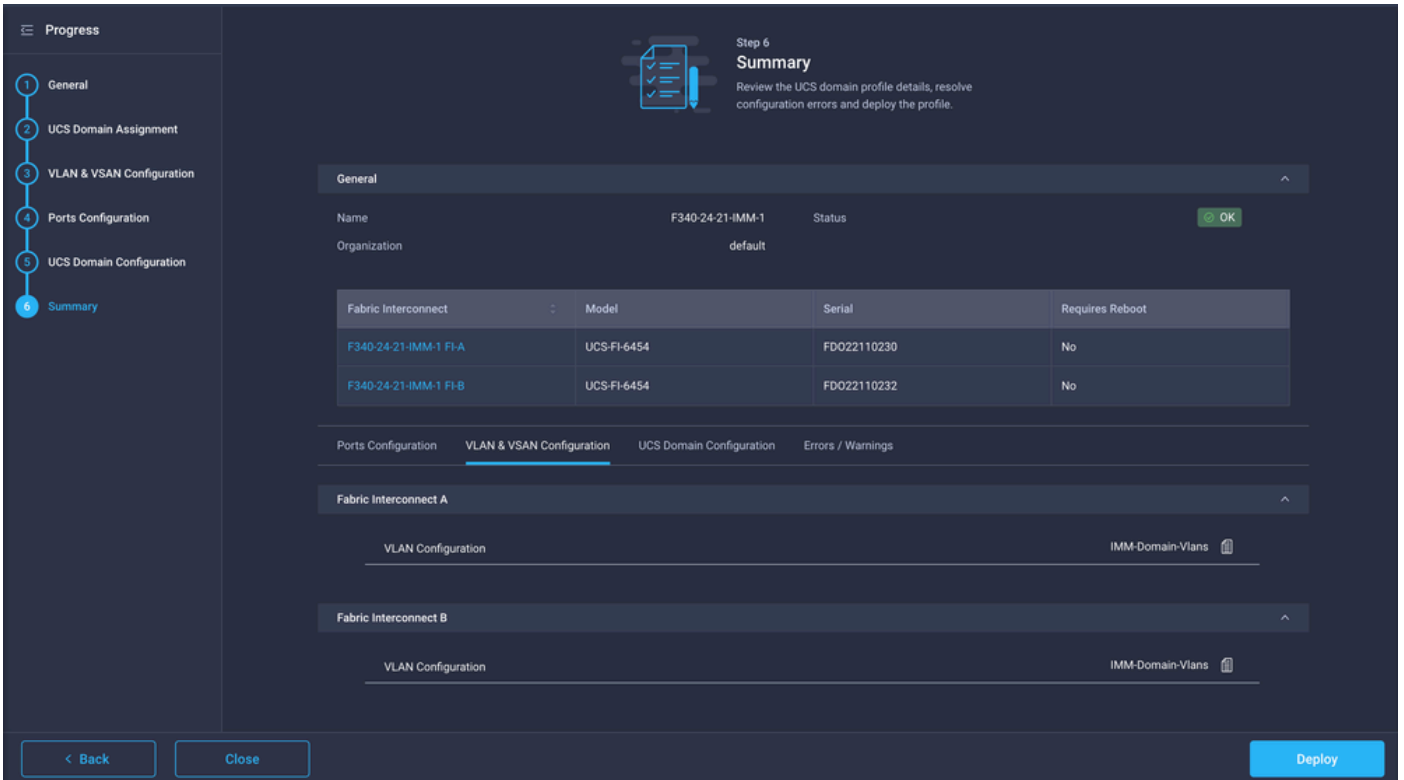
Navigate to the **Ports Configuration** section.



Assign the **Port Policy** created in Step 4. to Fabric Interconnect A and B and proceed to the **Summary** section.



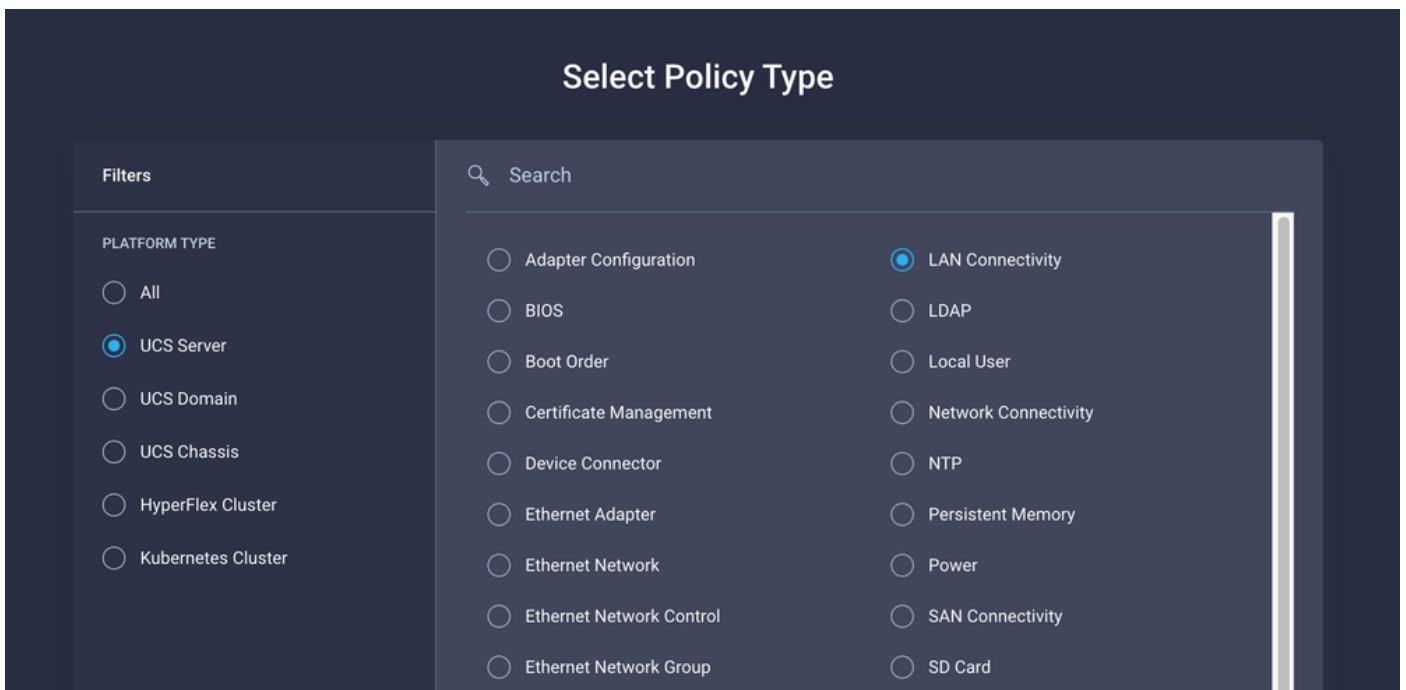
Review the configuration applied to the **Domain Profile** and click **Deploy**.



Step 6. Assign the Ethernet Group Policy to a LAN Connectivity Policy

You can use the LAN connectivity policy that already exists or create a new one.

Navigate to **Policies > Create Policy > Select LAN Connectivity**.



Enter a Name and click **Next**.



Step 1

General

Add a name, description and tag for the policy.

Organization *

default

Name *

IMM-LCP

Target Platform ⓘ



UCS Server (Standalone)



UCS Server (FI-Attached)

Set Tags

Description

<= 1024

Configure the vNICs with the desired settings and include the Ethernet Network group that was created in Step 3. or, you can reuse the group created in Step 2.

Progress

Step 2 Policy Details
Add policy details

1 General
2 Policy Details

Enable Azure Stack Host QoS

IQN

None Pool Static

This option ensures the IQN name is not associated with the policy

vNIC Configuration

Manual vNICs Placement Auto vNICs Placement

For manual placement option you need to specify placement for each vNIC. Learn more at [Help Center](#)

Add vNIC Graphic vNICs Editor

	Na... Edit	Slot ID	Switch ID	PCI Link	PCI Order	Failover	
<input checked="" type="checkbox"/>	vnic0	MLOM	A	0	0	Disabled	...
<input type="checkbox"/>	vnic3	MLOM	A	0	3	Disabled	...

Selected Pool IMM-MAC-POOL | X

Placement

Slot ID * MLOM PCI Link 0 0-1

Switch ID * A

PCI Order 0

Consistent Device Naming (CDN)

Source vNIC Name

Failover

Enabled

Ethernet Network Group Policy *
Selected Policy MGMT-VNIC-167 | X

Ethernet Network Control Policy *
Selected Policy IMM-Netcontrol | X

Ethernet QoS *



Assign the LAN Connectivity policy to a Service Profile and deploy.

Verify

Use this section to confirm that your configuration works properly.

Once the Domain profile has been deployed you can verify the VLANs are assigned to the appropriate Uplinks

Default (auto allow on all Uplinks) configuration:

```
<#root>
```

```
LAB-IMM-B(nx-os)#
```

```
show run interface ethernet 1/15
```

```
!Command: show running-config interface Ethernet1/15
!Running configuration last done at: Wed Mar 9 20:20:55 2022
!Time: Thu Mar 10 14:28:00 2022
version 9.3(5)I42(1g) Bios:version 05.42
interface Ethernet1/15
  description Uplink
  pinning border
```



```
switchport mode trunk
switchport trunk allowed

vlan 1,101-999

no shutdown

LAB-IMM-B(nx-os)#
show run interface ethernet 1/16
```

```
!Command: show running-config interface Ethernet1/16
!Running configuration last done at: Wed Mar 9 20:20:55 2022
!Time: Thu Mar 10 14:28:06 2022
version 9.3(5)I42(1g) Bios:version 05.42
interface Ethernet1/16
  description Uplink
  pinning border
  switchport mode trunk
  switchport trunk allowed

vlan 1,101-999
```

```
no shutdown
```

After the assignment of the DMZ VLANs to port 1/15 and Production Vlans to port 1/16:

```
<#root>
```

```
LAB-IMM-B(nx-os)#
show run interface ethernet 1/15
```

```
!Command: show running-config interface Ethernet1/15
!Running configuration last done at: Thu Mar 10 18:13:38 2022
!Time: Thu Mar 10 18:21:54 2022
version 9.3(5)I42(1g) Bios:version 05.42
interface Ethernet1/15
  description Uplink
  pinning border
  switchport mode trunk
  switchport trunk allowed

vlan 1,20-30
```

```
no shutdown
```

```
LAB-IMM-B(nx-os)#
show run interface ethernet 1/16
```

```
!Command: show running-config interface Ethernet1/16
!Running configuration last done at: Thu Mar 10 18:13:38 2022
!Time: Thu Mar 10 18:21:57 2022
version 9.3(5)I42(1g) Bios:version 05.42
```

```
interface Ethernet1/16
  description Uplink
  pinning border
  switchport mode trunk
  switchport trunk allowed
```

```
vlan 1,101-999
```

```
no shutdown
```

Related Information

- [Domain Profiles in Intersight](#)
- [Server Policies in Intersight](#)
- [Domain Policies in Intersight](#)
- [Troubleshoot IMM Network on UCS Domain with API Explorer and NXOS](#)
- [Technical Support & Documentation - Cisco Systems](#)