

VSANs

- VSANs, on page 1

VSANs

You can configure and manage Virtual SANs (VSANs) from Cisco Nexus Dashboard Fabric Controller. From the menu, choose **Virtual Management > VSANS** to view VSAN information. You can view or configure VSAN for the discovered fabrics, with either **Manageable** or **Manage Continuously** status. For a selected fabric, a VSAN Scope tree is displayed in the left panel.

You can achieve higher security and greater stability in Fibre Channel fabrics by using virtual SANs (VSANs) on Cisco Data Center Switches and Cisco MDS 9000 Series switches. VSANs provide isolation among devices that are physically connected to the same fabric. With VSANs, you can create multiple logical SANs over a common physical infrastructure. Each VSAN can contain up to 239 switches and has an independent address space that allows identical Fibre Channel IDs (FC IDs) to be used simultaneously in different VSANs.

Note Cisco Nexus Dashboard Fabric Controller does not discover, nor display any suspended VSAN.

Note When changing VSAN of the Switch port in Nexus Dashboard Fabric Controller, If the port was associated with Isolated VSAN, then the previous VSAN column will be blank.

For description on all fields that appear on the tabs, refer Field and Descriptions for VSANs, on page 10.

This section includes the following topics:

Information About VSANs

With the introduction of VSANs, the network administrator can build a single topology containing switches, links, and one or more VSANs. Each VSAN in this topology has the same behavior and property of a SAN. A VSAN has the following additional features:

- Multiple VSANs can share the same physical topology.

- The same Fibre Channel IDs (FC IDs) can be assigned to a host in another VSAN, thus increasing VSAN scalability.
- Every instance of a VSAN runs all required protocols such as FSPF, domain manager, and zoning.
- Fabric-related configurations in one VSAN don't affect the associated traffic in another VSAN.
- Events causing traffic disruptions in one VSAN are contained within that VSAN and aren't propagated to other VSANs.

A VSAN is in the operational state if the VSAN is active and at least one port is up. This state indicates that traffic can pass through this VSAN. This state can't be configured.

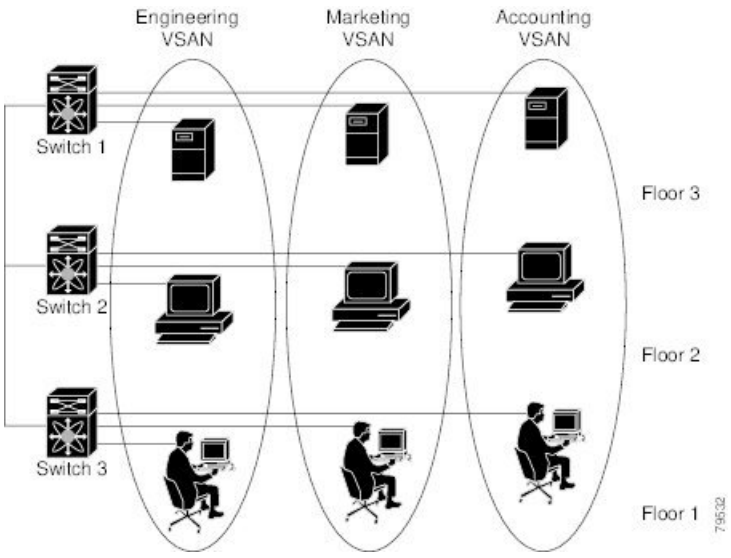
Interoperability enables the products of multiple vendors to come into contact with each other. Fibre Channel standards guide vendors towards common external Fibre Channel interfaces. You can enable FICON in up to eight VSANs.

This section describes VSANs and includes the following topics:

VSAN Topologies

The following figure shows a fabric with three switches, one on each floor. The geographic location of the switches and the attached devices is independent of their segmentation into logical VSANs. No communication between VSANs is possible. Within each VSAN, all members can talk to one another.

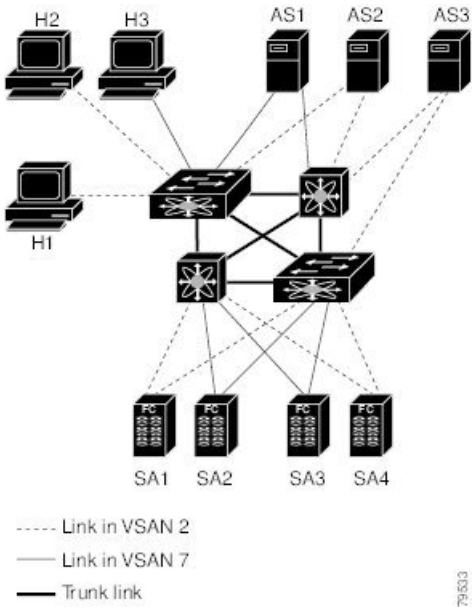
Figure 1: Logical VSAN Segmentation



The following shows a physical Fibre Channel switching infrastructure with two defined VSANs: VSAN 2 (dashed) and VSAN 7 (solid). VSAN 2 includes hosts H1 and H2, application servers AS2 and AS3, and storage arrays SA1 and SA4. VSAN 7 connects H3, AS1, SA2, and SA3.

The four switches in this network are interconnected by trunk links that carry both VSAN 2 and VSAN 7 traffic. The inter-switch topology of both VSAN 2 and VSAN 7 are identical. This isn't a requirement and a network administrator can enable certain VSANs on certain links to create different VSAN topologies.

Figure 2: Example of Two VSANs



Without VSANs, a network administrator would need separate switches and links for separate SANs. By enabling VSANs, the same switches and links may be shared by multiple VSANs. VSANs allow SANs to be built on port granularity instead of switch granularity. The above figure illustrates that a VSAN is a group of hosts or storage devices that communicate with each other using a virtual topology defined on the physical SAN.

The criteria for creating such groups differ based on the VSAN topology:

- VSANs can separate traffic based on the following requirements:
  - Different customers in storage provider data centers
  - Production or test in an enterprise network
  - Low and high security requirements
  - Back up traffic on separate VSANs
  - Replicating data from user traffic
- VSANs can meet the needs of a particular department or application.

VSAN Advantages

VSANs offer the following advantages:

- Traffic isolation—Traffic is contained within VSAN boundaries and devices reside only in one VSAN ensuring absolute separation between user groups, if desired.
- Scalability—VSANs are overlaid on top of a single physical fabric. The ability to create several logical VSAN layers increases the scalability of the SAN.
- Per VSAN fabric services—Replication of fabric services on a per VSAN basis provides increased scalability and availability.

- Redundancy—Several VSANs created on the same physical SAN ensure redundancy. If one VSAN fails, redundant protection (to another VSAN in the same physical SAN) is configured using a backup path between the host and the device.
- Ease of configuration—Users can be added, moved, or changed between VSANs without changing the physical structure of a SAN. Moving a device from one VSAN to another only requires configuration at the port level, not at a physical level.

Up to 256 VSANs can be configured in a switch. Of these, one is a default VSAN (VSAN 1), and another is an isolated VSAN (VSAN 4094). User-specified VSAN IDs range 2–4093.

VSAN Configuration

VSANs have the following attributes:

- VSAN ID—The VSAN ID identifies the VSAN as the default VSAN (VSAN 1), user-defined VSANs (VSAN 2–4093), and the isolated VSAN (VSAN 4094).
- State—The administrative state of a VSAN can be configured to an active (default) or suspended state. Once VSANs are created, they may exist in various conditions or states.
  - The active state of a VSAN indicates that the VSAN is configured and enabled. By enabling a VSAN, you activate the services for that VSAN.
  - The suspended state of a VSAN indicates that the VSAN is configured but not enabled. If a port is configured in this VSAN, it's disabled. Use this state to deactivate a VSAN without losing the VSAN's configuration. All ports in a suspended VSAN are disabled. By suspending a VSAN, you can preconfigure all the VSAN parameters for the whole fabric and activate the VSAN immediately.
- VSAN name—This text string identifies the VSAN for management purposes. The name can be 1–32 characters long and it must be unique across all VSANs. By default, the VSAN name is a concatenation of VSAN and a four-digit string representing the VSAN ID. For example, the default name for VSAN 3 is VSAN0003.



Note A VSAN name must be unique.

- Load balancing attributes—These attributes indicate the use of the source-destination ID (src-dst-id) or the originator exchange OX ID (src-dst-ox-id, the default) for load-balancing path selection.



Note OX ID-based load balancing of IVR traffic from IVR-enabled switches isn't supported on Generation 1 switching modules. OX ID-based load balancing of IVR traffic from a non-IVR MDS 9000 Series switch should work. Generation 2 switching modules support OX ID-based load balancing of IVR traffic from IVR-enabled switches.

- Load-balancing attributes indicate the use of the source-destination ID (src-dst-id) or the originator exchange OX ID (src-dst-ox-id, the default) for load-balancing path selection.

Port VSAN Membership

Port VSAN membership on the switch is assigned on a port-by-port basis. By default, each port belongs to the default VSAN. You can assign VSAN membership to ports using one of two methods:

- Statically—By assigning VSANs to ports
- Dynamically—By assigning VSANs based on the device WWN

  This method is referred to as dynamic port VSAN membership (DPVM).

Types of VSAN

The following are the different types of VSAN:

Default VSAN

The factory settings for switches in the Cisco MDS 9000 Series have only the default VSAN 1 enabled. We recommend that you don't use VSAN 1 as your production environment VSAN. If no VSANs are configured, all devices in the fabric are considered part of the default VSAN. By default, all ports are assigned to the default VSAN.

Note VSAN 1 can't be deleted, but it can be suspended.

Up to 256 VSANs can be configured in a switch. Of these, one is a default VSAN (VSAN 1), and another is an isolated VSAN (VSAN 4094). User-specified VSAN IDs range 2–4093.

Isolated VSAN

VSAN 4094 is an isolated VSAN. All nontrunking ports are transferred to this VSAN when the VSAN to which they belong is deleted. This avoids an implicit transfer of ports to the default VSAN or to another configured VSAN. All ports in the deleted VSAN are isolated (disabled).

Note When you configure a port in VSAN 4094 or move a port to VSAN 4094, that port is immediately isolated.

Caution Don't use an isolated VSAN to configure ports.

Up to 256 VSANs can be configured in a switch. Of these, one is a default VSAN (VSAN 1), and another is an isolated VSAN (VSAN 4094). User-specified VSAN IDs range 2–4093.

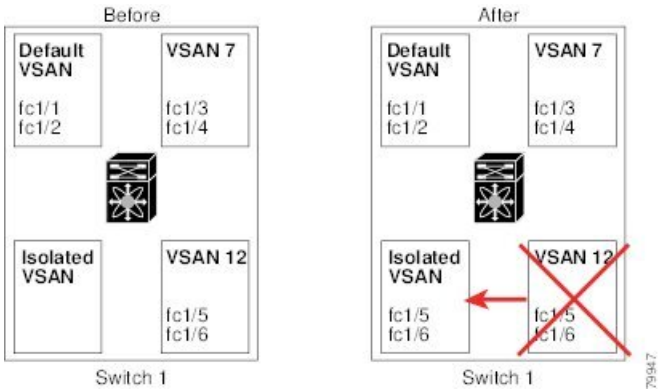
Static VSAN Deletion

When an active VSAN is deleted, all of its attributes are removed from the running configuration. VSAN-related information is maintained by the system software as follows:

- VSAN attributes and port membership details are maintained by the VSAN manager. This feature is affected when you delete a VSAN from the configuration. When a VSAN is deleted, all the ports in that

VSAN are made inactive and the ports are moved to the isolated VSAN. If the same VSAN is recreated, the ports don't automatically get assigned to that VSAN. Reconfigure the port VSAN membership explicitly (see the following figure).

Figure 3: VSAN Port Membership Details



- VSAN-based runtime (name server), zoning, and configuration (static routes) information is removed when the VSAN is deleted.
- Configured VSAN interface information is removed when the VSAN is deleted.

Note The allowed VSAN list isn't affected when a VSAN is deleted.

Any commands for a non-configured VSAN are rejected. For example, if VSAN 10 isn't configured in the system, then a command request to move a port to VSAN 10 is rejected.

Feature Information for Configuring and Managing VSANs

The following table shows the licensing requirements for this feature:

License Description

ENTERPRISE_PKG The enterprise license is required to enable VSAN. For a complete explanation of the licensing scheme, see the Cisco Nexus Dashboard Fabric Controller Licensing Guide.

License	License Description
ENTERPRISE_PKG	The enterprise license is required to enable VSAN. For a complete explanation of the licensing scheme, see the Cisco Nexus Dashboard Fabric Controller Licensing Guide.

Default VSAN Settings

The following table lists the default settings for all configured VSANs.

Parameters	Default
Default VSAN	VSAN 1.
State	Active State
Name	Concatenation of VSAN and a four-digit string representing the VSAN ID. For example, VSAN 3 is VSAN0003.
Load-balancing attribute	OX ID (src-dst-ox-id).

Create VSAN Wizard

VSAN Creation Wizard workflow includes:

- Specify VSAN ID and name.
- Select Switches.
- Specify VSAN attributes.
- Specify VSAN Domain.
- Specify VSAN Members.

Choose **Virtual Management > VSANS**. After you select a Fabric from the drop-down list, click **Create New VSAN** icon. The Welcome screen of the wizard is displayed.

Note Ensure that the VSAN is not already created.

To create and configure VSANs from the Cisco Nexus Dashboard Fabric Controller Web UI, perform the following steps:

Before you begin

You cannot configure any application-specific parameters for a VSAN before creating the VSAN.

Ensure that the VSAN is not already created. Do not create the VSAN in suspended state.

Note The suspended VSANs are not managed.

Procedure

Step 1 In the VSAN ID and Name window, perform the following steps:

a) Ensure that the correct Fabric is against the Fabric field.
b) In the VSAN ID field, select VSAN ID from the drop-down list.

The range is 2–4094. Create the list of VSAN ID in at least one Switch in the Fabric. VSAN ID 4079 is for reserved VSAN.

c) In the VSAN Name field, enter a name for VSAN.

Note
If the field is left blank, the Switch assigns a default name to the VSAN.

d) Click the FICON check box to enable FICON on the switch.
e) Click Next.

Step 2 In the Select Switches screen, click the check box next to the Switch Name, to create the VSAN.

If the switch name is grayed out, it implies that the switch is already part of a VSAN. It may also imply that the switch doesn't have FICON feature enabled, if FICON is checked in the previous step.

Click **Next**.

Step 3 In the Configure VSAN Attributes screen, configure the VSAN attributes.

Note
If you create a VSAN in a suspended state, it doesn't appear on the Cisco Nexus Dashboard Fabric Controller as it doesn't manage suspended VSANs.

a) In Load Balancing, select the load balancing type to be used on the VSAN.

The following types are available:

- Src ID/Dest ID: Based on only source ID (Src_ID) and destination ID (Dest_ID).
- Src ID/Dest ID/Ox ID (default): Originator exchange ID (Ox_ID) is also used for load balancing, in addition to Src_ID and Dest_ID. 0x_ID is an exchange ID assigned by the originator Interconnect Port for an exchange with the target Interconnect Port.

Note
Src ID/Dest ID/0x ID is the default Load Balancing type for non-FICON VSAN and it isn't available for FICON VSAN, Src ID/Dest ID is the default for FICON VSAN.

b) In InterOp, select an interoperability value.

The InterOp value is used to interoperate with different vendor devices. You can choose from one of the following:

- Default: implies that the interoperability is disabled.
- InterOp-1: implies that the VSAN can interoperate with all the Fibre Channel vendor devices.
- InterOp-2: implies that the VSAN can interoperate with specific Fibre Channel vendor devices for basic to advanced functionalities.
- InterOp-3: implies that the VSAN can interoperate with specific Fibre Channel vendor devices for basic to advanced functionalities.
- InterOp-4: implies that the VSAN can interoperate with specific Fibre Channel vendor devices for basic to advanced functionalities.

Note
InterOp isn't supported on FICON VSAN.

c) In Admin State, select the configurable state for this VSAN.

- Active: implies that the VSAN is configured and services for this VSAN is activated.
- Suspended: implies that the VSAN is configured, but the service for this VSAN is deactivated.

  Choose this state to preconfigure all the VSAN parameters for the whole Fabric.

  Note
  Nexus Dashboard Fabric Controller doesn't manage a suspended VSAN, and therefore it does not appear in the VSAN scope.

d) Check the InOrder delivery check box to allow in-order delivery.

When the value of fcInorderDelivery is changed, the value of this object is set to the new value of that object.

e) Check the Add Fabric Binding DB check box if you want to enable the fabric binding for the FICON VSAN.

If the check box is selected, all the peers in the selected switches are added to each switch in the selected list.

f) Check the All Port Prohibited check box if you want to prohibit all the ports for FICON VSAN.

If the check box is selected, the FICON VSAN is created as all Ports prohibited, by default.

g) Click **Next**.

Step 4 In the Configure VSAN Domain screen, configure the static domain IDs for FICON VSAN.

a) Check the Use Static Domain IDs check box to configure the domain ID for the switches in the VSAN.
b) The Available Domain IDs field shows all the available Domain IDs in the Fabric.

Click **Automatically apply available domain IDs** to assign the domain ID for every switch that is selected to be a part of the VSAN.

c) For every switch in the table, enter the domain ID from the list of available Domain IDs.
d) Click **Next**.

Step 5 In the Configure Port Membership screen, for every switch in the VSAN, configure the interfaces as the member of the new VSAN.

Note
Modifying the Port VSAN may affect the I/O of the interface.

Click **Next**.

Step 6 In the Review screen, verify if you have configured the VSAN correctly.

Click **Previous** to navigate to the earlier screen and modify the configuration.

Click **Finish** to confirm and configure the VSAN. The VSAN creation result is displayed at the bottom of the window.

Note
After the VSAN is created, it will take few minutes for the new VSAN to appear in the VSAN scope tree.

Note
If the switch port is associated with Isolated VSAN then the previous VSAN information will be blank.

Delete VSAN

To delete a VSAN and its attributes from the Cisco Nexus Dashboard Fabric Controller Web UI, perform the following steps:

Procedure

Step 1 Choose **Virtual Management > VSANS**.

The **VSANS** window is displayed.

Step 2 From the Select a fabric drop-down list, select the Fabric to which the VSAN is associated.

The VSAN scope tree for the selected Fabric is displayed in the VSANS area.

Step 3 Expand the Fabric and click the delete icon next to the VSAN.

The Delete VSAN screen appears, showing the switches associated with the VSAN.

Note
You can't delete Segmented VSAN.

Step 4 Select the check box of the Switch for which you want to remove the VSAN.

Click **Delete VSAN**.

A confirmation window appears.

Step 5 Click **Confirm** to confirm the deletion or click **Cancel** to close the dialog box without deleting the VSAN.

Note
After the VSAN is deleted, it will take few minutes for the new VSAN to disappear from the VSAN scope tree.

Field and Descriptions for VSANs

The Field and Descriptions for all the tabs that are displayed on **Virtual Management > VSANS** are explained in the following tables.

Switches Tab

This tab displays Switches in the VSAN scope. Click the Switch name to view the summary information of the switch. The following table describes the fields that appear on the Switches tab.

Table 1: Field and Description on Switches Tab

Field	Description
Name	Specifies the name of the switch in the VSAN. Click the name to view the switch summary. Click **Show more Details** to view complete information.

Field	Description
Domain ID	Specifies an insistent domain ID.
VSAN WWN	Specifies the world wide name (WWN) of the VSAN.
Principal WWN	Specifies the world wide name (WWN) of the switch. **Note** For the principal switch, the value is *self*.
Model	Specifies the model name of the switch.
Release	Specifies the NX-OS version on the switch.
Up Time	Specifies the time from which the switch is up.

ISLs Tab

This tab displays information about the ISLs about the switches in the VSAN scope. The following table describes the fields that appear on the ISLs tab. If the VSAN is configured on both the switches across the ISL and if VSAN is not enabled on the ISL, Nexus Dashboard Fabric Controller considers VSAN as segmented. Therefore, add the VSAN to the trunked VSANs across the ISL to clear the warning message. Alternatively, you can ignore this warning message.

Table 2: Field and Description on ISL Tab

Field	Description
VSANs	All VSANs which this ISL runs traffic on.
From Switch	The source switch of the link.
From Interface	The port index of source E_port of the link.
To Switch	The switch on the other end of the link.
To Interface	The port index of destination E_port of the link.
Speed	The speed of this ISL.
Status	The operational status of the link.
Port Channel Members	The member of Port Channel if the ISL is a Port Channel.
Additional Info	Additional information for this ISL, such as, TE/TF/TNP ISL.

Host Ports Tab

This tab displays information about the host ports on the switches in the VSAN scope. The following table describes the fields that appear on the Host Ports tab.

Table 3: Field and Description on Host Ports Tab

Field	Description
Enclosure	The name of the enclosure.
Device Alias	The device alias of this entry.

Field	Description
Port WWN	The assigned PWWN for this host.
Fcid	The FC ID assigned for this host.
Switch Interface	Interface on the switch that is connected with the end device.
Link Status	The operational status of the link.
Vendor	Specifies the name of the vendor.
Serial Number	Specifies the serial number of the enclosure.
Model	Specifies the name of the model.
Firmware	The version of the firmware that is executed by this HBA.
Driver	The version of the driver that is executed by this HBA.
Additional Info	The information list corresponding to this HBA.

Storage Ports Tab

This tab displays information about the storage ports on the switches in the VSAN scope. The following table describes the fields that appear on the Storage Ports tab.

Table 4: Field and Description on Storage Ports Tab

Field	Description
Enclosure	The name of the enclosure.
Device Alias	The device alias of this entry.
Port WWN	The assigned PWWN for this host.
Fcid	The FC ID assigned for this host.
Switch Interface	Interface on the switch that is connected with the end device.
Link Status	The operational status of the link.

Attributes Tab

This tab displays the attributes of all the switches in the VSAN scope. The following table describes the fields that appear on the Attributes tab.

Table 5: Field and Description on Attributes Tab

Field	Description
Edit	Click **Edit** to modify the attributes of the VSAN and to push the same VSAN attributes to the selected switches. If the VSAN is FICON VSAN in any selected switch, the following fields won't appear on the UI, as they can't be modified for the FICON VSAN. • vsanLoadBalancing • InterOp • Inorder Delivery After modify the attributes, you can click **Save** to save changes or **Cancel** to discard.
Switch Name	Displays the name of the switch that is associated with the VSAN.
VSAN Name	Displays the name of the VSAN.
Admin	Specifies if the status of the Admin is either Active or Suspend. • **Active** implies that the VSAN is configured and services for the VSAN is activated. • **Down** implies that the VSAN is configured; however, the service for the VSAN is deactivated. You can use set this state to preconfigure all the VSAN parameters by using the CLI only. **Note** If you suspend a VSAN, it's removed from Cisco Nexus Dashboard Fabric Controller as well.
Oper	The operational state of the VSAN.
MTU	Displays the MTU for the switch.
Load Balancing	Specifies the load-balancing type that is used in the VSAN. The type of load balancing used on this VSAN. • srcId/DestId—use source and destination ID for path selection • srcdId/DestId/Oxld—use source, destination, and exchange IDs
InterOp	The interoperability mode of the local switch on this VSAN. • default • interop-1 • interop-2 • interop-3

Field	Description
Inorder Delivery	The Inorder Delivery guarantee flag of device. If true, then the inorder delivery is guaranteed. If false, it's not guaranteed.
FICON	True if the VSAN is FICON-enabled.

Domain ID Tab

This tab displays information about the VSAN domain and its parameters. The following table describes the fields that appear on the Domain ID tab.

Table 6: Field and Description on Domain ID Tab

Field	Description
Edit	Select a switch and click the Edit icon to modify the Domain ID information for the selected switch.
Switch Name	Specifies the switch name in the VSAN. **Note** NPV switches aren't listed in this column. However, the NPV switches exist in this VSAN fabric.
State	Specifies the state of the Switch.
Enable	Specifies if the Domain ID is enabled or disabled.
Running	Specifies the running domain.
Config	Specifies the configuration.
Config Type	Specifies the usage of the domain ID type—**preferred** or **static**.
Icons	
Total	The number next to Table specifies the entries under this tab.
Refresh Icon	Click the Refresh icon to refresh the entries.

VSAN Membership Tab

This tab displays information about the interfaces on the switches that form the VSAN. The following table describes the fields that appear on the VSAN Membership tab.

Table 7: Field and Description on VSAN Membership Tab

Field	Description
Edit	Select a switch and click the Edit icon to modify Port VSAN Membership for selected VSAN and selected switch. Port VSAN Membership is presented by different types including FC (physical), Port Channel, FCIP, iSCSI, VFC (slot/port), VFC (ID), VFC Channel, VFC FEX, and VFC Breakout, PortChooser is provided for each type to show all existing interfaces on a selected switch for the user to choose from. **Note** If you modify Post VSAN Membership for any operational trunking port or port channel members, a warning appears. Use the Device Manager to change Allowed VSAN List for Trunking Interface.
Switch Name	Name of the switch
Interfaces	FC Ports in VSAN