



# Cisco ACI Multi-Site Orchestrator Release Notes, Release 2.2(4)

This document describes the features, issues, and limitations for the Cisco Application Centric Infrastructure (ACI) Multi-Site Orchestrator software.

Cisco ACI Multi-Site is an architecture that allows you to interconnect separate Cisco APIC cluster domains (fabrics), each representing a different availability zone, all part of the same region. This helps ensure multitenant Layer 2 and Layer 3 network connectivity across sites and extends the policy domain end-to-end across the entire system.

Cisco ACI Multi-Site Orchestrator is the intersite policy manager. It provides single-pane management that enables you to monitor the health of all the interconnected sites. It also allows you to centrally define the intersite policies that can then be pushed to the different Cisco APIC fabrics, which in term deploys them on the physical switches that make up those fabrics. This provides a high degree of control over when and where to deploy those policies.

For more information, see [Related Content](#).

Date	Description
October 21, 2021	Additional open issue CSCvt23491.
December 2, 2020	Additional open issue CSCvw61549.
August 17, 2020	Additional open issue CSCvv35532.
August 10, 2020	Release 2.2(4f) became available. Additional open issue CSCvu21656 open in 2.2(4e) and resolved in 2.2(4f).
July 20, 2020	Additional open issue CSCvu23330.
June 16, 2020	Additional resolved issue CSCvt38422.
May 13, 2020	Removed a known issue CSCvr70198. The issue is resolved in Release 2.2(3j) and all later releases.
April 23, 2019	Release 2.2(4e) became available.

## Contents

- New Software Features
- New Hardware Features
- Changes in Behavior
- Open Issues
- Resolved Issues
- Known Issues

## New Software Features

- Usage Guidelines
- Compatibility
- Scalability
- Related Content
- Legal Information

## New Software Features

Cisco ACI Multi-Site, Release 2.2(3) supports the following new features.

Feature	Description
vzAny Contracts	<p>Cisco ACI Multi-Site Orchestrator now supports grouping of all EPGs within a VRF using the vzAny object, which greatly simplifies contract configurations for a number of use cases.</p> <p>For more information, see the <a href="#">Cisco ACI Multi-Site Configuration Guide</a></p>
Simplified setup for ESX deployments	<p>We now provide an 'mso-setup' script for Multi-Site Orchestrator deployments directly in a VMware ESX server, which simplifies network configurations required to deploy the Orchestrator cluster.</p> <p>For more information, see the <a href="#">Cisco ACI Multi-Site Orchestrator Installation and Upgrade Guide</a></p>
Scale enhancements	<p>Cisco ACI Multi-Site Orchestrator now supports up to 10 templates per schema and 500 EPGs in a Preferred Group. In addition, each site may have up to 500 leaf switches across all PODs in the site and each POD may have up to 400 leaf switches.</p> <p>Note: The <i>Verified Scalability Guide</i> document will be available in the near future</p>

## New Hardware Features

There is no new hardware supported in this release.

The complete list of supported hardware is available in the [Cisco ACI Multi-Site Hardware Requirements Guide](#).

## Changes in Behavior

If you are upgrading to this release, you will see the following changes in behavior:

- Starting with Release 2.2(3j), the template deployment screen has been updated to show additional details about the objects and policies being deployed. You can now see precisely what is being added, removed, or updated for each object and policy on each APIC site.

The following screenshot shows an example of initial Schema deployment where all objects will be created on two APIC sites:

The screenshot shows a 'Deploy To Sites' dialog with a table of objects. The table has columns for Object Type, Name, and two sites (site1 5.0(0.230) and site2 4.2(3.74)). Each cell in the table contains a '+ Created' button. A 'DEPLOY' button is located at the bottom right.

Object Type	Name	site1 5.0(0.230)	site2 4.2(3.74)
EPG	epg1	+ Created	+ Created
	epg2	+ Created	+ Created
Bridge Domain	bd1	+ Created	+ Created
	bd2	+ Created	+ Created
VRF	vrf1	+ Created	+ Created
Filter	filter1	+ Created	+ Created
Contract	c1	+ Created	+ Created

If you then modify one of the objects and re-deploy the schema, the action changes from “Created” to “Modified” and you can mouse over it to display specific changes:

The screenshot shows the 'Deploy To Sites' dialog with a table of objects. The table has columns for Object Type, Name, and two sites (site1 5.0(0.230) and site2 4.2(3.74)). Each cell in the table contains a 'Modified' button. A tooltip titled 'Modified Properties' is shown over the 'Modified' button for the 'epg2' object, displaying the change: 'BdName bd2 -> bd1'.

Object Type	Name	site1 5.0(0.230)	site2 4.2(3.74)
EPG	epg2	Modified	Modified

**Modified Properties**

BdName  
bd2 → bd1

- Additional External EPG subnet flags have been exposed through the Multi-Site Orchestrator GUI.

Prior to Release 2.2(3), **only the following subset of external EPG subnet flags available on each site's APIC** was managed by the Multi-Site Orchestrator:

- Shared Route Control—configurable in the Orchestrator GUI
- Shared Security Import—configurable in the Orchestrator GUI
- Aggregate Shared Routes—configurable in the Orchestrator GUI
- External Subnets for External EPG—not configurable in the GUI, but always implicitly enabled

Starting with Release 2.2(3), all subnet flags available from the APIC can be configured and managed from the Orchestrator:

- Export Route Control
- Import Route Control
- Shared Route Control
- Aggregate Shared Routes
- Aggregate Export (enabled for 0.0.0.0 subnet only)
- Aggregate Import (enabled for 0.0.0.0 subnet only)
- External Subnets for External EPG
- Shared Security Import

When upgrading to this release from Release 2.2(2) or earlier, any subnet flags previously unavailable in the Orchestrator GUI will be imported from the APIC and added to the Orchestrator configuration. All imported flags will retain their state (enabled or disabled) with the exception of External Subnets for External EPG, which will remain enabled post-upgrade. If you had previously explicitly disabled the External Subnets for External EPG flag directly in the APIC (for example, in Cloud APIC use case) you will need to disable it again through the Orchestrator GUI.

When downgrading from this release to Release 2.2(2) or earlier, the subnet flags not available in those releases will be cleared and set to disabled **in the sites' APICs**. You can then manually enable them directly in each site's APIC if necessary.

For additional information on these flags, see the [Cisco ACI Multi-Site Configuration Guide](#).

- When upgrading from a release prior to Release 2.2(1), a GUI lockout timer for repeated failed login attempts is automatically enabled by default and is set to 5 login attempts before a lockout with the lockout duration incremented exponentially every additional failed attempt.
- If you configure read-only user roles in Release 2.1(2) or later and then choose to downgrade your Multi-Site Orchestrator to an earlier version where the read-only roles are not supported:
  - You will need to reconfigure your external authentication servers to the old attribute-value (AV) pair string format. For details, see the "Administrative Operations" chapter in the *Cisco ACI Multi-Site Configuration Guide*.
  - The read-only roles will be removed from all users. This also means that any user that has only the read-only roles will have no roles assigned to them and a Power User or User Manager will need to re-assign them new read-write roles.
- Starting with Release 2.1(2), the 'phone number' field is no longer mandatory when creating a new Multi-Site Orchestrator user. However, because the field was required in prior releases, any user created in Release 2.1(2) or

## Open Issues

later without a phone number provided will be unable to log into the GUI if the Orchestrator is downgraded to Release 2.1(1) or earlier. In this case, a Power User or User Manager will need to provide a phone number for the user.

- If you are upgrading from any release prior to Release 2.1(1), the default password and the minimum password requirements for the Multi-Site Orchestrator GUI have been updated. The default password has been changed from **'We1come!'** to **"We1come2msc!"** and the new password requirements are:

- At least 12 characters
- At least 1 letter
- At least 1 number
- At least 1 special character apart from \* and space

You will be prompted to reset your passwords when you:

- First install Release 2.2(x)
  - Upgrade to Release 2.2(x) from a release prior to Release 2.1(1)
  - Restore the Multi-Site Orchestrator configuration from a backup
- Starting with Release 2.1(1), **Multi-Site Orchestrator encrypts all stored passwords, such as each site's APIC passwords and the external authentication provider passwords.** As a result, if you downgrade to any release prior to Release 2.1(1), you will need to re-enter all the passwords after the Orchestrator downgrade is completed.

To update APIC passwords:

- a. Log in to the Orchestrator after the downgrade.
- b. From the main navigation menu, select Sites.
- c. For each site, edit its properties and re-enter its APIC password.

To update external authentication passwords:

- a. Log in to the Orchestrator after the downgrade.
- b. From the navigation menu, select Admin → Providers.
- c. For each authentication provider, edit its properties and re-enter its password.

## Open Issues

This section lists the resolved issues. Click the bug ID to access the Bug Search tool and see additional information about the issue. The "Fixed In" column of the table specifies the relevant releases.

## Open Issues

Bug ID	Description	Exists in
<a href="#">CSCvu21656</a>	MSO GUI throwing error " BD does not have a L3-MultiCast enabled VRF associated" when associating to VRF defined in different schema.  same config works fine in 2.2(2b), issue is seen in 2.2(4e)	2.2(4e )
<a href="#">CSCvu23330</a>	In multisite environment the instantiation of the service graph fails with fault F1690	2.2(4e ) and later
<a href="#">CSCvt48924</a>	MSO sending Remote Address tty10 to ISE	2.2(4e ) and later
<a href="#">CSCvo84218</a>	When service graphs or devices are created on Cloud APIC by using the API and custom names are specified for AbsTermNodeProv and AbsTermNodeCons, a brownfield import to the Multi-Site Orchestrator will fail.	2.2(4e ) and later
<a href="#">CSCvo20029</a>	Contract is not created between shadow EPG and on-premises EPG when shared service is configured between Tenants.	2.2(4e ) and later
<a href="#">CSCvq58349</a>	shadow of extepg's vrf not getting updated.	2.2(4e ) and later
<a href="#">CSCvn98355</a>	Inter-site shared service between VRF instances across different tenants will not work, unless the tenant is stretched explicitly to the cloud site with the correct provider credentials. That is, there will be no implicit tenant stretch by Multi-Site Orchestrator.	2.2(4e ) and later
<a href="#">CSCvq79052</a>	Updating TEP pool may cause a validation error.	2.2(4e ) and later
<a href="#">CSCvr19577</a>	If a template with empty AP (cloudApp without any cloudEpgs) is defined and it's undeployed, it deletes the cloudApp. If other templates are defined with same AP name and have cloudEpgs, then as a result of cloudApp deletion, all those cloudEpgs defined in other templates are also deleted.	2.2(4e ) and later
<a href="#">CSCvr99291</a>	Unable to take backup from MSO GUI.	2.2(4e ) and later
<a href="#">CSCvs32126</a>	Traffic may stop for EPGs stretched between on-premises and cloud sites.	2.2(4e ) and later
<a href="#">CSCvs31527</a>	Object import from Cloud APIC doesn't show the forward rule info and unable to save new rules.	2.2(4e ) and later
<a href="#">CSCvs99052</a>	Deployment window may show more policies been modified than the actual config changed by the user in the Schema.	2.2(4e ) and later

## Open Issues

<a href="#">CSCvt06351</a>	Deployment window may not show all the service graph related config values that have been modified.	2.2(4e) and later
<a href="#">CSCvt00663</a>	Deployment window may not show all the cloud related config values that have been modified.	2.2(4e) and later
<a href="#">CSCvs22418</a>	Traffic is impacted when changing the VRF associated with BDs referred by PG enabled EPGs that have a global contract between them	2.2(4e) and later
<a href="#">CSCvt39879</a>	Preferred group gets disabled on the APIC VRF when deployed from MSO.	2.2(4e) and later
<a href="#">CSCvt41883</a>	DB cleanup is not happening even after deleting the Tenant.	2.2(4e) and later
<a href="#">CSCvt41911</a>	After brownfield import, the BD subnets are present in site local and not in the common template config	2.2(4e) and later
<a href="#">CSCvt42771</a>	MSO shows the L3Outs of another tenant when associating it with a BD.	2.2(4e) and later
<a href="#">CSCvt44081</a>	In shared services use case, if one VRF has preferred group enabled EPGs and another VRF has vzAny contracts, traffic drop is seen.	2.2(4e) and later
<a href="#">CSCvt47568</a>	Let's say APIC has EPGs with some contract relationships. If this EPG and the relationships are imported into MSO and then the relationship was removed and deployed to APIC, MSO doesn't delete the contract relationship on the APIC.	2.2(4e) and later
<a href="#">CSCvt47581</a>	fvImportExtRoutes flag is created for VRF even though site1 & site3 external-epgs have provider contract.	2.2(4e) and later
<a href="#">CSCvt56139</a>	When you try to upgrade MSO from 2.0(x) to 2.2(4), the upgrade script shows the following errors in the logs:  ERROR site 5e5eff4b120000892d98c2dd of templateSite (schema: 5e688b0c110000480b02b3f6 template: Template1) not found in schema!  ERROR schema not found for schemaId: 5e66c0911200004f2c6e542e  However, the upgrade completes correctly.	2.2(4e) and later
<a href="#">CSCvt89710</a>	If a DHCP policy is associated to two bridge domains in different templates but in the same schema, then if you make a change in the DHCP policy and come to schema, only 1 template becomes deployable, i.e. the deploy button gets enabled.	2.2(4e) and later
<a href="#">CSCvs71068</a>	MSO-owned VRF exists on APIC when the owner Template on MSO is un-deployed.	2.2(4e) and later

## Resolved Issues

<a href="#">CSCvt91895</a>	Schema save fails intermittently when L3Out is in one template and external EPG is in another template.	2.2(4e) and later
<a href="#">CSCvt02480</a>	The REST API call "/api/v1/execute/schema/5e43523f1100007b012b0fcd/template/Template_11?undeploy=all" can fail if the template being deployed has a large object count	2.2(4e) and later
<a href="#">CSCvt71692</a>	If one template contains an application profile with some EPGs or an empty application profile and another another template with same application profile name with more EPGs, if you undeploy the first template then the EPGs in the second template also get undeployed.	2.2(4e) and later
<a href="#">CSCvt15312</a>	Shared service traffic drops from external EPG to EPG in case of EPG provider and L3Out vzAny consumer	2.2(4e) and later
<a href="#">CSCvt11713</a>	Intersite L3Out traffic is impacted because of missing import RT for VPN routes	2.2(4e) and later
<a href="#">CSCvw35532</a>	"External Subnets for External EPG" is removed from L3Out subnets after an MSO template deploy.	2.2(4e) and later
<a href="#">CSCvw61549</a>	Unable to select the site local L3Out for a newly created BD from MSO.	2.2(4e) and later
<a href="#">CSCvt23491</a>	Enhancement to add the ability in MSO to configure multiple DHCP relay polices for a BD.	2.2(4e) and later

## Resolved Issues

This section lists the resolved issues. Click the bug ID to access the Bug Search tool and see additional information about the issue. The "Fixed In" column of the table specifies whether the bug was resolved in the base release or a patch release.



## Resolved Issues

Bug ID	Description	Fixed in
<a href="#">CSCvs77524</a>	Cannot completely import ACI tenant into MSO when L3out uses other tenant VRF.  L3out object option is missing for import.	2.2(4e)
<a href="#">CSCvt14266</a>	When a user opens, saves or deploys a schema, MSO produces a red error message NONE.GET. This prevents a user to apply any configuration changes.	2.2(4e)
<a href="#">CSCvs57670</a>	+ The verification is always successful, even in scenarios when we know it should fail (ex. we delete from the APIC GUI an object created and still configured in the MSC GUI)  + The " Last verified" date doesn't change after triggering the verification	2.2(4e)
<a href="#">CSCvs90027</a>	If the VRF, BD, and EPGs in PG are in different schemas and objects are deployed in order VRF, then BD, then the EPGs, VRF is not enabled for PG.	2.2(4e)
<a href="#">CSCvt16836</a>	When customer deletes a BD from the MSO and deploys the config, the BD gets repopulated in the APIC GUI	2.2(4e)
<a href="#">CSCvt18134</a>	Capturing tech-support doesn't collect msc_install.log and msc_upgrade.log file since mount is not available.	2.2(4e)
<a href="#">CSCvt21657</a>	Stale Shadow EPG/BD present in a site2 from local EPG in Site1.  It might create traffic disruption for a subnets defined in the stale Shadow EPG/BD.	2.2(4e)
<a href="#">CSCvs33590</a>	BDs not part of Schema, but part of VRF that is modified in another Schema suddenly have their Subnet changed from " nd" to " no default-gateway" or vice-versa.	2.2(4e)
<a href="#">CSCvs79493</a>	While setting the user preferences generates the correct HTTP request and response messages to NOT display the "What's New" window on login, the window is still always displayed.	2.2(4e)
<a href="#">CSCvt38457</a>	During MSO upgrade Docker image cleanup sometimes hangs due to stale containers.	2.2(4e)
<a href="#">CSCvt38701</a>	After restoring a backup containing a customer certificate the GUI keeps using the " default" MSO certificate	2.2(4e)
<a href="#">CSCvs69260</a>	There is no capability to capture packet flow.	2.2(4e)
<a href="#">CSCvn71413</a>	When the EPG are stretched to all sites and when EPGs are in preferred group. WE notice that the number of policy objects per site increases due to shadow objects created for PG.	2.2(4e)
<a href="#">CSCvp97388</a>	After migrating an EPG object from Site X to Site Y, the VRF object referenced by the migrated object is not deleted from Site X	2.2(4e)
<a href="#">CSCvq19270</a>	When cloning a template from Tenant 1 to Tenant 2 fails with error " Wrong Objectld (length != 24): "".	2.2(4e)
<a href="#">CSCvq97495</a>	After un-deploying and deleting a template that contains an external EPG, L3out and a VRF (CTX), unable to create and deploy a new template with the same external EPG, L3out and VRF (CTX) names. Following error is seen - " Bad Request: VRF: ctx<VRF name> is already deployed by schema: <schma name> - template: <template name> on site <site name>"	2.2(4e)
<a href="#">CSCvs09024</a>	System status may show all containers and nodes healthy even when a node is down.	2.2(4e)

## Known Issues

<a href="#">CSCvs08458</a>	When one node of the cluster is down, and MSO application activation (upgrade or downgrade) is permitted in the MSO Firmware Management page.	2.2(4e)
<a href="#">CSCvt65036</a>	When a VRF is deployed from MSO to APIC, it is enabling L3Mcast even when L3Mcast flag is not enabled. Disabling the L3Mcast flag on the VRF is not disabling the flag on the APIC.	2.2(4e)
<a href="#">CSCvt38422</a>	The sclass mapping on the site 100 spine switch does not have an sclass entry that maps to the leaked VRF table, causing the traffic to get dropped with drop reason DCI_SCLASS_XLATE_MISS.	2.2(4e)
<a href="#">CSCvu21656</a>	MSO GUI throwing error "BD does not have a L3-MultiCast enabled VRF associated" when associating to VRF defined in different schema.  same config works fine in 2.2(2b), issue is seen in 2.2(4e)	2.2(4f)

## Known Issues

This section lists known behaviors. Click the Bug ID to access the Bug Search Tool and see additional information about the issue. The "Exists In" column of the table specifies the relevant releases.

## Usage Guidelines

Bug ID	Description
CSCvo82001	Unable to download Multi-Site Orchestrator report and debug logs when database and server logs are selected
CSCvo32313	Unicast traffic flow between Remote Leaf Site1 and Remote Leaf in Site2 may be enabled by default. This feature is not officially supported in this release.
CSCvn38255	After downgrading from 2.1(1), preferred group traffic continues to work. You must disable the preferred group feature before downgrading to an earlier release.
CSCvn90706	No validation is available for shared services scenarios
CSCvo59133	The upstream server may time out when enabling audit log streaming
CSCvd59276	<p>For Cisco ACI Multi-Site, Fabric IDs Must be the Same for All Sites, or the Querier IP address Must be Higher on One Site.</p> <p>The Cisco APIC fabric querier functions have a distributed architecture, where each leaf switch acts as a querier, and packets are flooded. A copy is also replicated to the fabric port. There is an Access Control List (ACL) configured on each TOR to drop this query packet coming from the fabric port. If the source MAC address is the fabric MAC address, unique per fabric, then the MAC address is derived from the fabric-id. The fabric ID is configured by users during initial bring up of a pod site.</p> <p>In the Cisco ACI Multi-Site Stretched BD with Layer 2 Broadcast Extension use case, the query packets from each TOR get to the other sites and should be dropped. If the fabric-id is configured differently on the sites, it is not possible to drop them.</p> <p>To avoid this, configure the fabric IDs the same on each site, or the querier IP address on one of the sites should be higher than on the other sites.</p>
CSCvd61787	<p>STP and "Flood in Encapsulation" Option are not Supported with Cisco ACI Multi-Site.</p> <p>In Cisco ACI Multi-Site topologies, regardless of whether EPGs are stretched between sites or localized, STP packets do not reach remote sites. Similarly, the "Flood in Encapsulation" option is not supported across sites. In both cases, packets are encapsulated using an FD VNID (fab-encap) of the access VLAN on the ingress TOR. It is a known issue that there is no capability to translate these IDs on the remote sites.</p>
CSCve40295	<p>Proxy ARP is not supported in Cisco ACI Multi-Site Stretched BD without Flooding use case.</p> <p>Unknown Unicast Flooding and ARP Glean are not supported together in Cisco ACI Multi-Site across sites.</p>
CSCvi61260	If an infra L3Out that is being managed by Cisco ACI Multi-Site is modified locally in a Cisco APIC, Cisco ACI Multi-Site might delete the objects not managed by Cisco ACI Multi-Site in an L3Out.
CSCvp10518	Downgrading From 2.1(1) to 2.0(2) may fail if node runs out of space
CSCvq07769	"Phone Number" field is required in all releases prior to Release 2.2(1). Users with no phone number specified in Release 2.2(1) or later will not be able to log in to the GUI when Orchestrator is downgraded to a an earlier release.

## Usage Guidelines

This section lists usage guidelines for the Cisco ACI Multi-Site software.

- In Cisco ACI Multi-Site topologies, we recommend that First Hop Routing protocols such as HSRP/VRRP are not stretched across sites.
- HTTP requests are redirected to HTTPS and there is no HTTP support globally or per user basis.
- Up to 12 interconnected sites are supported.
- Proxy ARP glean and unknown unicast flooding are not supported together.

Unknown Unicast Flooding and ARP Glean are not supported together in Cisco ACI Multi-Site across sites.

- Flood in encapsulation is not supported for EPGs and Bridge Domains that are extended across ACI fabrics that are part of the same Multi-Site domain. However, flood in encapsulation is fully supported for EPGs or Bridge Domains that are locally defined in ACI fabrics, even if those fabrics may be configured for Multi-Site.
- The leaf and spine nodes that are part of an ACI fabric do not run Spanning Tree Protocol (STP). STP frames originated from external devices can be forwarded across an ACI fabric (both single Pod and Multi-Pod), but are not forwarded across the inter-site network between sites, even if stretching a BD with BUM traffic enabled.
- GOLF L3Outs for each tenant must be dedicated, not shared.

The inter-site L3Out functionality introduced on MSO release 2.2(1) does not apply when deploying GOLF L3Outs. This means that for a given VRF there is still the requirement of deploying at least one GOLF L3Out per site in order to enable north-south communication. An endpoint connected in a site cannot communicate with resources reachable via a GOLF L3Out connection deployed in a different site.

- While you can create the L3Out objects in the Multi-Site Orchestrator GUI, the physical L3Out configuration (logical nodes, logical interfaces, and so on) must be done directly in each site's APIC.
- VMM and physical domains must be configured in the Cisco APIC GUI at the site and will be imported and associated within the Cisco ACI Multi-Site.

Although domains (VMM and physical) must be configured in Cisco APIC, domain associations can be configured in the Cisco APIC or Cisco ACI Multi-Site.

- Some VMM domain options must be configured in the Cisco APIC GUI.

The following VMM domain options must be configured in the Cisco APIC GUI at the site:

- NetFlow/EPG CoS marking in a VMM domain association
- Encapsulation mode for an AVS VMM domain

- Some uSeg EPG attribute options must be configured in the Cisco APIC GUI.

The following uSeg EPG attribute options must be configured in the Cisco APIC GUI at the site:

- Sub-criteria under uSeg attributes
- match-all and match-any criteria under uSeg attributes

- Site IDs must be unique.

In Cisco ACI Multi-Site, site IDs must be unique.

- To change a Cisco APIC fabric ID, you must erase and reconfigure the fabric.

Cisco APIC fabric IDs cannot be changed. To change a Cisco APIC fabric ID, you must erase the fabric configuration and reconfigure it.

However, Cisco ACI Multi-Site supports connecting multiple fabrics with the same fabric ID.

- Caution: When removing a spine switch port from the Cisco ACI Multi-Site infrastructure, perform the following steps:
  - a. Click Sites.
  - b. Click Configure Infra.
  - c. Click the site where the spine switch is located.
  - d. Click the spine switch.
  - e. Click the x on the port details.
  - f. Click Apply.

- Shared services use case: order of importing tenant policies

When deploying a provider site group and a consumer site group for shared services by importing tenant policies, deploy the provider tenant policies before deploying the consumer tenant policies. This enables the relation of the consumer tenant to the provider tenant to be properly formed.

- Caution for shared services use case when importing a tenant and stretching it to other sites

When you import the policies for a consumer tenant and deploy them to multiple sites, including the site where they originated, a new contract is deployed with the same name (different because it is modified by the inter-site relation). To avoid confusion, delete the original contract with the same name on the local site. In the Cisco APIC GUI, the original contract can be distinguished from the contract that is managed by Cisco ACI Multi-Site, because it is not marked with a cloud icon.

- When a contract is established between EPGs in different sites, each EPG and its bridge domain (BD) are mirrored to and appear to be deployed in the other site, while only being actually deployed in its own site. These mirrored objects are known as "shadow" EPGs and BDs.

For example, if one EPG in Site 1 and another EPG in Site 2 have a contract between them, in the Cisco APIC GUI at Site 1 and Site 2, you will see both EPGs. They appear with the same names as the ones that were deployed directly to each site. This is expected behavior and the shadow objects must not be removed.

For more information, see the Schema Management chapter in the [Cisco ACI Multi-Site Configuration Guide](#).

- Inter-site traffic cannot transit sites.

Site traffic cannot transit sites on the way to another site. For example, when Site 1 routes traffic to Site 3, it cannot be forwarded through Site 2.

- The ? icon in Cisco ACI Multi-Site opens the menu for Show Me How modules, which provide step-by-step help through specific configurations.

- If you deviate while in progress of a Show Me How module, you will no longer be able to continue.
- You must have IPv4 enabled to use the Show Me How modules.

- User passwords must meet the following criteria:

- Minimum length is 8 characters
- Maximum length is 64 characters
- Fewer than three consecutive repeated characters

## Compatibility

- At least three of the following character types: lowercase, uppercase, digit, symbol
  - Cannot be easily guessed
  - Cannot be the username or the reverse of the username
  - Cannot be any variation of " cisco" , " isco" , or any permutation of these characters or variants obtained by changing the capitalization of letters therein
- If you are associating a contract with the external EPG, as provider, choose contracts only from the tenant associated with the external EPG. Do not choose contracts from other tenants. If you are associating the contract to the external EPG, as consumer, you can choose any available contract.
  - Policy objects deployed from ACI Multi-Site software should not be modified or deleted from any site-APIC. If any such operation is performed, schemas have to be re-deployed from ACI Multi-Site software.
  - The Rogue Endpoint feature can be used within each site of an ACI Multi-Site deployment to help with misconfigurations of servers that cause an endpoint to move within the site. The Rogue Endpoint feature is not designed for scenarios where the endpoint may move between sites.

## Compatibility

This release supports the hardware listed in the [Cisco ACI Multi-Site Hardware Requirements Guide](#).

Multi-Site Orchestrator releases have been decoupled from the APIC releases. The APIC clusters in each site as well as the Orchestrator itself can now be upgraded independently of each other and run in mixed operation mode. For more information, see the Interoperability Support section in the “Infrastructure Management” chapter of the [Cisco ACI Multi-Site Configuration Guide](#).

## Scalability

For the verified scalability limits, see the [Cisco ACI Verified Scalability Guide](#).

## Related Content

See the [Cisco Application Policy Infrastructure Controller \(APIC\)](#) page for ACI Multi-Site documentation. On that page, you can use the "Choose a topic" and "Choose a document type" fields to narrow down the displayed documentation list and find a desired document.

The documentation includes installation, upgrade, configuration, programming, and troubleshooting guides, technical references, release notes, and knowledge base (KB) articles, and videos. KB articles provide information about a specific use cases or topics. The following tables describe the core Cisco Application Centric Infrastructure Multi-Site documentation.

Document	Description
<a href="#">Cisco ACI Multi-Site Release Notes</a>	This document. Provides release information for the Cisco ACI Multi-Site Orchestrator product.
<a href="#">Cisco ACI Multi-Site Fundamentals Guide</a>	Provides basic concepts and capabilities of the Cisco ACI Multi-Site.
<a href="#">Cisco ACI Multi-Site Hardware Requirements Guide</a>	Provides the hardware requirements and compatibility.
<a href="#">Cisco ACI Multi-Site Installation and Upgrade Guide</a>	Describes how to install Cisco ACI Multi-Site Orchestrator and perform day-0 operations.
<a href="#">Cisco ACI Multi-Site Configuration Guide</a>	Describes Cisco ACI Multi-Site configuration options and procedures.
<a href="#">Cisco ACI Multi-Site REST API Configuration Guide</a>	Describes how to use the Cisco ACI Multi-Site REST APIs.
<a href="#">Cisco ACI Multi-Site Troubleshooting Guide</a>	Provides descriptions of common operations issues and Describes how to troubleshoot common Cisco ACI Multi-Site issues.
<a href="#">Cisco ACI Verified Scalability</a>	Contains the maximum verified scalability limits for Cisco Application Centric Infrastructure (Cisco ACI), including Cisco ACI Multi-Site.
<a href="#">Cisco ACI YouTube channel</a>	Contains videos that demonstrate how to perform specific tasks in the Cisco ACI Multi-Site.

## Documentation Feedback

To provide technical feedback on this document, or to report an error or omission, send your comments to [apic-docfeedback@cisco.com](mailto:apic-docfeedback@cisco.com). We appreciate your feedback.

## Legal Information

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: <http://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)

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

© 2019 Cisco Systems, Inc. All rights reserved.