Cisco ACI Multi-Site Orchestrator Release Notes, Release 3.0(1)

This document describes the features, issues, and deployment guidelines 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 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.
May 14, 2020	Release 3.0(1i) became available.

Contents

New Software Features

This release adds the following new features:

Feature	Description
Support for SR-MPLS handoff	Prior to Cisco ACI Multi-Site Orchestrator release 3.0(1), Multi-Site architecture supported only sites connected via IP handoff, otherwise known as VRF-Lite. Beginning with Cisco ACI Multi-Site release 3.0(1), you can use the Multi-Site Orchestrator to also manage ACI fabrics that are connected via segment routing (SR) Multiprotocol Label Switching (MPLS) handoff. For details about SR-MPLS handoff design, policy model, and implementation, see Cisco APIC Layer 3 Networking Configuration Guide, Release 5.0(x). For MSO SR-MPLS configuration, see Cisco ACI Multi-Site Configuration Guide, Release 3.0(x).
Support for SR-MPLS custom QoS policies	Beginning with Cisco ACI Multi-Site release 3.0(1), you can create custom QoS translation policies for traffic coming into or leaving the ACI fabric via an SR-MPLS interface. For more information, see Cisco ACI Multi-Site Configuration Guide, Release 3.0(x).
Support for multicast filtering	Beginning with Cisco ACI Multi-Site release 3.0(1), you can create custom multicast route map policies to enable source or destination filtering for multicast traffic for all EPGs within a bridge domain. For more information, see Cisco ACI Multi-Site Configuration Guide, Release 3.0(x).
Support for Rendezvous Points (RPs)	Beginning with Cisco ACI Multi-Site release 3.0(1), you can use the Multi-Site Orchestrator GUI to add multicast rendezvous points (RPs) for multicast-enabled VRFs. The RPs can be inside or outside the ACI fabric and you can create custom route map policies if you want to limit the RPs to specific multicast groups only. For more information, see Cisco ACI Multi-Site Configuration Guide, Release 3.0(x).
Support for Transit Gateway (TWG) for Cloud APIC sites in AWS	Beginning with Cisco ACI Multi-Site release 3.0(1), you can use Amazon Web Services (AWS) Transit Gateway with Cisco Cloud APIC to automate connectivity between virtual private clouds (VPCs). For more information, see *Increasing Bandwidth Between VPCs by Using AWS Transit Gateway*.

MSO GUI enhancements	The Multi-Site Orchestrator Graphical User Interface (GUI) has been redesigned for consistency across Cisco ACI products, improved user experience, and simplified configuration workflows.

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(3), 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 *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 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 2.1(x)
  - Upgrade to Release 2.1(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 open issues. Click the bug ID to access the Bug Search Tool and see additional information about the bug. The "Exists In" column of the table specifies the 3.0(1) releases in which the bug exists. A bug might also exist in releases other than the 3.0(1) releases.

Bug ID	Description	Exists in
CSCvt48924	MSO sending Remote Address tty10 to ISE	3.0(1i) and later
CSCvo84218	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.	3.0(1i) and later
CSCvo20029	Contract is not created between shadow EPG and on-premises EPG when shared service is configured between Tenants.	3.0(1i) and later
CSCvq58349	shadow of extepg's vrf not getting updated.	3.0(1i) and later
CSCvn98355	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.	3.0(1i) and later
CSCvr19577	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.	3.0(1i) and later
CSCvr99291	Unable to take backup from MSO GUI.	3.0(1i) and later
CSCvs32126	Traffic may stop for EPGs stretched between on-premises and cloud sites.	3.0(1i) and later
CSCvs99052	Deployment window may show more policies been modified than the actual config changed by the user in the Schema.	3.0(1i) and later
CSCvt06351	Deployment window may not show all the service graph related config values that have been modified.	3.0(1i) and later
CSCvt00663	Deployment window may not show all the cloud related config values that have been modified.	3.0(1i) and later
CSCvs22418	Traffic is impacted when changing the VRF associated with BDs referred by PG enabled EPGs that have a global contract between them	3.0(1i) and later
CSCvt41883	DB cleanup is not happening even after deleting the Tenant.	3.0(1i) and later

CSCvt41911	After brownfield import, the BD subnets are present in site local and not in the common template config	3.0(1i) and later
CSCvt42771	MSO shows the L3Outs of another tenant when associating it with a BD.	3.0(1i) and later
CSCvt44081	In shared services use case, if one VRF has preferred group enabled EPGs and another VRF has vzAny contracts, traffic drop is seen.	3.0(1i) and later
CSCvt47568	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.	3.0(1i) and later
CSCvt47581	fvImportExtRoutes flag is created for VRF even though site1 & site3 external-epgs have provider contract.	3.0(1i) and later
CSCvt56139	When you try to upgrade MSO from 2.0(x) to 3.0(1), 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.	3.0(1i) and later
CSCvs71068	MSO-owned VRF exists on APIC when the owner Template on MSO is un-deployed.	3.0(1i) and later
CSCvt02480	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	3.0(1i) and later
CSCvt71692	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.	3.0(1i) and later
CSCvt15312	Shared service traffic drops from external EPG to EPG in case of EPG provider and L3Out vzAny consumer	3.0(1i) and later
CSCvt11713	Intersite L3Out traffic is impacted because of missing import RT for VPN routes	3.0(1i) and later
CSCvt99784	Traffic between onPrem ExternalEPG (aka InstP) and the cloudEPG is disrupted due to a) the deletion of the shadow InstP created for the cloudEPG on the OnPrem Site and b) the deletion of cloudEPG's shadow VRF on the OnPrem Site.	3.0(1i) and later
CSCvu02398	When BD's subnets are changed, the cloud ExtEpg doesnt get the updated cloud extepselector.	3.0(1i) and later

CSCvt11713	Intersite L3Out traffic is impacted because of missing import RT for VPN routes	3.0(1i) and later
CSCvu15073	APIC rejects the deployment from MSO on a cloud APIC site with error: "Following CtxProfiles are associated with this VRF: <ctxprofile-dn> Delete all the CtxProfiles associated with this VRF, before deleting this VRF"	3.0(1i) and later
CSCvu26874	HTTPs listener configuration for Load Balancer doesn't work from MSO for Azure cloud site and MSO may throw error when trying to save schema with HTTPs listener configuration.	3.0(1i) and later
CSCvu26941	Unable to configure BGP Remote Peer Address when BGP-Label Unicast Source IPv4 address is a /31 mask on a SR-MPLS BL/RL node.	3.0(1i) and later
CSCvv35532	"External Subnets for External EPG" is removed from L3Out subnets after an MSO template deploy.	3.0(1i) and later
CSCvw61549	Unable to select the site local L3Out for a newly created BD from MSO.	3.0(1i) and later
CSCvt23491	Enhancement to add the ability in MSO to configure multiple DHCP relay polices for a BD.	3.0(1i) 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.

Bug ID	Description	Fixed in
CSCvt39879	Preferred group gets disabled on the APIC VRF when deployed from MSO.	3.0(1i) and later
CSCvq79052	Updating TEP pool may cause a validation error.	3.0(1i) and later
CSCvs31527	Object import from Cloud APIC doesn't show the forward rule info and unable to save new rules.	3.0(1i) and later
CSCvt89710	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.	3.0(1i) and later
CSCvt91895	Schema save fails intermittently when L3Out is in one template and external EPG is in another template.	3.0(1i) and later

Known Issues

This section lists known behaviors. Click the Bug ID to access the Bug Search Tool and see additional information about the issue.

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	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. 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. 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. 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.
CSCvd61787	STP and "Flood in Encapsulation" Option are not Supported with Cisco ACI Multi-Site. 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.
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.
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

  — 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 feaure 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 Orchestrator Installation and Upgrade 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
Cisco ACI Multi-Site Release Notes	This document. Provides release information for the Cisco ACI Multi-Site Orchestrator product.
Cisco ACI Multi-Site Fundamentals Guide	Provides basic concepts and capabilities of the Cisco ACI Multi-Site.
Cisco ACI Multi-Site Hardware Requirements Guide	Provides the hardware requirements and compatibility.
Cisco ACI Multi-Site Installation and Upgrade Guide	Describes how to install Cisco ACI Multi-Site Orchestrator and perform day-0 operations.
Cisco ACI Multi-Site Configuration Guide	Describes Cisco ACI Multi-Site configuration options and procedures.
Cisco ACI Multi-Site REST API Configuration Guide	Describes how to use the Cisco ACI Multi-Site REST APIs.
Cisco ACI Multi-Site Troubleshooting Guide	Provides descriptions of common operations issues and Describes how to troubleshoot common Cisco ACI Multi-Site issues.
Cisco ACI Verified Scalability	Contains the maximum verified scalability limits for Cisco Application Centric Infrastructure (Cisco ACI), including Cisco ACI Multi-Site.
Cisco ACI YouTube channel	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. We appreciate your feedback.

Legal Information