

# Cisco Secure Agile Exchange Solution Release Notes, Release 2.3

---

**First Published:** 2021-06-15

## About Cisco SAE

The Cisco® Secure Agile Exchange (SAE) solution enables enterprises to interconnect users to applications quickly and securely by virtualizing the network edge (DMZ) and extending it to colocation centers, the crossroads of Internet traffic. For more information on the SAE solution, see [Cisco Secure Agile Exchange \(SAE\) Solution Guide](#).

Find all the information you need about this SAE release—new features, known behavior, and related information, in this document.



---

**Note** Explore [Content Hub](#), the all new portal that offers an enhanced product documentation experience. Content Hub offers the following features to personalize your content experience.

- Faceted Search to help you find content that is most relevant
  - Customized PDFs
  - Contextual Recommendations
- 

## What's New

- **Mixed SAE Versions Per Site:** Supports mixed SAE release versions per site. This will allow users to take a step-by-step approach for upgrading sites with existing deployments from SAE 2.0.1 to 2.3.0 although SAE is versatile to deploy or modify services on sites with older SAE infrastructure releases.
- **VxLAN Traffic HandOff on External End Point:** Supports VxLAN traffic hand off on external endpoint so that user can now specify VNID. In previous SAE release without this feature, user had to define VLAN ID on external endpoint and if required VxLAN handoff, SAE allocates VNID for it. So, user does not have the option to define VNID in Spine-Leaf infrastructure configuration.



---

**Note** This feature is applicable only in case of Nexus 9000 Spine-Leaf infrastructure configuration.

---

- **Issues Fixed Since SAE 2.2:** The following issues are fixed since SAE 2.2 release:

Bug IDs	Description
<a href="#">CSCvy11974</a>	Clean-up action for service chain is stuck.
<a href="#">CSCvw88287</a>	Custom template utils will allow single iteration or variable.
<a href="#">CSCvx27712</a>	RO will check for enough CPUs when Affinity rules are used.

## Known Issues

The following are known bugs associated with SAE. The table below provides a workaround to resolve them temporarily.

**Table 1: Open Bugs**

Bug ID	Description and Workaround
<a href="#">CSCvw54128</a>	<b>Description:</b> SAE-ACI: Custom-template error when applying it on second Fabric as End-Point Gateway as NIC_1_IP_ADDRESS value is not provided by SAE. This issue could happen when second Fabric-as-End-Point Gateway is deployed with the custom template as same as the deployment of the first Fabric-as-End-Point Gateway.
<a href="#">CSCvw77024</a>	<b>Description:</b> VNFs recover would be failed from a down CSP to a live CSP in CSP non-Gluster mode. This issue could happen when recovering multiple VNFs by using "sae-actions recover-vnf-on-vim ..." request without waiting for the first vnf-recovery to be completed before issuing the second request for the second VNF recovery.
<a href="#">CSCvw76626</a>	<b>Description:</b> Ran out of IP addresses on fabric end of HA Half-Chain within Spine-Leaf or ACI environment. This issue could happen when assigning the CSPs from different clusters in Spine-Leaf or ACI environment to the resource zone(s) under a tenant.
<a href="#">CSCvy49846</a>	<b>Description:</b> Nexus 9000 NED migration in SAE 2.3 would fail in NSO GEO-HA with "Internal Error." message. This issue could happen when migrating Nexus 9000 NED after upgrading the SAE pre-2.3 version to 2.3 in NSO GEO-HA environment. It wouldn't happen in a standalone NSO.

Bug ID	Description and Workaround
<a href="#">CSCvw72086</a>	<b>Description:</b> When deploying a service, sometimes the service deployment would be failed as some of the VNF(s) in the service cannot be deployed by the assigned CSP with “Cannot set interface MAC/vlanid to 02:05:2a:43:4e:66/22 for ifname Eth4-2 vf 3: Resource temporarily unavailable” error message. This issue is caused by the current X710 driver running on the CSP.
<a href="#">CSCvw07383</a>	<b>Description:</b> The first NIC port went down on X710 card after fresh-install or upgrade of the CSP. This issue could happen with CSP 2.8.0 or 2.9.0 within SAE 2.3.
<a href="#">CSCvw72380</a>	<b>Description:</b> Failed to properly create cluster with gluster storage due to slow DNS look up. This issue may happen when storage network feature is enabled.
<a href="#">CSCvy42015</a>	<b>Description:</b> NSO-Info does not display HA Info when a browser refresh is done on SAE GUI page.
<a href="#">CSCvw12259</a>	<b>Description:</b> CSP's gets stuck in repository, when one node is down in cluster (GlusterFS). There is no workaround for it however it is observed that in other CSP GUI the <b>Services</b> tab would still function as expected.

#### Release Notes for Components within SAE 2.3

- [Cisco Cloud Services Platform Release Notes, Release 2.9.0](#)
- [Cisco Elastic Services Controller 5.3 Release Notes](#)
- [SAE Core Function Pack Release 2.3.0 Release Notes](#)

## Related Documentation

- [Cisco Secure Agile Exchange Solution Guide](#)
- [Release Notes Cisco Secure Agile Exchange \(all releases\)](#)
- [Cisco SAE Core Function Pack Installation Guide](#)
- [Cisco SAE Core Function Pack User Guide](#)
- [Cisco Network Services Orchestrator Datasheet](#)
- [Cisco Network Services Orchestrator \(NSO\) Solutions](#)
- [Release Notes for Cisco Elastic Services, Release 4.5](#)
- [Release Notes for Cisco Elastic Services \(all releases\)](#)

- [Cisco Elastic Services Controller User Guides](#)
- [Cisco Elastic Services Controller Install and Upgrade Guide](#)
- [Cisco Cloud Services Platform Release Notes](#)
- [Cisco Cloud Services Platform Datasheet](#)
- [Cisco Cloud Services Platform Configuration Guide](#)
- [Cisco Cloud Services Platform Quick Start Guide](#)
- [Cisco Nexus 9000 Series NX-OS Interfaces Configuration Guide, Release 9.x](#)
- [SAE 1.2 Payloads](#)

#### **Notices and Bulletins**

- [Field Notices](#)
- [Deferral Notices](#)
- [Cisco Bulletins](#)

