# Cisco Secure Agile Exchange Solution Release Notes, Release 2.2

**First Published:** 2021-02-26

## 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

- **Support for Application Centric Integration (ACI) with SAE:** Support has been added for SAE service chain to be orchestrated on an ACI fabric using the DataCenter Core Function Pack (DC-CFP) which manages the APIC (Application Policy Infrastructure Controller).

  **Note**
  1. ACI is more flexible and easily supports VXLAN stretching and overlay on the fabric.
  2. SAE with ACI Multi-Pods will eaasily allow you to extend the VXLAN environment across multiple locations.

- **Live Image Recovery (LIR):** The Live Image Recovery (LIR) consists of Network Service Orchestration (NSO), Elastic Service Controller (ESC) and Cloud Service Platform (CSP) which will allow the recover of images within SAE cluster on GlusterFS enabled Cloud Service Platform (CSP) node. Basically, GlusterFS is a software based distributed file system that combines all the disk storage resources from multiple Cloud Service Platform servers into a single global namespace and supports high availability storage solution.

- **Support for Leaf Switch as End Point GateWay (EPGW):** Support has been added to deploy the Nexus N9K switch as Endpoint Gateway. When this EPGW service will be stitched to another service, it will provide a direct connection between the leaf and first VNF of another SAE service thus minimizing the number of VNFs in a service. To deploy it as a service, the leaf switch which has been already present in the SAE environment will be added as PNF in the infrastructure and it will get deployed with another service.
- **Support to Deploy VNF without External Endpoints:** Support has been added to deploy a VNF service without attaching any external-end-point to it. Now, you can add the external endpoints later to the deployed VNF service. The day0 configuration file of this VNF service will only have the management variables and will not have any variables related to any external-end-points.

  **Note** The naming format for VNF without external-end-points is **{site-name}-{tenant name}-(service name)-{vnf-profile name}-basic**

- **Support for MD5 Hash Name for VIM & VM Name for SAE Service:** While creating the VNF service, if you specify that the service will use MD5 naming technique, a unique md5 hash will be generated with the service path and vnf-profile. The fixed length of the generated md5 hash will be 32 characters. Before this release, the default naming format of a VNF service without md5 hash was **{site-name}-{tenant name}-(service name)-{vnf-profile name}-basic**; depending on your inputs if the character length increases I.e. 72 char; ESC can reject the service and the service can fail. Hence, the md5 hash can be used to eliminate the char restriction of the VNF service name. You can also use the md5 naming to hide the VM name from other neighbors in the network.

  **Note** 1. The naming format of a VNF service with md5 hash will be **{site-name}-{tenant name}-(service name)-{vnf-profile name}-basic{md5-naming}**

  2. Before this release the naming format of a VNF service was 58 character in length however, generated md5 hash will be 32 character in length.

- **Upgraded Support for VNF (CSR, PAFW) Deployment:** This release allows you to upgrade VNFs after they are deployed.
- **Support for Actions to Displays NSD Variable Names:** Support has been added to generate the NSD variable name before a VNF service has been deployed and henceforward the action will not require the deployment of a VNF. The command used to request the NSD variable is **sae-actions nsd variables nsd** *nsd name* **nsd-flavor** *nsd-flavor name* **vnf-profile** *vnf-profile name* which gives the information about the variables used in creating day0/day1 configuration files.
- **Support for Username and Password as Variables:** In this release, the username and password set under devices **authgroup** for the **vnf-config** is available as *$USER* (username), *$CRED* (password) variables in the day0 file of the VNF. You also have an option to select the password to be in a hash format according to the VNF vendor specifications. Currently, this feature is necessary for Palo Alto Firewall day0.

**Note** NSO will provide the username and password values to the variables in ESC to be substituted in the day0 configuration file before VNF process starts.

- **Support for Addition of Day0/Day1 Configurations Under Network-Service Deployment:** Support has been added to allow you to attach separate day0/day1 configuration details to a particular vnf-profile. This will overwrite the details for day0/day1 configuration already stored under the vnf-config.
- **Support Dynamic Day0 Creation:** Before this release, when deploying a VNF from GUI, day0 file was created manually in Command Line Interface (CLI) and referenced it to the VNFD deployment to use it. This feature supports dynamic creation of day0 file as per the requirement and will send the created day0 file to GUI to edit/view the VNF content.

**Note** The limitations added for the day0 creations are as follow:

1. Supports only one VNF in NSD
2. Support has been added for EPGW and HC
3. Supports only Certificate Signing Request (CSR), Cisco Adaptive Security Appliance (ASA) and Palo Alto network.
4. VNFD_DEPL should have the same NSO_IP on the day0 url.

## 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 |
|---|---|
| CSCvw07383 | **Description:** The first port of the four on X710 NIC ports gets down on fresh install or upgrade.<br>**Workaround:** To resolve the issue, you need to open CSP's CIMC GUI.<br>Click on **Host Power tab** > **Power Cycle**, or in the KVM console window, click on **Power tab** > **Power Cycle System** (cold boot). |
| CSCvw66956 | **Description:** CSP service migration fails when VNF image is not present on destination CSP<br>**Workaround:** You have to make sure QCOW2 images are available on all CSPs. Also check QCOW2 images in all CSP's repository from SAE GUI. |

| Bug ID | Description and Workaround |
|---|---|
| CSCvw72086 | **Description:** VNF fails to deploy on MAC due to "vf 3: Resource temporarily unavailable".<br>**Workaround:** Follow these steps to deploy VNF on MAC:<br>• **Step 1:** Identify X710 10GB port and enable SR-IOV on it.<br>• **Step 2:** Create a service (VNF), using the SR-IOV enabled X710 port for a VNIC.<br>• **Step 3:** Deploy the VNF and verify if symptom of issue happens.<br>• **Step 4:** If the deploy fails, delete the deployed failed VNF and try to create and deploy the VNF again. |
| CSCvw72380 | **Description:** Cluster creation with gluster storage fails due to slow DNS look up?<br>**Workaround:** Follow these steps to create cluster with gluster storage:<br>• **Step 1:** Correct the DNS configuration in the /etc/resolv.conf file on the CSP box<br>• **Step 2:** Delete the failed cluster and retry the cluster creation again. |
| CSCvw54128 | **Description:** SAE-ACI: Custom-template error on second Fab-EPGW by NIC_1_IP_ADDRESS, value is not provided.<br>**Workaround:** There are 2 workarounds :<br>• **Step 1:** Deploy EPGW and wait till it is completely in deployed state. Once the EPGW is deployed, apply the custom template.<br>• **Step 2:** Create the custom template with a different name and apply to each EPGW i.e. create multiple copies of the same custom template. The custom template which is used in another service should not be used while deploying the service. |
| CSCvw77024 | **Description:** VNFs recover failed on VIM from a down CSP to another CSP with local storage in non-cluster.<br>**Workaround:** You have to recover the VNFs on the CSP one at a time and wait for the recovery to be done successfully before you recover the next VNF. Follow these steps to recover the VNF:<br>• **Step 1:** Request **sae-actions recover-vnf-on-vim sae-site** *SANJOSE***sae-provider 1 sae-tenant 2 service-chain** *T2_HA1_E2E_***Recovery vnf-profile** *VP_CSR_CS*<br>• **Step 2:** Wait for VNF *VP_CSR_CS* to be completely recovered on a running CSP.<br>• **Step 3:** Request **sae-actions recover-vnf-on-vim sae-site** *SANJOSE***sae-provider 1 sae-tenant 2 service-chain** *T2_HA1_E2E_***Recovery vnf-profile** *VP_CSR_CS*<br>• **Step 4:** Wait for VNF *VP_CSR_PS* to be completely recovered on a running CSP.<br>• **Step 5:** Request **sae-actions recover-vnf-on-vim sae-site** *SANJOSE***sae-provider 1 sae-tenant 2 service-chain** *T2_HA1_E2E_***Recovery vnf-profile** *VP_PAFW_MS* |

# 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