# DevOps Secrets Safe 20.3.1 Release Notes

**September 3, 2020**

**Requirements:**

- DevOps Secrets Safe deployment is only supported using Helm 3.
- DevOps Secrets Safe is currently supported on Kubernetes up to version 1.17.
- DevOps Secrets Safe CLI (ssrun) is supported on any standard Unix / Linux environment that has python 3.5 or higher and pip3 installed.
- The MD5 signature is: 29cc8e76988ee91c2d2f1aead04ee88d.
- The SHA-1 signature is: caa2da545aa6f677fb1a8f8f85d001f2bd5446e5.

**Updates:**

- Create users for Kubernetes ServiceAccounts
  - The DSS user creation endpoint now allows specification of a Kubernetes ServiceAccount name for user creation.
- Kubernetes integration image name
  - Image name used for secret retrieval is now "beyondtrust/secrets-agent".
- Kubernetes Integration retrieves all secrets under a scope
  - The secrets-agent Kubernetes integration container can be used to retrieve all secrets under a target scope and unpack the contents of those secrets into a directory.
- Configure Kubernetes identity provider without input file
  - The Kubernetes Identity Provider for DSS, when targeting the cluster that DSS is running on, can be configured without any input file from the CLI, using **ssrun identity create -n kubernetes**.

**Changes:**

- Kubernetes integration image name
  - Image name used for secret retrieval is now "beyondtrust/secrets-agent".
- Kubernetes integration cluster RBAC
  - Pre-creation of DSS principals for Kubernetes ServiceAccounts requires additional permissions for DSS on the target Kubernetes cluster. These permissions are documented in the Kubernetes integration guide.
- Refresh tokens in request body
  - DSS refresh tokens for authentication are transmitted in the request body rather than as query parameters.