

# Secrets Stores API 参考

---

Barbican提供API来管理部署中可用的秘密商店。这些API可以列出可用的秘密商店，管理项目级别的秘密商店映射。Barbican提供了两种类型的秘密商店：一种是默认用于所有项目的全局秘密商店，另一种项目首先秘密商店，用于储存本项目新创建的机密。关于另一个多存储后端支持的介绍，详见[Using Multiple Secret Store Plugins](#)。本文主要集中于Barbican **/v1/secret-stores** REST API。

如果在服务端配置中未开启多机密存储后端支持，那么以下所有的API都将返回资源未找到（404）错误。错误信息文本将突出显示配置中未启用支持。

## GET /v1/secret-stores

---

项目管理员可以请求列出所有可用秘密商店后端。响应信息包括Barbican部署时支持的所有秘密商店。如果多存储后端支持不可用，则返回资源未找到（404）错误。

### 请求/响应

#### Request:

```
GET /secret-stores
```

#### Headers:

```
X-Auth-Token: "f9cf2d480ba3485f85bdb9d07a4959f1"
Accept: application/json
```

#### Response:

```
HTTP/1.1 200 OK
```

```
Content-Type: application/json
```

```
{
  "secret_stores": [
    {
      "status": "ACTIVE",
      "updated": "2016-08-22T23:46:45.114283",
      "name": "PKCS11 HSM",
      "created": "2016-08-22T23:46:45.114283",
      "secret_store_ref": "http://localhost:9311/v1/secret-
stores/4d27b7a7-b82f-491d-88c0-746bd67dad8",
      "global_default": True,
      "crypto_plugin": "p11_crypto",
      "secret_store_plugin": "store_crypto"
    },
    {
      "status": "ACTIVE",
      "updated": "2016-08-22T23:46:45.124554",
      "name": "KMIP HSM",
      "created": "2016-08-22T23:46:45.124554",
      "secret_store_ref": "http://localhost:9311/v1/secret-
stores/93869b0f-60eb-4830-adb9-e2f7154a080b",

```

```
    "global_default": False,
    "crypto_plugin": None,
    "secret_store_plugin": "kmip_plugin"
  },
  {
    "status": "ACTIVE",
    "updated": "2016-08-22T23:46:45.127866",
    "name": "Software Only Crypto",
    "created": "2016-08-22T23:46:45.127866",
    "secret_store_ref": "http://localhost:9311/v1/secret-
stores/0da45858-9420-42fe-a269-011f5f35deaa",
    "global_default": False,
    "crypto_plugin": "simple_crypto",
    "secret_store_plugin": "store_crypto"
  }
}
```

## 响应属性

名称	类型	说明
secret_stores	list	一组机密存储的引用列表
name	string	由“+”分隔的存储和加密插件
secret_store_ref	string	特定机密存储的URL引用

## HTTP状态码

code	说明
200	成功
401	无效的X-Auth-Token或者此token无权访问该资源
403	访问被拒绝。用户已经通过验证，但是无权执行此操作。
404	未找到。未启用多机密后端支持时触发

## GET /v1/secret-stores/{secret\_store\_id}

项目管理员（拥有admin角色的用户）可以通过id来获取机密存储的详细信息。返回的响应将会高亮显示该机密存储是否已被配置为全局默认值。

## 请求/响应

Request:

```
GET /secret-stores/93869b0f-60eb-4830-adb9-e2f7154a080b
Headers:
X-Auth-Token: "f9cf2d480ba3485f85bdb9d07a4959f1"
```

```
Accept: application/json
```

Response:

```
HTTP/1.1 200 OK
```

```
Content-Type: application/json
```

```
{
  "status": "ACTIVE",
  "updated": "2016-08-22T23:46:45.124554",
  "name": "KMIP HSM",
  "created": "2016-08-22T23:46:45.124554",
  "secret_store_ref": "http://localhost:9311/v1/secret-
stores/93869b0f-60eb-4830-adb9-e2f7154a080b",
  "global_default": False,
  "crypto_plugin": None,
  "secret_store_plugin": "kmip_plugin"
}
```

## 响应属性

名称	类型	说明
name	string	由“+”分隔的存储和加密插件
global_default	boolean	标识该机密存储是否是默认的全局机密存储
status	list	机密存储的状态
updated	time	最近一次更新时间
created	time	最初创建时间
secret_store_ref	string	特定机密存储的URL引用

## HTTP状态码

code	说明
200	成功
401	无效的X-Auth-Token或者此token无权访问该资源
403	访问被拒绝。用户已经通过验证，但是无权执行此操作。
404	未找到。未启用多机密后端支持时触发

## GET /v1/secret\_stores/preferred

若事先已经设置了首选项，项目管理员（拥有admin角色的用户）可以请求首选机密存储的引用。当项目的首选机密存储设置成功，将使用此存储后端存储新的项目机密。如果多存储后端支持不可用，则返回资源未找到（404）错误。

## 请求/响应

### Request:

GET /v1/secret-stores/preferred

#### Headers:

X-Auth-Token: "f9cf2d480ba3485f85bdb9d07a4959f1"

Accept: application/json

### Response:

HTTP/1.1 200 OK

Content-Type: application/json

```
{
  "status": "ACTIVE",
  "updated": "2016-08-22T23:46:45.114283",
  "name": "PKCS11 HSM",
  "created": "2016-08-22T23:46:45.114283",
  "secret_store_ref": "http://localhost:9311/v1/secret-stores/4d27b7a7-
b82f-491d-88c0-746bd67dad8",
  "global_default": True,
  "crypto_plugin": "p11_crypto",
  "secret_store_plugin": "store_crypto"
}
```

## 响应属性

名称	类型	说明
secret_store_ref	string	特定机密存储的URL引用

## HTTP状态码

code	说明
200	成功
401	无效的X-Auth-Token或者此token无权访问该资源
403	访问被拒绝。用户已经通过验证，但是无权执行此操作。
404	未找到。当未设置首选机密存储或未启用多机密后端支持时触发

## POST /v1/secret-stores/{secret\_store\_id}/preferred

项目管理员可以为他的项目设置一个首选存储后端。此时，该项目下的任何新机密都将使用此插件进行存储和访问。已存储的机密不受影响，因为机密存储时就已已经获取了存储插件的信息。如果多存储后端支持不可

用，则返回资源未找到（404）错误。

## 请求/响应

### Request:

```
POST /v1/secret-stores/7776adb8-e865-413c-8ccc-4f09c3fe0213/preferred
```

### Headers:

```
X-Auth-Token: "f9cf2d480ba3485f85bdb9d07a4959f1"
```

### Response:

```
HTTP/1.1 204 No Content
```

## HTTP状态码

code	说明
200	成功
401	无效的X-Auth-Token或者此token无权访问该资源
403	访问被拒绝。用户已经通过验证，但是无权执行此操作。
404	请求实例未找到或未启用多机密后端支持时触发

## DELETE /v1/secret-stores/{secret\_store\_id}/preferred

项目管理员可以移除设置中的首选机密存储。如果多存储后端支持不可用，则返回资源未找到（404）错误。

## 请求/响应

### Request:

```
DELETE /v1/secret-stores/7776adb8-e865-413c-8ccc-4f09c3fe0213/preferred
```

### Headers:

```
X-Auth-Token: "f9cf2d480ba3485f85bdb9d07a4959f1"
```

### Response:

```
HTTP/1.1 204 No Content
```

## HTTP状态码

code	说明
200	成功

code	说明
401	无效的X-Auth-Token或者此token无权访问该资源
403	访问被拒绝。用户已经通过验证，但是无权执行此操作。
404	请求实例未找到或未启用多机密后端支持时触发

## GET /v1/secret-stores/global-default

项目或服务管理员可以骑牛部署是设置的默认存储后端的引用。

### 请求/响应

Request:

```
GET /v1/secret-stores/global-default
```

Headers:

```
X-Auth-Token: "f9cf2d480ba3485f85bdb9d07a4959f1"
```

```
Accept: application/json
```

Response:

```
HTTP/1.1 200 OK
```

```
Content-Type: application/json
```

```
{
  "status": "ACTIVE",
  "updated": "2016-08-22T23:46:45.114283",
  "name": "PKCS11 HSM",
  "created": "2016-08-22T23:46:45.114283",
  "secret_store_ref": "http://localhost:9311/v1/secret-stores/4d27b7a7-
b82f-491d-88c0-746bd67dad8",
  "global_default": True,
  "crypto_plugin": "p11_crypto",
  "secret_store_plugin": "store_crypto"
}
```

### 响应属性

名称	类型	说明
secret_store_ref	string	特定机密存储的URL引用

### HTTP状态码

code	说明
------	----

code	说明
200	成功
401	无效的X-Auth-Token或者此token无权访问该资源
403	访问被拒绝。用户已经通过验证，但是无权执行此操作。
404	请求实例未找到或未启用多机密后端支持时触发