BeyondTrust

BeyondInsight and Password Safe 24.1 API Guide

TC:5/6/2024

Table of Contents

BeyondInsight and Password Safe API Overview

This document specifies the Representational State Transfer (REST) compliant Application Programmer Interface (API) over HTTPS for BeyondInsight and Password Safe. It is a way to integrate a portion of the BeyondInsight and Password Safe functionality into your own applications.

Using the REST API makes it easier for users to build customized solutions for their specific needs while ensuring secure data transmission. The API provides a set of predefined operations, or endpoints, that can be accessed using HTTP Requests, including GET requests to retrieve data, POST requests to create new data, PUT requests to update existing data, and DELETE requests to remove data.

This resource is intended for readers with knowledge of HTTPS request and response processing, web development, and JSON notation.

For more information about enabling API Access, please see the following:

- *BeyondInsight User Guide at https://www.beyondtrust.com/docs/beyondinsight-password-safe/bi/user/index.htm*
- *Password Safe Admin Guide at https://www.beyondtrust.com/docs/beyondinsight-password-safe/ps/admin/index.htm*

Usage

API Key

The API key is a cryptographically strong random sequence of numbers hashed into a 128-character string. It is encrypted and stored internally using AES 256 encryption. Any language with a Representational State Transfer (REST) compliant interface can access the API with the API key and RunAs in the authorization header.

> ***Note:*** *Some environments may still use an old-style API key, which is a formatted Globally Unique Identifier (GUID). Rotating the API Key produces the new-style API key described above.*

Session State

Session state is maintained between API calls. The method is dependent on the scripting language. Initiate a session using API **POST Auth/SignAppIn** and always call **POST Auth/Signout** when you are done.

Base Endpoint

The following base endpoint is used throughout this document. For on-premises instances, **the-server** is a placeholder and should be replaced with the server name in your environment.

```
<base> = https://the-server/BeyondTrust/api/public/v3
```

For cloud instances, **the-cloud-instance-url** is a placeholder and should be replaced with the cloud instance URL in your environment.

```
<base> = https://the-cloud-instance-url/BeyondTrust/api/public/v3
```

SSL is required to use the Password Safe Public API.

Authorization Header

Use the web request authorization header to communicate the API application key, the **RunAs** username, and the user password:

- **key:** The API key configured in BeyondInsight for your application.
- **runas:** The username of a BeyondInsight user that has been granted permission to use the API key.
- **pwd:** The **RunAs** user password surrounded by square brackets (optional; required only if the **User Password** is required on the application API registration).

```
Authorization=PS-Auth key=c479a66f…c9484d; runas=doe-main\johndoe; pwd=[un1qu3];
```

> ***Note:*** *The API keys in the examples have been shortened for brevity. A domain user is being used. When using a domain user, depending on the programming or scripting tool used, you may need to escape the backslash (\) character between the domain name and username.*

Two-Factor Authentication

Depending on how the two-factor server is configured, a programmatic two-factor challenge is sometimes required.

No Challenge

If the two-factor server is configured to authenticate through a push or mobile two-factor challenge, a challenge response is often not required. The first call to **POST Auth/SignAppIn** logs the user in, as long as the authentication request to the two-factor server does not time out.

Challenge

When a two-factor challenge is configured, two calls to **POST Auth/SignAppIn** are required and session state must be maintained between these two calls to validate the two-factor challenge.

The initial call to POST Auth/SignAppIn results in a *401 Unauthorized response* which contains a header WWW-Authenticate-2FA containing the prompt from the authentication service. The prompt can be used to prompt the user for the challenge answer.

> ***Note:*** *If the WWW-Authenticate-2FA header is not present, a two-factor authentication challenge has not been configured for the user.*

When the challenge answer has been received from the user, **POST Auth/SignAppIn** is called again with the challenge answer in the authorization header, similar to the other authorization parameters:

- **challenge:** The answer to the two-factor challenge.

```
Authorization=PS-Auth key=c479a66f…c9484d; runas=doe-main\johndoe; pwd=[un1qu3];
challenge=543687;
```

> ***Note:*** *The challenge answer is only required on the second call to **POST Auth/SignAppIn** and not on subsequent requests.*

OAuth Public API Authentication

The OAuth sign-in method uses the OAuth client credential flow. The client credentials grant type is used by clients to obtain an access token outside of the context of a user.

Only users with user type **Application**, who are associated to an **API Access Policy** API registration in BeyondInsight, can use this authentication method.

> ***Note:*** *Impersonation for the OAuth client credential flow is different than API key. Instead of providing the **RunAs** user as part of the Authorization header you provide the RunAs user using a new **RunAs** header. You can only impersonate users who are in the same group as the application user.*

> ***Note:*** *Setting up an OAuth authentication method requires the following steps:*
> - *Create an API Registration using the API Access Policy type*
> - *Create an application user*
> - *Assign your access policy to the user*
> - *Record their client ID and secret for later use*
> - *Assign user to a group with necessary permissions*

> *For more information, please see OAuth 2.0 Client Credentials Grant at https://oauth.net/2/grant-types/client-credentials.*

Use Certificates with APIs

When **Client certificate required** is enabled on API authentication, the following items are required to authenticate via API:

- Client certificate must be present on the calling machine/instance.
- Client certificate must be trusted by the appliance/Instance.
- Client certificate must be included in script when calling Password Safe API.

For cloud certificate authentication, the client certificate must be signed by a well-known CA for cloud instance to trust it and allow authentication.

> ***Tip:*** *The client cert can be downloaded from the Password Safe appliance/Instance in the* ***Configuration > System > Downloads*** *menu.*
>
> *For examples of utilizing a client cert in your API script, refer to the default scripts in the resource kit for your relevant version.*

Request Body

For Password Safe API Endpoints, some request bodies have multiple versions available. The request body versions allow for different sets of data to be sent to a API endpoint dependent on what needs to be accomplished by the request. Each request body version is outlined on its relevant endpoint and these body versions are only relevant to their listed URI.

When using a request body, if no version is specified in the URI, the default listed version is used (typically v3.0). To use a specific version, the version must be included in the URI.

> ***Example:*** *https://server/BeyondTrust/api/public/v3.1/endpoint*

Common Response Codes

Below are response codes common to all APIs. Custom responses are detailed in the individual endpoints.

- 200 – Request successful.
- 204 – Request successful. No content in body.

- 400 – Bad Request – Validation failure, missing request body, or string values exceed the maximum length. Reason in response body.
- 401 – Unauthorized – User is not authenticated. Typical reasons include:
    - An invalid product license was detected.
    - The request headers were not set properly.
    - The server could not verify the validity of the request (due to one or more API factors).
    - The user session has expired.
    - The API key has been rotated but has not been updated in the calling script or application.

Tip: *When you encounter a 401 error due to factor validation failure, a User Audit entry is created in BeyondInsight and an email is sent to the administrator detailing the reason. Look here first for the reason why authorization failed.*

- 403: – Access forbidden. User does not have the appropriate role or permission.

Tip: *A 403 can also occur when SSL trust cannot be established.*

- 404 – Object not found where expected. Reason in response body.
- 500 – Unexpected server error occurred. Please contact the developers.

Examples

Example: *C#*

Create and reuse a persistent connection using the System.Net.Http.HttpClient class.

```
HttpClient client = new HttpClient();
client.DefaultRequestHeaders.Add("Authorization",
"PS-Auth key= c479a66f…c9484d; runas=doe-main\\johndoe;");

string json = Newtonsoft.Json.JsonConvert.SerializeObject(null);
System.Net.Http.StringContent content = new StringContent(json);
content.Headers.ContentType = new System.Net.Http.Headers.MediaTypeHeaderValue
("application/json");

HttpResponseMessage signInResponse = client.PostAsync("<base>/Auth/SignAppin",
content).Result;
```

Subsequent calls:

```
HttpResponseMessage getResponse = client.GetAsync("<base>/ManagedAccounts").Result;
```

User Password Factor Enabled (header example only)

```
HttpClient client = new HttpClient();
client.DefaultRequestHeaders.Add("Authorization",
"PS-Auth key= c479a66f…c9484d; runas=doe-main\\johndoe; pwd=[un1qu3];");
```

Example: *Powershell*

Powershell internally creates a session variable to use for each subsequent call; Invoke-RestMethod CmdLet options -SessionVariable and -WebSession respectively. In the below example, the variable is named "session" and has script-level scope.

```
$headers = @{ Authorization="PS-Auth key=c479a66f…c9484d; runas=doe-main\\johndoe;"; };
$uri = "<base>/Auth/SignAppin";
$signinResult = Invoke-RestMethod -Uri $uri -Method POST -Headers $headers -
SessionVariable script:session;
```

Subsequent calls:

```
$uri = "<base>/ManagedAccounts";
$accounts = Invoke-RestMethod -Uri $uri -Method GET -WebSession $script:session -Headers
$headers;
```

Example: *Java*

Create and reuse a persistent connection using the java.net.HttpURLConnection class.

```
URL baseURL = new URL("HTTPS", "the-server", 443, "/BeyondTrust/api/public/v3/");
URL url = new URL(baseURL, "Auth/SignAppIn");
HttpURLConnection conn = (HttpURLConnection)url.openConnection();
conn.setRequestProperty("Authorization","PS-Auth key=c479a66f…c9484d; runas=doe-
main\\johndoe;");
```

Example: *Ruby*

Using the rest-client gem, carry over the ASP.NET_SessionId header.

```
samp_key = 'PS-Auth key= c479a66f…c9484d; runas=doe-main\\johndoe;'
result = RestClient::Request.execute(method: :post, url: '<base>/Auth/SignAppin',
:headers => {'Authorization' => samp_key} )
session_id = result.cookies["ASP.NET_SessionId"]
```

Subsequent calls:

```
result = RestClient::Request.execute(method: :get, url: '<base>/ManagedAccounts',
:headers=>{'Authorization' => samp_key, :cookies => {'ASP.NET_SessionId' => session_id}}
)
```

Example: *Python*

Create and reuse a persistent connection using the requests module.

```
header = {'Authorization': 'PS-Auth key=c479a66f…c9484d; runas=doe-main\\johndoe;'}
session = requests.Session()
session.headers.update(header)
response = session.post('<base>/Auth/SignAppin')
```

Subsequent calls:

```
accounts = session.get('<base>/ManagedAccounts')
```

Example: *Bash*

Using curl, option ***–c*** *stores authentication information for subsequent requests and* ***–b*** *uses it in subsequent API calls.*

```
curl -i -c apiToken -X POST https:<base>/Auth/SignAppin -H "Content-Type:
application/json" -H "Authorization: PS-Auth key=c479a66f…c9484d; runas=doe-
main\\johndoe;" -d ""
```

Subsequent calls:

```
curl -i -b apiToken -X GET https:<base>/ManagedAccounts
```

Workflow

There are some loose dependencies between the APIs. A typical sequence is to list accounts or find an account, request a password, retrieve that password (once approved), and then release the password.

Create and Manage an Asset, Create User Group, Assign Roles

Case: Create and manage an asset, create a managed account, create a managed account quick rule, create/provision an LDAP/AD/BeyondInsight user group, grant **Read** access to new Smart Rule with requester role and access policy.

- **POST <base>/Auth/SignAppin**
- **POST <base>/Workgroups/{ID}/Assets**
- **POST <base>/Assets/{assetId}/ManagedSystems**
- **POST <base>/ManagedSystems/{managedSystemId}/ManagedAccounts**
- **POST <base>/QuickRules**
- **POST <base>/UserGroups**
- **POST <base>/UserGroups/{userGroupId}/SmartRules/{smartRuleId}/Roles**
- **POST <base>/Auth/Signout**

Retrieve a Password

Case: request, retrieve, and check in a password for a managed account:

- **POST <base>/Auth/SignAppin**
- **GET <base>/ManagedAccounts** OR **GET <base>/ManagedAccounts?systemName={systemName}&accountName={accountName}**
- **POST <base>/Requests**
- **GET <base>/Credentials/{requestId}**
- **PUT <base>/Requests/{requestId}/Checkin**
- **POST <base>/Auth/Signout**

Create a Session

Case: request a session, create a session, and check in the request for a managed account:

- **POST <base>/Auth/SignAppin**
- **GET <base>/ManagedAccounts** OR **GET <base>/ManagedAccounts?systemName={systemName}&accountName={accountName}**
- **POST <base>/Requests (AccessType="RDP" or AccessType="SSH" or AccessType="App")**
- **POST <base>/Requests/{requestId}/Sessions (SessionType == Request.AccessType above)**
- **PUT <base>/Requests/{requestId}/Checkin**
- **POST <base>/Auth/Signout**

Retrieve a Password as an ISA

Case: create an ISA password request:

- **POST <base>/Auth/SignAppin**
- **GET <base>/ManagedAccounts** OR **GET <base>/ManagedAccounts?systemName={systemName}&accountName={accountName}**
- **POST <base>/ISARequests**
- **POST <base>/Auth/Signout**

Create a Session as an ISA

Case: create an ISA session:

- **POST <base>/Auth/SignAppin**
- **GET <base>/ManagedAccounts** OR **GET <base>/ManagedAccounts?systemName={systemName}&accountName={accountName}**
- **POST <base>/ISASessions**
- **POST <base>/Auth/Signout**

Authentication

Quick Navigation

POST Auth/SignAppin

Purpose

Authenticates the provided credentials and creates a user session.

Required Permissions

A user group to which the user belongs must be granted access to the API key given in authorization header. Must be running script from a valid source address as configured in API registration for the given API key.

Request Body

None.

Response Body

Content-Type: application/json

```
{
    UserId: int,
    SID: string,
    EmailAddress: string,
    UserName: string,
    Name: string
}
```

Response Codes

- 200 – Request successful. User model in the response body.
- 403 – Access forbidden. Returned if the Password Safe license is not valid.
- 410 – API version has been disabled.

For more information, please see "Common Response Codes" on page 17.

POST Auth/Signout

Purpose

Terminates the current user session.

Required Permissions

None.

Request Body

None.

Response Body

None.

Response Codes

- 200 – Request successful.

For more information, please see "Common Response Codes" on page 17.

OAuth Public API Authentication

POST Auth/Connect/Token

Purpose

Authenticates the provided credentials and allows access to the public API.

Required Permissions

Application user must be associated to an API Access Policy API registration and must belong to a user group with necessary permissions.

Request Body

Content-Type: application/x-www-form-urlencoded

```
grant_type=client_credentials&client_id=[user-client-id]&client_secret=[user-client-secret]
```

Response Body

Content-Type: application/x-www-form-urlencoded

```
{
        access_token: string,
        expires_in: int,
        token_type:string = "Bearer",
        scope: string
}
```

Response Body Details

- **access_token**: The privileged credential to use in the Authorization header for API requests to authenticate the use.
- **expires_in**: Lifetime (in seconds) that the token is valid.
- **token_type**: Describes the access token (always **Bearer**).
- **scope**: Describes the scope of the access token, which is what the token is allowed to perform. For application users, this consists of only a scope called **publicapi**.

POST Auth/SignAppIn

Request Body

None .

Header

Authorization: Bearer [access_token]

Note: *Cookies are still supported using this sign-in method.*

BeyondInsight APIs

The BeyondInsight APIs require a valid BeyondInsight license and are available to Password Safe-licensed installs.

Access Levels

(i.e., None, Read, Read/Write)

Quick Navigation

GET AccessLevels

Purpose

Returns a list of access levels for permissions, for example, **None**, **Read**, and **Read/Write**.

Required Permissions

User Accounts Management (Read).

Request Body

None.

Response Body

Content-Type: application/json

```
[
    {
        AccessLevelID:int,
        Name: string,
    },
    …
]
```

Response Codes

200 - Request successful. Access Levels in the response body.

> *For more information, please see "Common Response Codes" on page 17.*

POST UserGroups/{userGroupId}/SmartRules/{smartRuleId}/AccessLevels

Purpose

Sets the Access Level for a User Group Smart Rule.

Required Permissions

- User Accounts Management (Read/Write).

URL Parameters

- **userGroupId:** ID of the user group.
- **smartRuleId:** ID of the Smart Rule.

Request Body

Content-Type: application/json

```
{
    AccessLevelID: int
}
```

Response Body

None.

Response Codes

- 200 - Request successful.

For more information, please see "Common Response Codes" on page 17.

Address Groups

Quick Navigation

GET Organizations/{orgID}/addressgroups

Purpose

List the address groups for a given organization.

Required Permissions

- Current user has access to the organization.
- Asset Management (Read).

URL Parameters

orgId: Organization ID.

Request Body

None.

Response Body

Content-Type: application/json

```
[
    {
        AddressGroupID: int,
        Name: string,
        OrganizationID: guid // can be null
    }
]
```

Response Codes

200 - Request successful.

> *For more information, please see "Common Response Codes" on page 17.*

GET Addressgroups

Purpose

List the address groups.

Required Permissions

- Current user has access to the organization.
- Asset Management (Read).

URL Parameters

None.

Request Body

None.

Response Body

Content-Type: application/json

```
[
    {
        AddressGroupID: int,
        Name: string,
        OrganizationID: guid // can be null
```

```
    {
]
```

Response Codes

200 - Request successful.

> *For more information, please see "Common Response Codes" on page 17.*

GET Addressgroups/{addressGroupId}/addresses

Purpose

List the addresses for an address group.

Required Permissions

- Current user has access to the organization.
- Asset Management (Read).

URL Parameters

addressGroupId: Address Group ID.

Request Body

None.

Response Body

Content-Type: application/json

```
[
    {
        AddressID: int,
        AddressGroupID: int,
        Omit: boolean,
        Type: string,
        Value: string,
        LastUpdatedDate: datetime
    }
]
```

Response Codes

200 - Request successful.

For more information, please see "Common Response Codes" on page 17.

POST AddressGroups/{id}/Addresses

Purpose

Create an address in an Address Book.

Required Permissions

- Asset Management (Read/Write).

URL Parameters

addressGroupId: Address Group ID.

Request Body

```
{
    Type: int,
    Value: string,
    Omit: bool
}
```

Request Body Details

Max string length for Value is 225.

Response Body

Content-Type: application/json

```
{
    AddressID: int,
    AddressGroupID: int,
    Omit: bool,
    Type: int,
    Value: string,
```

```
    LastUpdatedDate: datetime
}
```

Response Codes

201 - Request successful. Address in the response body.

For more information, please see "Common Response Codes" on page 17.

DELETE Addressgroups/{addressGroupId}

Purpose

Delete the address group and all it's addresses.

Required Permissions

- Current user has access to the organization.
- Asset Management (Read/Write).

URL Parameters

addressGroupId: Address Group ID.

Request Body

None.

Response Body

None.

Response Codes

200 - Request successful.

For more information, please see "Common Response Codes" on page 17.

DELETE Addressgroups/{addressGroupId}/addresses

Purpose

Delete the addresses within the address group.

Required Permissions

- Current user has access to the organization.
- Asset Management (Read/Write).

URL Parameters

addressGroupId: Address Group ID.

Request Body

None.

Response Body

None.

Response Codes

200 - Request successful.

For more information, please see "Common Response Codes" on page 17.

GET AddressGroups/?name={name}

Purpose

Returns the Address Group by name.

Required Permissions

- Asset Management (Read).

Query Parameters

name: Name of the Address Group.

Request Body

None.

Response Body

Content-Type: application/json

```
{
    AddressGroupID: int,
    Name: string
}
```

Response Codes

200 - Request successful. Address Group in the response body.

For more information, please see "Common Response Codes" on page 17.

GET AddressGroups/{id}

Purpose

Returns the Address Group by ID.

Required Permissions

- Asset Management (Read).

URL Parameters

id: ID of the Address Group.

Request Body

None.

Response Body

Content-Type: application/json

```
{
    AddressGroupID: int,
    Name: string
}
```

Response Codes

200 - Request successful. Address Group in the response body.

For more information, please see "Common Response Codes" on page 17.

PUT Addresses/{id}

Purpose

Updates and Address by ID.

Required Permissions

- Asset Management (Read/Write).

Request Body

Content-Type: application/json

```
{
    Type: int,
    Value: string,
    Omit: bool
}
```

Request Body Details

Max string length for Value is 225.

Response Body

Content-Type: application/json

```
{
    AddressD: int,
    AddressGroupID: int,
    Omit: bool,
    Type: int,
    Value: string,
    LastUpdateDate: datetime
}
```

Response Codes

200 - Request successful. Address in the response body.

For more information, please see "Common Response Codes" on page 17.

PUT AddressGroups/{id}

Purpose

Updates and Address Group by ID.

Required Permissions

- Asset Management (Read/Write).

Request Body

Content-Type: application/json

```
{
    Name: string,
}
```

Request Body Details

Max string length for Name is 225.

Response Body

Content-Type: application/json

```
{
    AddressGroupID: int,
```

```
    Name: string
}
```

Response Codes

200 - Request successful. Address Group in the response body.

> *For more information, please see "Common Response Codes" on page 17.*

POST AddressGroups

Purpose

Creates an Address Book.

Required Permissions

- Asset Management (Read/Write).

Request Body

Content-Type: application/json

```
{
    Name: string
}
```

Request Body Details

Max string length for Name is 225.

Response Body

Content-Type: application/json

```
{
    AddressGroupID: int,
    Name: string
}
```

Response Codes

201 - Request successful. Address Group in the response body.

For more information, please see "Common Response Codes" on page 17.

GET Addresses/{id}

Purpose

Returns the Address by ID.

Required Permissions

- Asset Management (Read).

URL Parameters

id: ID of the Address.

Request Body

None.

Response Body

Content-Type: application/json

```
{
    AddressId: int,
    AddressGroupId : int,
    Omit: bool,
    Type: string,
    Value: string,
    LastUpdateDate: datetime
}
```

Response Codes

200 - Request successful. Address in the response body.

For more information, please see "Common Response Codes" on page 17.

DELETE Addresses/{id}

Purpose

Deletes an Address by ID.

Required Permissions

Asset Management (Read/Write).

Request Body

None.

Response Body

None.

Response Codes

200 - Request successful.

For more information, please see "Common Response Codes" on page 17.

API Registrations

Quick Navigation

GET ApiRegistrations

Purpose

Returns a list of all API registrations.

Required Permissions

API Registration Management (Read).

Query Parameters

...

Request Body

None.

Response Body

Content-Type: application/json

```
{
            Id: int,
            Name: string,
            RegistrationType: string,
            Active: bool,
            Visible: bool,
            MultiFactorAuthenticationEnforced: bool,
            ClientCertificateRequired: bool,
            UserPasswordRequired: bool,
```

```
            VerifyPsrunSignature: bool,
            IPAuthenticationRules:[
                  {
                        Id: int,
                        Type: string,
                        Value: string,
                        Description: string,
                        CreatedDate: date
                  },
                  ...
            ],
            PSRUNRules:[
                  {
                        Id:int,
                        IPAddress: string,
                        MacAddress: string,
                        SystemName: string,
                        FQDN: string,
                        DomainName: string,
                        UserId: string,
                        RootVolumeId: string,
                        OSVersion: string,
                        CreatedDate: date
                  },

                  ...
            ],
            XForwardedForAuthenticationRules:[
                  {
                        Id: int,
                        Type: string,
                        Value: string,
                        Description: string,
                        CreatedDate: date
                  },
                  ...

            ]
}
```

Response Codes

200 – Request successful. API Registration in the response body.

For more information, please see "Common Response Codes" on page 17.

GET ApiRegistrations/{id}

Purpose

Returns an API registration by ID.

Required Permissions

API Registration Management (Read).

Query Parameters

Id: ID of the API registration.

Request Body

None.

Response Body

Content-Type: application/json

```
{
        Id: int,
        Name: string,
        RegistrationType: string,
        Active: bool,
        Visible: bool,
        MultiFactorAuthenticationEnforced: bool,
        ClientCertificateRequired: bool,
        UserPasswordRequired: bool,
        VerifyPsrunSignature: bool,
        IPAuthenticationRules:[
                  {
                          Id: int,
                          Type: string,
                          Value: string,
                          Description: string,
                          CreatedDate: date
                  },
                  ...
            ],
            PSRUNRules:[
                  {
                          Id:int,
                          IPAddress: string,
                          MacAddress: string,
                          SystemName: string,
```

```
                        FQDN: string,
                        DomainName: string,
                        UserId: string,
                        RootVolumeId: string,
                        OSVersion: string,
                        CreatedDate: date
                },

                ...
        ],
        XForwardedForAuthenticationRules: [
                {
                        Id: int,
                        Type: string,
                        Value: string,
                        Description: string,
                        CreatedDate: date
                },
                ...

        ]
}
```

Response Codes

200 – Request successful. API Registration in the response body.

For more information, please see "Common Response Codes" on page 17.

POST ApiRegistrations

Purpose

Creates an API registration.

Required Permissions

API Registration Management (Read/Write).

Query Parameters

...

Request Body

The request body differs by RegistrationType.

Content-Type: application/json

ApiKeyPolicy

```
{
            Id: int,
            Name: string,
            RegistrationType: string = "ApiKeyPolicy",
            Active: bool,
            Visible: bool,
            MultiFactorAuthenticationEnforced: bool,
            ClientCertificateRequired: bool,
            UserPasswordRequired: bool,
            VerifyPsrunSignature: bool,
            IPAuthenticationRules:[
                  {
                        Id: int,
                        Type: string,
                        Value: string,
                        Description: string,
                  },
                  ...
            ],
            PSRUNRules:[
                  {
                        Id:int,
                        IPAddress: string,
                        MacAddress: string,
                        SystemName: string,
                        FQDN: string,
                        DomainName: string,
                        UserId: string,
                        RootVolumeId: string,
                        OSVersion: string,
                  },

                  ...
            ],
            XForwardedForAuthenticationRules:[
                  {
                        Id: int,
                        Type: string,
                        Value: string,
                        Description: string,
                  },
                  ...

            ]
}
```

ApiAccessPolicy

```
{
            Id: int,
            Name: string,
            RegistrationType: string = "ApiAccessPolicy",
            AccessTokenDuration: int = 60,
            Active: bool,
            Visible: bool,
            ClientCertificateRequired: bool,
            IPAuthenticationRules:[
                  {
                        Id: int,
                        Type: string,
                        Value: string,
                        Description: string,
                  },
                  ...
            ],
            XForwardedForAuthenticationRules:[
                  {
                        Id: int,
                        Type: string,
                        Value: string,
                        Description: string,
                  },
                  ...

            ]
}
```

Response Body

Content-Type: application/json

```
{
            Id: int,
            Name: string,
            RegistrationType: string,
            AccessTokenDuration: int,
            Active: bool,
            Visible: bool,
            MultiFactorAuthenticationEnforced: bool,
            ClientCertificateRequired: bool,
            UserPasswordRequired: bool,
            VerifyPsrunSignature: bool,
            IPAuthenticationRules:[
                  {
                        Id: int,
                        Type: string,
                        Value: string,
                        Description: string,
```

```
                        CreatedDate; date
                },
                ...
        ],
        PSRUNRules:[
                {
                        Id:int,
                        IPAddress: string,
                        MacAddress: string,
                        SystemName: string,
                        FQDN: string,
                        DomainName: string,
                        UserId: string,
                        RootVolumeId: string,
                        OSVersion: string,
                        CreatedDate; date
                },

                ...
        ],
        XForwardedForAuthenticationRules:[
                {
                        Id: int,
                        Type: string,
                        Value: string,
                        Description: string,
                        CreatedDate; date
                },
                ...

        ]
}
```

Response Codes

200 – Request successful. API Registration in the response body.

For more information, please see "Common Response Codes" on page 17.

PUT ApiRegistrations/{id}

Purpose

Updates an API registration by ID.

Required Permissions

API Registration Management (Read/Write).

Query Parameters

Id: ID of the API registration.

Request Body

The request body differs by Registration Type.

Content-Type: application/json

ApiKeyPolicy

```
{
            Id: int,
            Name: string,
            RegistrationType: string = "ApiKeyPolicy",
            Active: bool,
            Visible: bool,
            MultiFactorAuthenticationEnforced: bool,
            ClientCertificateRequired: bool,
            UserPasswordRequired: bool,
            VerifyPsrunSignature: bool,
            IPAuthenticationRules:[
                  {
                        Id: int,
                        Type: string,
                        Value: string,
                        Description: string,
                  },
                  ...
            ],
            PSRUNRules:[
                  {
                        Id:int,
                        IPAddress: string,
                        MacAddress: string,
                        SystemName: string,
                        FQDN: string,
                        DomainName: string,
                        UserId: string,
                        RootVolumeId: string,
                        OSVersion: string,
                  },

                  ...
            ],
            XForwardedForAuthenticationRules:[
                  {
                        Id: int,
                        Type: string,
                        Value: string,
                        Description: string,
```

```
                },
                ...

        ]
}
```

ApiAccessPolicy

```
{
        Id: int,
        Name: string,
        RegistrationType: string = "ApiAccessPolicy",
        AccessTokenDuration: int = 60,
        Active: bool,
        Visible: bool,
        ClientCertificateRequired: bool,
        IPAuthenticationRules:[
                {
                        Id: int,
                        Type: string,
                        Value: string,
                        Description: string,
                },
                ...
        ],
        XForwardedForAuthenticationRules:[
                {
                        Id: int,
                        Type: string,
                        Value: string,
                        Description: string,
                },
                ...

        ]
}
```

Response Body

Content-Type: application/json

```
{
        Id: int,
        Name: string,
        RegistrationType: string,
        AccessTokenDuration: int,
        Active: bool,
        Visible: bool,
        MultiFactorAuthenticationEnforced: bool,
        ClientCertificateRequired: bool,
```

```
            UserPasswordRequired: bool,
            VerifyPsrunSignature: bool,
            IPAuthenticationRules:[
                  {
                        Id: int,
                        Type: string,
                        Value: string,
                        Description: string,
                        CreatedDate; date
                  },
                  ...
            ],
            PSRUNRules:[
                  {
                        Id:int,
                        IPAddress: string,
                        MacAddress: string,
                        SystemName: string,
                        FQDN: string,
                        DomainName: string,
                        UserId: string,
                        RootVolumeId: string,
                        OSVersion: string,
                        CreatedDate; date
                  },

                  ...
            ],
            XForwardedForAuthenticationRules:[
                  {
                        Id: int,
                        Type: string,
                        Value: string,
                        Description: string,
                        CreatedDate; date
                  },
                  ...

            ]
}
```

Response Codes

200 – Request successful. API Registration in the response body.

For more information, please see "Common Response Codes" on page 17.

DELETE ApiRegistrations/{id}

Purpose

Deletes the API Registration for the ID provided.

Required Permissions

API Registration Management (Read/Write).

Request Body

None.

Response Body

None.

Response Codes

200 – Request successful.

For more information, please see "Common Response Codes" on page 17.

POST ApiRegistrations/{id}/Rotate

Note: *For API Key Policy only.*

Purpose

Rotates the API key for an API Key policy API Registration

Required Permissions

API Registration Management (Read/Write).

Query Parameters

...

Request Body

None.

Response Body

Content-Type: application/json

```
string
```

Response Codes

201 – Request successful. API key in the response body.

For more information, please see "Common Response Codes" on page 17.

GET ApiRegistrations/{id}/Key

Note: *For API Key Policy only.*

Purpose

Retrieves the API key for an API Key policy API Registration.

Required Permissions

API Registration Management (Read/Write).

Query Parameters

...

Request Body

None.

Response Body

Content- Type: application/json

```
string
```

Response Codes

200 – Request successful. API Key in the response body.

For more information, please see "Common Response Codes" on page 17.

Assets

Quick Navigation

For more information on related topics, please see:

- *"Workgroups" on page 149*
- *"Smart Rules" on page 107*
- *"Managed Systems" on page 284*

GET Assets/{id}

Purpose

Returns an asset by ID.

Required Permissions

Asset Management (Read).

URL Parameters

id: ID of the asset.

Request Body

None.

Response Body

Content-Type: application/json

```
{
    WorkgroupID: int,
    AssetID: int,
    AssetName: string,
    DnsName: string,
    DomainName: string,
    IPAddress: string,
    MacAddress: string,
    AssetType: string,
    OperatingSystem: string,
    CreateDate: datetime,
    LastUpdateDate: datetime
}
```

Response Codes

200 - Request successful. Asset in response body.

For more information, please see "Common Response Codes" on page 17.

GET Workgroups/{workgroupID}/Assets

Purpose

Returns a list of assets by Workgroup ID.

Required Permissions

Asset Management (Read).

URL Parameters

workgroupID: ID of the Workgroup.

Query Parameters (Optional)

- **limit:** (default: 100000) Number of records to return.
- **offset:** (default: 0) Number of records to skip before returning <limit> records (can be used in conjunction only with limit).

Request Body

None.

Response Body (when limit is not given)

Content-Type: application/json

```
[
    {
        WorkgroupID: int,
        AssetID: int,
        AssetName: string,
        DnsName: string,
        DomainName: string,
        IPAddress: string,
        MacAddress: string,
        AssetType: string,
        OperatingSystem: string,
        CreateDate: datetime,
        LastUpdateDate: datetime
    },
    …
]
```

Response Body (when limit is given)

Content-Type: application/json

```
{
    TotalCount : int,
    Data :
    [
        {
            WorkgroupID: int,
            AssetID: int,
            AssetName: string,
            DnsName: string,
            DomainName: string,
            IPAddress: string,
            MacAddress: string,
            AssetType: string,
            OperatingSystem: string,
            CreateDate: datetime,
            LastUpdateDate: datetime
        },
        …
    ]
}
```

Response Codes

200 - Request successful. Assets in response body.

For more information, please see "Common Response Codes" on page 17.

GET Workgroups/{workgroupName}/Assets

Purpose

Returns a list of assets by Workgroup name.

Required Permissions

Asset Management (Read).

URL Parameters

workgroupName: Name of the Workgroup.

Query Parameters (Optional)

- **limit:** (default: 100000) Number of records to return.
- **offset:** (default: 0) Number of records to skip before returning <limit> records (can only be used in conjunction with limit).

Request Body

None.

Response Body (when limit is not given)

Content-Type: application/json

```
[
    {
        WorkgroupID: int,
        AssetID: int,
        AssetName: string,
        DnsName: string,
        DomainName: string,
        IPAddress: string,
        MacAddress: string,
        AssetType: string,
        OperatingSystem: string,
        CreateDate: datetime,
        LastUpdateDate: datetime
    },
    …
]
```

Response Body (when limit is given)

Content-Type: application/json

```
{
    TotalCount : int,
    Data :
    [
        {
            WorkgroupID: int,
            AssetID: int,
            AssetName: string,
            DnsName: string,
            DomainName: string,
            IPAddress: string,
            MacAddress: string,
            AssetType: string,
            OperatingSystem: string,
            CreateDate: datetime,
            LastUpdateDate: datetime
        },
        …
    ]
}
```

Response Codes

200 - Request successful. Assets in response body.

For more information, please see "Common Response Codes" on page 17.

GET Workgroups/{workgroupName}/Assets?name={name}

Purpose

Returns an asset by Workgroup name and asset name.

Required Permissions

Asset Management (Read).

URL Parameters

workgroupName: Name of the Workgroup.

Query Parameters

name: Name of the asset.

Request Body

None.

Response Body

Content-Type: application/json

```
{
    WorkgroupID: int,
    AssetID: int,
    AssetName: string,
    DnsName: string,
    DomainName: string,
    IPAddress: string,
    MacAddress: string,
    AssetType: string,
    OperatingSystem: string,
    CreateDate: datetime,
    LastUpdateDate: datetime
}
```

Response Codes

200 - Request successful. Asset in response body.

For more information, please see "Common Response Codes" on page 17.

POST Workgroups/{workgroupID}/Assets

Purpose

Creates a new asset in the Workgroup, referenced by ID.

Required Permissions

Asset Management (Read/Write).

URL Parameters

workgroupID: ID of the Workgroup.

Request Body

Content-Type: application/json

```
{
    IPAddress: string,
    AssetName: string,
    DnsName: string,
    DomainName: string,
    MacAddress: string,
    AssetType: string,
    OperatingSystem: string
}
```

Request Body Details

- **IPAddress:** (required) Asset IP address. Max string length is 45.
- **AssetName:** (optional) Asset name. If not given, a padded IP address is used. Max string length is 128.
- **DnsName:** (optional) Asset DNS name. Max string length is 255.
- **DomainName:** (optional) Asset domain name. Max string length is 64.
- **MacAddress:** (optional) Asset MAC address. Max string length is 128.
- **AssetType:** (optional) Asset type. Max string length is 64.
- **OperatingSystem:** (optional) Asset operating system. Max string length is 255.

Response Body

Content-Type: application/json

```
{
    WorkgroupID: int,
    AssetID: int,
    AssetName: string,
    DnsName: string,
    DomainName: string,
    IPAddress: string,
    MacAddress: string,
    AssetType: string,
    OperatingSystem: string,
    CreateDate: datetime,
    LastUpdateDate: datetime
}
```

Response Codes

201 - Request successful. Asset in response body.

For more information, please see "Common Response Codes" on page 17.

POST Workgroups/{workgroupName}/Assets

Purpose

Creates a new asset in the Workgroup referenced by name.

Required Permissions

Asset Management (Read/Write).

URL Parameters

workgroupName: Name of the Workgroup.

Request Body

Content-Type: application/json

```
{
    IPAddress: string,
    AssetName: string,
    DnsName: string,
    DomainName: string,
    MacAddress: string,
    AssetType: string,
    OperatingSystem: string
}
```

Request Body Details

- **IPAddress:** (required) Asset IP address. Max string length is 45.
- **AssetName:** (optional) Asset name. If not given, a padded IP address is used. Max string length is 128.
- **DnsName:** (optional) Asset DNS name. Max string length is 255.
- **DomainName:** (optional) Asset domain name. Max string length is 64.
- **MacAddress:** (optional) Asset MAC address. Max string length is 128.
- **AssetType:** (optional) Asset type. Max string length is 64.
- **OperatingSystem:** (optional) Asset operating system. Max string length is 255.

Response Body

Content-Type: application/json

```
{
    WorkgroupID: int,
    AssetID: int,
    AssetName: string,
    DnsName: string,
    DomainName: string,
    IPAddress: string,
    MacAddress: string,
    AssetType: string,
    OperatingSystem: string,
    CreateDate: datetime,
    LastUpdateDate: datetime
}
```

Response Codes

201 - Request successful. Asset in response body.

For more information, please see "Common Response Codes" on page 17.

PUT Assets/{id}

Purpose

Updates an existing asset by ID.

> ***Tip:*** *Call **GET Assets/{id}** (or equivalent) first to get the current state of the asset before calling **PUT Assets/{id}** to update it with new values.*

Required Permissions

Asset Management (Read/Write).

URL Parameters

id: ID of the asset.

Request Body

Content-Type: application/json

```
{
    WorkgroupID: int,
    AssetName: string,
    DnsName: string,
    DomainName: string,
    IPAddress: string,
    MacAddress: string,
    AssetType: string,
    OperatingSystem: string,
}
```

Request Body Details

- **WorkgroupID:** (required) ID of the Workgroup to which the asset belongs.
- **AssetName:** (required) Asset name.
- **DnsName:** (required) Asset DNS name.
- **DomainName:** (required) Asset domain name.
- **IPAddress:** (required) Asset IP address.
- **MacAddress:** (required) Asset MAC address. An empty value is accepted and clears any existing value.
- **AssetType:** (required) Asset type. An empty value is accepted and clears any existing value.
- **OperatingSystem:** (required) Asset operating system. An empty value is accepted and clears any existing value.

Response Body

Content-Type: application/json

```
{
    WorkgroupID: int,
    AssetID: int,
    AssetName: string,
    DnsName: string,
    DomainName: string,
    IPAddress: string,
    MacAddress: string,
    AssetType: string,
    OperatingSystem: string,
    CreateDate: datetime,
    LastUpdateDate: datetime
}
```

Response Codes

200 - Request successful. Asset in response body.

For more information, please see "Common Response Codes" on page 17.

POST Assets/Search

Purpose

Returns a list of assets that match the given search criteria.

Required Permissions

Asset Management (Read).

Query Parameters (Optional)

- **limit:** (default: 100000) Number of records to return.
- **offset:** (default: 0) Number of records to skip before returning <limit> records (can only be used in conjunction with limit).

Request Body

Content-Type: application/json

```
{
    AssetName: string,
    DnsName: string,
    DomainName: string,
    IPAddress: string,
    MacAddress: string,
    AssetType: string,
}
```

Request Body Details

At least one request body property should be provided; any property not provided is ignored. All search criteria is case insensitive and is an exact match (equality), except for **IPAddress**.

IPAddress can be a single IP address (10.0.0.1), a comma-delimited list of IPs (10.0.0.1,10.0.0.2,10.0.0.3), an IP range (10.0.0.1-10.0.0.25), or CIDR notation (10.0.0.0/24).

Response Body (when limit is not given)

Content-Type: application/json

```
[
    {
        WorkgroupID: int,
        AssetID: int,
        AssetName: string,
```

```
        DnsName: string,
        DomainName: string,
        IPAddress: string,
        MacAddress: string,
        AssetType: string,
        OperatingSystem: string,
        CreateDate: datetime,
        LastUpdateDate: datetime
    },
    …
]
```

Response Body (when limit is given)

Content-Type: application/json

```
{
    TotalCount : int,
    Data :
    [
        {
            WorkgroupID: int,
            AssetID: int,
            AssetName: string,
            DnsName: string,
            DomainName: string,
            IPAddress: string,
            MacAddress: string,
            AssetType: string,
            OperatingSystem: string,
            CreateDate: datetime,
            LastUpdateDate: datetime
        },
        …
    ]
}
```

Response Codes

200 - Request successful. Assets in response body.

For more information, please see "Common Response Codes" on page 17.

DELETE Assets/{id}

Purpose

Deletes an asset by ID.

Required Permissions

Asset Management (Read/Write).

URL Parameters

id: ID of the asset.

Request Body

None.

Response Body

None.

Response Codes

200 - Request successful.

For more information, please see "Common Response Codes" on page 17.

DELETE Workgroups/{workgroupName}/Assets?name={name}

Purpose

Deletes an asset by Workgroup name and asset name.

Required Permissions

Asset Management (Read/Write).

URL Parameters

workgroupName: Name of the Workgroup.

Query Parameters

name: Name of the asset.

Request Body

None.

Response Body

None.

Response Codes

200 - Request successful.

For more information, please see "Common Response Codes" on page 17.

Smart Rule Assets

GET SmartRules/{id}/Assets

Purpose

Returns a list of assets by Smart Rule ID.

Required Permissions

Read access to the Smart Rule referenced by ID.

URL Parameters

id: ID of the Smart Rule.

Query Parameters (Optional)

- **limit:** (default: 100000) Number of records to return.
- **offset:** (default: 0) Number of records to skip before returning <limit> records (can be used only in conjunction with limit).

Request Body

None.

Response Body (when limit is not given)

Content-Type: application/json

```
[
    {
        WorkgroupID: int,
        AssetID: int,
        AssetName: string,
        DnsName: string,
        DomainName: string,
        IPAddress: string,
        MacAddress: string,
        AssetType: string,
        OperatingSystem: string,
        CreateDate: datetime,
        LastUpdateDate: datetime
    },
    …
]
```

Response Body (when limit is given)

Content-Type: application/json

```
{
    TotalCount : int,
    Data :
    [
        {
            WorkgroupID: int,
            AssetID: int,
            AssetName: string,
            DnsName: string,
            DomainName: string,
            IPAddress: string,
            MacAddress: string,
            AssetType: string,
            OperatingSystem: string,
            CreateDate: datetime,
            LastUpdateDate: datetime
        },
        …
    ]
}
```

Response Codes

200 - Request successful. Assets in response body.

For more information, please see "Common Response Codes" on page 17.

Asset Attributes

Quick Navigation

GET Assets/{assetID}/Attributes

Purpose

Returns a list of attributes by Asset ID.

Required Permissions

Asset Management (Read), Attribute Management (Read).

URL Parameters

assetID: ID of the asset.

Request Body

None.

Response Body

Content-Type: application/json

```
[
    {
        AttributeID : int, AttributeTypeID : int,
        ParentAttributeID : int, // can be null
        ShortName : string,
        LongName : string,
        Description : string,
        ValueInt : int, // can be null
        IsReadOnly: bool
    },
    …
]
```

Response Codes

200 – Request successful. Attributes associated with the asset in the response body.

For more information, please see "Common Response Codes" on page 17.

POST Assets/{assetID}/Attributes/{attributeID}

Purpose

Assigns an attribute to an asset.

Required Permissions

Asset Management (Read/Write), Attribute Management (Read/Write).

URL Parameters

- **assetID:** ID of the asset.
- **attributeID:** ID of the attribute Request Body.

Response Body

Content-Type: application/json

```
{
    AttributeID : int, AttributeTypeID : int,
    ParentAttributeID : int, // can be null
    ShortName : string,
    LongName : string,
    Description : string,
    ValueInt : int, // can be null
    IsReadOnly: bool,
}
```

Response Codes

201 – Request successful. Attributes in the response body.

For more information, please see "Common Response Codes" on page 17.

DELETE Assets/{assetID}/Attributes

Purpose

Deletes all asset attributes by asset ID.

Required Permissions

Asset Management (Read/Write), Attribute Management (Read/Write).

URL Parameters

assetID: ID of the asset.

Request Body

None.

Response Body

None.

Response Codes

200 – Request successful.

For more information, please see "Common Response Codes" on page 17.

DELETE Assets/{assetID}/Attributes/{attributeID}

Purpose

Deletes an asset attribute by asset ID and attribute ID.

Required Permissions

- Asset Management (Read/Write).
- Attribute Management (Read/Write).

URL Parameters

assetID: ID of the asset attributeID and ID of the attribute.

Request Body

None.

Response Body

None.

Response Codes

200 – Request successful.

For more information, please see "Common Response Codes" on page 17.

Attribute Types

Quick Navigation

GET AttributeTypes

Purpose

Returns a list of attribute types.

Required Permissions

Attribute Management (Read).

Request Body

None.

Response Body

Content-Type: application/json

```
[
    {
        AttributeTypeID : int,
        Name : string,
        IsReadOnly: bool
    },
    …
]
```

Response Codes

200 – Request successful. Attribute types in the response body.

> *For more information, please see "Common Response Codes" on page 17.*

GET AttributeTypes/{id}

Purpose

Returns an attribute type by ID.

Required Permissions

Attribute Management (Read).

URL Parameters

id: ID of the attribute type.

Request Body

None.

Response Body

Content-type: application/json

```
{
    AttributeTypeID : int,
    Name : string,
    IsReadOnly: bool
}
```

Response Codes

200 – Request successful. Attribute type in the response body.

For more information, please see "Common Response Codes" on page 17.

POST AttributeTypes

Purpose

Creates a new attribute type.

Required Permissions

Attribute Management (Read/Write).

Request Body

Content-Type: application/json

```
{
    Name : string
}
```

Request Body Details

Max string length for Name is 64.

Response Body

Content-type: application/json

```
{
    AttributeTypeID : int,
    Name : string,
    IsReadOnly: bool
}
```

Response Codes

201 – Request successful. Attribute type in the response body.

For more information, please see "Common Response Codes" on page 17.

DELETE AttributeTypes/{id}

Purpose

Deletes an attribute type and all related attributes by ID.

Required Permissions

Attribute Management (Read/Write).

URL Parameters

id: ID of the attribute type.

Request Body

None.

Response Body

None.

Response Codes

200 – Request successful.

For more information, please see "Common Response Codes" on page 17.

Attributes

Quick Navigation

GET AttributeTypes/{attributeTypeID}/Attributes

Purpose

Returns a list of attribute definitions by attribute type.

Required Permissions

Attribute Management (Read).

URL Parameters

attributeTypeID: ID of the attribute type.

Request Body

None.

Response Body

Content-Type: application/json

```
[
    {
        AttributeID : int,
        AttributeTypeID : int,
        ParentAttributeID : int, // can be null
        ShortName : string,
        LongName : string,
        Description : string,
        ValueInt : int, // can be null
        IsReadOnly: bool,
        ChildAttributes :
        [
            {
```

```
                AttributeID : int,
                AttributeTypeID : int,
                ParentAttributeID : int,
                ShortName : string,
                LongName : string,
                Description : string,
                ValueInt : int, // can be null
                IsReadOnly: bool,
            },
            …
        ]
    },
    …
]
```

Response Codes

200 – Request successful. Attributes in the response body.

For more information, please see "Common Response Codes" on page 17.

GET Attributes/{id}

Purpose

Returns an attribute definition by ID.

Required Permissions

Attribute Management (Read).

URL Parameters

id: ID of the attribute.

Request Body

None.

Response Body

Content-Type: application/json

```
{
    AttributeID : int,
    AttributeTypeID : int,
    ParentAttributeID : int, // can be null
    ShortName : string,
    LongName : string,
    Description : string,
    ValueInt : int, // can be null
    IsReadOnly: bool,
    ChildAttributes :
    [
        {
            AttributeID : int,
            AttributeTypeID : int,
            ParentAttributeID : int,
            ShortName : string,
            LongName : string,
            Description : string,
            ValueInt : int, // can be null
            IsReadOnly: bool,
        },
        …
    ]
}
```

Response Codes

200 – Request successful. Attributes in the response body.

For more information, please see "Common Response Codes" on page 17.

POST AttributeTypes/{attributeTypeID}/Attributes

Purpose

Creates a new attribute definition by attribute type ID.

Required Permissions

Attribute Management (Read/Write).

URL Parameters

attributeTypeID: ID of the attribute type.

Request Body

Content-Type: application/json

```
{
    ParentAttributeID : int, // can be null
    ShortName : string,
    LongName : string,
    Description : string,
    ValueInt : int // can be null
}
```

Request Body Details

Max string length for ShortName and LongName is 64. Max string length for Description is 255.

Response Body

Content-Type: application/json

```
{
    AttributeID : int,
    AttributeTypeID : int,
    ParentAttributeID : int, // can be null
    ShortName : string,
    LongName : string,
    Description : string,
    ValueInt : int, // can be null
    IsReadOnly: bool,
    ChildAttributes :
    [
        {
            AttributeID : int,
            AttributeTypeID : int,
            ParentAttributeID : int,
            ShortName : string,
            LongName : string,
            Description : string,
            ValueInt : int, // can be null
            IsReadOnly: bool,
        },
        …
    ]
}
```

Response Codes

201 – Request successful. Attributes in the response body.

For more information, please see "Common Response Codes" on page 17.

DELETE Attributes/{id}

Purpose

Deletes an attribute definition by ID.

Required Permissions

Attribute Management (Read/Write).

URL Parameters

id: ID of the attribute.

Request Body

None.

Response Body

None.

Response Codes

200 – Request successful.

For more information, please see "Common Response Codes" on page 17.

Configuration

GET Configuration/Version

Purpose

Returns the current system version.

Request Body

None.

Response Body

Content-Type: application/json

```
{
    Version : string
}
```

Response Codes

200 – Request successful. Version model in the response body.

For more information, please see "Common Response Codes" on page 17.

Databases

Quick Navigation

For more information on related topics, please see:

- *"Assets" on page 54*
- *"Platforms" on page 352*
- *"Managed Systems" on page 284*

GET Databases

Purpose

Returns a list of databases.

Required Permissions

Asset Management (Read).

Request Body

None.

Response Body

Content-Type: application/json

```
[
    {
        AssetID: int,
        DatabaseID : int,
        PlatformID : int,
        InstanceName : string,
```

```
        IsDefaultInstance : bool,
        Port : int,
        Version : string,
        Template:string
    },
    …
]
```

Response Codes

201 – Request successful. Databases in the response body.

> *For more information, please see "Common Response Codes" on page 17.*

GET Databases/{id}

Purpose

Returns a database by ID.

Required Permissions

Asset Management (Read).

URL Parameters

id: ID of the database.

Request Body

None.

Response Body

Content-Type: application/json

```
{
    AssetID:int,
    DatabaseID : int,
    PlatformID : int,
    InstanceName : string,
    IsDefaultInstance : bool,
    Port : int,
```

```
    Version : string
}
```

Response Codes

201 – Request successful. Databases in the response body.

For more information, please see "Common Response Codes" on page 17.

GET Assets/{id}/Databases

Purpose

Returns a list of databases for the given asset.

Required Permissions

Asset Management (Read).

URL Parameters

id: ID of the asset.

Request Body

None.

Response Body

Content-Type: application/json

```
[
    {
        AssetID: int,
        DatabaseID : int,
        PlatformID : int,
        InstanceName : string,
        IsDefaultInstance : bool,
        Port : int,
        Version : string,
        Template:string
    },
…
```

Response Codes

201 – Request successful. Databases in the response body.

For more information, please see "Common Response Codes" on page 17.

POST Assets/{id}/Databases

Purpose

Creates a new database in the asset referenced by ID.

Required Permissions

Asset Management (Read/Write).

URL Parameters

id: ID of the asset.

Request Body

Content-Type: application/json

```
{
    PlatformID : int,
    InstanceName : string,
    IsDefaultInstance : bool,
    Port : int,
    Version : string,
    Template : string,
}
```

Request Body Details

- **PlatformID:** (required) ID of the platform
- **InstanceName:** Name of the database instance. Required when **IsDefaultInstance** is false. Max string length is 100.
- **IsDefaultInstance:** True if the database instance is the default instance, otherwise false.

Note: *Only MS SQL Server and MySQL platforms support setting this value to true.*

- **Port:** (required) The database port.
- **Version:** The database version. Max string value is 20.

- **Template:** The database connection template.

Response Body

Content-Type: application/json

```
{
    AssetID: int,
    DatabaseID : int,
    PlatformID : int,
    InstanceName : string,
    IsDefaultInstance : bool,
    Port : int,
    Version : string,
    Template:string
}
```

Response Codes

200 – Request successful. Databases in the response body.

For more information, please see "Common Response Codes" on page 17.

PUT Databases/{id}

Purpose

Updates an existing database by ID.

Required Permissions

Asset Management (Read/Write).

URL Parameters

id: ID of the database.

Request Body

Content-Type: application/json

```
{
    PlatformID: int,
    InstanceName: string,
```

```
    IsDefaultInstance: bool,
    Port: int,
    Version: string,
    Template: string
}
```

Request Body Details

- **PlatformID:** (required) ID of the platform.
- **InstanceName:** Name of the database instance. Required when **IsDefaultInstance** is false. Max string length is 100.
- **IsDefaultInstance:** True if the database instance is the default instance, otherwise false.

> ***Note:*** *Only MS SQL Server and MySQL platforms support setting this value to true.*

- **Port:** The database port.
- **Version:** The database version. Max string length is 20.
- **Template:** The database connection template.

Response Body

Content-Type: application/json

```
{
    AssetID: int,
    DatabaseID: int,
    PlatformID: int,
    InstanceName: string,
    IsDefaultInstance: bool,Port: int,
    Version: string,
    Template: string
}
```

Response Codes

200 – Request successful. Databases in the response body.

> *For more information, please see "Common Response Codes" on page 17.*

DELETE Databases/{id}

Purpose

Deletes a database by ID.

Required Permissions

Asset Management (Read/Write).

URL Parameters

id: ID of the database.

Request Body

None.

Response Body

None.

Response Codes

200 – Request successful.

For more information, please see "Common Response Codes" on page 17.

Entitlements

Quick Navigation

GET Entitlements

Purpose

Returns user entitlements.

Required Permissions

Analytics and Reporting (Read).

URL Parameters

None.

Request Body

None.

Response Body

Content-Type: application/json

```
[
    {
        GroupID : int,
        Name : string,
        SmartRuleId : int,
        DistinguishedName : string,
        AccessLevel : string, // can be null
        RoleId : int,
        RoleName : string,
        DedicatedAccountPermissionOverride : string, // can be null
        DedicatedToAppUserID : int, // can be null
        DedicatedToAppUserName : string, // can be null
        IsAdministratorGroup : bool,
        UserID : int,
        UserName : string,
        ManagedAccountId : int,
```

```
        AccountName : string,
        RationalizedSystemName : string,
        ApplicationName : string,
        AccessPolicyName : string
    }
]
```

GET Entitlements?groupIDs={groupID1,groupID2,groupID3…}

Purpose

Returns user entitlements for the specified group IDs.

Required Permissions

Analytics and Reporting (Read).

URL Parameters

groupIDs: Comma separated list of group IDs

Request Body

None.

Response Body

Content-Type: application/json

```
[
    {
        GroupID : int,
        Name : string,
        SmartRuleId : int,
        Title : string,
        SmartRuleType : string,
        AccessLevel : string, // can be null
        RoleId : int,
        RoleName : string,
        DedicatedAccountPermissionOverride : string, // can be null
        DedicatedToAppUserID : int, // can be null
        DedicatedToAppUserName : string, // can be null
        IsAdministratorGroup : bool,
        UserID : int,
        UserName : string,
```

```
        ManagedAccountId : int,
        AccountName : string,
        RationalizedSystemName : string,
        ApplicationName : string,
        AccessPolicyName : string
    }
]
```

Imports

POST Imports

Purpose

Queues a third-party import.

Required Permissions

Scan Management (Read/Write).

Request Body

Content-Type: application/json

```
{
    WorkgroupID: int,
    ImportType: string,
    Filter: string,
    FileName: string,
    FileContents: byte[],
    Base64FileContents: string
}
```

> ***Note:*** *Provide either* ***FileContents*** *or* ***Base64FileContents****.*

Request Body Details

- **WorkgroupID:** ID of the Workgroup to import the assets into
- **ImportType:** (case-senstitive, default: PASSWORDSAFE) Type of import being queued:
  - **PASSWORDSAFE:** Password Safe import file. Expected file extension: .xml.
  - **RETINARTD:** Retina© RTD file. Expected file extension: .rtd.

    > ***Note:*** *Support for the following file types has been deprecated and will be removed from the product in a future version.*
  - **NESSUS:** Nessus© import file. Expected file extension: .csv.
  - **NESSUSSECCEN:** NessusSecurityCenter© import file. Expected file extension: .csv.
  - **NEXPOSE:** Nexpose© import file. Expected file extension: .csv or .xml.
  - **QUALYSGUARD:** QualysGuard© file. Expected file extension: .csv or .xml.

  - **METASPLOIT:** METASPLOIT© import file. Expected file extension: .xml.
  - **MCAFEEVM:** McAfee Vulnerability Management© import file. Expected file extension: .csv.
  - **TRIPWIRE:** Tripwire© import file. Expected file extension: .csv.
- **Filter:** (default: All Assets) Asset selection filter:
  - All Assets: No filter, import all.
  - Single IPv4 address (i.e. 10.0.0.1).
  - IPv4 range (i.e. 10.0.0.1-10.0.0.5).
  - CIDR (i.e. 10.0.0.0/24).
- **FileName:** Filename (including extension) of the import file. One of the following is required:
  - **FileContents:** The array containing the content of the import file.
  - **Base64FileContents:** Base64 string containing the content of the import file.

Response Body

Content-Type: application/json

```
{
    ImportID: int
}
```

Response Codes

200 – Request successful. Import ID in the response body.

For more information, please see "Common Response Codes" on page 17.

Operating Systems

GET OperatingSystems

Purpose

Returns a list of operating systems.

Required Permissions

Asset Management (Read).

Request Body

None.

Response Body

Content-Type: application/json

```
[
    {
        OperatingSystemID : int,
        Name : string
    },
    …
]
```

Response Codes

200 – Request successful. Operating systems in the response body.

For more information, please see "Common Response Codes" on page 17.

Organizations

Quick Navigation

GET Organizations

Purpose

Returns a list of organizations to which the current user has permission.

Required Permissions

Asset Management (Read).

Request Body

None.

Response Body

Content-Type: application/json

```
[
    {
        OrganizationID : string,
        Name : string,
        IsActive : bool
    },
    …
]
```

Response Codes

200 – Request successful. Organizations in the response body.

> *For more information, please see "Common Response Codes" on page 17.*

GET Organizations/{id}

Purpose

Returns an organization by ID.

Required Permissions

- Current user has permission to the organization.
- Asset Management (Read).

URL Parameters

id: ID of the organization.

Request Body

None.

Response Body

Content-Type: application/json

```
{
    OrganizationID : string,
    Name : string,
    IsActive : bool
}
```

Response Codes

200 – Request successful. Organizations in the response body.

For more information, please see "Common Response Codes" on page 17.

GET Organizations?name={name}

Purpose

Returns an organization by name.

Required Permissions

- Current user has permission to the organization
- Asset Management (Read).

Query Parameters

name: Name of the organization.

Request Body

None.

Response Body

Content-Type: application/json

```
{
    OrganizationID : string,
    Name : string,
    IsActive : bool
}
```

Response Codes

200 – Request successful. Organizations in the response body.

For more information, please see "Common Response Codes" on page 17.

Permissions

(i.e., Asset Management, User Accounts Management, Scan Management, etc.)

Quick Navigation

GET Permissions

Purpose

Returns a list of permissions.

Required Permissions

User Accounts Management (Read).

Request Body

None.

Response Body

Content-Type: application/json

```
[
    {
        PermissionID : int,
        Name : string
    },
    …
]
```

Response Codes

200 – Request successful. Permissions in the response body.

For more information, please see "Common Response Codes" on page 17.

User Group Permissions

GET UserGroups/{userGroupID}/Permissions

Purpose

Gets all permissions for the user group referenced by ID.

Required Permissions

User Accounts Management (Read).

URL Parameters

userGroupId: ID of the user group.

Request Body

None.

Response Body

Content-Type: application/json

```
[
    {
        PermissionID : int,
        AccessLevelID : int
    },
…]
```

Response Codes

200 – Request successful. Permissions in the response body.

For more information, please see "Common Response Codes" on page 17.

POST UserGroups/{userGroupId}/Permissions

Purpose

Sets permissions for the user group referenced by ID.

Required Permissions

User Accounts Management (Read/Write).

> ***Note:***
> - *Adding the Secrets Safe feature/permission to a user group requires the caller to be an administrator.*
> - *The access level for Secrets Safe cannot be changed to disabled if the group has associated secrets.*

URL Parameters

userGroupId: ID of the user group.

Request Body

Content-Type: application/json

```
[
    {
        PermissionID : int,
        AccessLevelID : int
    },
    …
]
```

Response Body

None.

Response Codes

204 – Request successful. No content in body.

> *For more information, please see "Common Response Codes" on page 17.*

DELETE UserGroups/{userGroupId}/Permissions

Purpose

Deletes all permissions for the user group referenced by ID.

Required Permissions

User Accounts Management (Read/Write).

> ***Note:***
> - *Removing the Secrets Safe feature/permission from a user group requires the caller to be an administrator.*
> - *Permissions for a User Group that has the Secrets Safe feature enabled cannot be deleted if the group has associated secrets.*

URL Parameters

userGroupId: ID of the user group.

Request Body

None.

Response Body

None.

Response Codes

200 – Request successful.

> *For more information, please see "Common Response Codes" on page 17.*

Smart Rules

Quick Navigation

For more information on related topics, please see:

- *"Quick Rules" on page 364*
- *"Assets" on page 54*
- *"GET SmartRules/{id}/Assets" on page 71*
- *"Smart Rule Managed Accounts" on page 277*
- *"GET SmartRules/{smartRuleID}/ManagedAccounts" on page 277*
- *"GET QuickRules/{quickRuleID}/ManagedAccounts" on page 267*
- *"Managed Systems" on page 284*
- *"Smart Rule Managed Systems" on page 342*

GET SmartRules

Purpose

Returns a list of Smart Rules to which the current user has at least read access.

Query Parameters

type: (optional, default: all) Type of Smart Rules to return (all, managed account, managed system, and asset).

Request Body

None.

Response Body

Content-Type: application/json

```
[
    {
        SmartRuleID: int,
        OrganizationID : string, // can be null
        Title: string,
        Description: string,
        Category: string,
        Status: int,
        LastProcessedDate: datetime,
        IsReadOnly: bool,
        RuleType: string
    },
    …
]
```

Response Codes

200 – Request successful. Smart Rule in the response body.

For more information, please see "Common Response Codes" on page 17.

GET SmartRules/{id}

Purpose

Returns a Smart Rule by ID.

Required Permissions

Read access to the Smart Rule referenced by ID.

URL Parameters

id: ID of the Smart Rule.

Request Body

None.

Response Body

Content-Type: application/json

```
{
    SmartRuleID: int,
    OrganizationID : string, // can be null
    Title: string,
    Description: string,
    Category: string,
    Status: int,
    LastProcessedDate: datetime,
    IsReadOnly: bool,
    RuleType: string
}
```

Response Codes

200 – Request successful. Smart Rule in the response body.

For more information, please see "Common Response Codes" on page 17.

GET UserGroups/{id}/SmartRules/

Purpose

Returns a list of Smart Rules to which the given user group ID has at least read access.

Requirements

User Accounts Management (Read).

URL Parameters

id: ID of the user group.

Query Parameters

accessLevel: (optional, default: **1**,**3**) User group Smart Rule access level - A single value or comma-delimited list of values:

- **0:** None.
- **1:** Read.
- **3:** Read/Write.

Request Body

None.

Response Body

Content-Type: application/json

```
[{
    SmartRuleID: int,
    OrganizationID : string, // can be null
    Title: string,
    Description: string,
    Category: string,
    Status: int,
    LastProcessedDate: datetime,
    IsReadOnly: bool,
    RuleType: string,
    AccessLevelID: int,
}
,...
]
```

Response Codes

200 – Request successful. Smart Rules with user group access level in the response body.

GET SmartRules?title={title}

Purpose

Returns a Smart Rule by title.

In a multi-tenant environment, assumes global organization.

Required permissions

Read access to the Smart Rule referenced by title.

Query Parameters

title: Title of the Smart Rule.

Request Body

None.

Response Body

Content-Type: application/json

```
{
    SmartRuleID: int,
    OrganizationID : string, // can be null
    Title: string,
    Description: string,
    Category: string,
    Status: int,
    LastProcessedDate: datetime,
    IsReadOnly: bool,
    RuleType: string
}
```

Response Codes

200 – Request successful. Smart Rule in the response body.

For more information, please see "Common Response Codes" on page 17.

GET Organizations/{orgID}/SmartRules?title={title}

Purpose

Returns a Smart Rule by organization ID and title. This is only valid in a multi-tenant environment.

Required Permissions

Read access to the Smart Rule referenced by organization and title.

URL Parameters

orgID: ID of the organization.

Query Parameters

title: Title of the Smart Rule.

Request Body

None.

Response Body

Content-Type: application/json

```
{
    SmartRuleID: int,
    OrganizationID : string, // can be null
    Title: string,
    Description: string,
    Category: string,
    Status: int,
    LastProcessedDate: datetime,
    IsReadOnly: bool,
    RuleType: string
}
```

Response Codes

200 – Request successful. Smart Rule in the response body.

For more information, please see "Common Response Codes" on page 17.

POST SmartRules/FilterAssetAttribute

Purpose

Specialized action for creating an asset type Smart Rule for filtering assets by attributes.

Required Permissions

Asset Management (Read/Write).

Request Body

Content-Type: application/json

```
{
    AttributeIDs: [ int, …],
    Title: string,
    Category: string,
    Description: string,
    ProcessImmediately: bool
}
```

Request Body Details

- **AttributeIDs:** (required) A list of attribute IDs to filter by. All the attributes must be of the same attribute type.
- **Title:** (required) The title/name of the new Smart Rule. Must be unique across all Smart Rules. Max string length is 75.
- **Category:** (required) The category in which to place the Smart Rule. Max string length is 50.
- **Description:** (optional, default: <value of Title>) The Smart Rule description.
- **ProcessImmediately:** (optional, default: true) True to process the Smart Rule immediately, otherwise false to defer processing to the background Smart Rule processor.

Response Body

Content-Type: application/json

```
{
    SmartRuleID: int,
    OrganizationID : string, // can be null
    Title: string,
    Description: string,
    Category: string,
    Status: int,
    LastProcessedDate: datetime,
    IsReadOnly: bool
}
```

Response Codes

201 - Request successful. Smart Rule in response body.

For more information, please see "Common Response Codes" on page 17.

POST SmartRules/{id}/Process

Purpose

Process a Smart Rule by ID.

Required Permissions

Read/Write access to the Smart Rule.

URL Parameters

ID: ID of the Smart Rule.

Query Parameters

Queue: (default: false) True to queue the Smart Rule for processing; false to process the Smart Rule immediately.

Request Body

None.

Response Body

Content-Type: application/json

```
{
    SmartRuleID: int,
    OrganizationID : string, // can be null
    Title: string,
    Description: string,
    Category: string,
    Status: int,
    LastProcessedDate: datetime,
    IsReadOnly: bool,
    RuleType: string
}
```

Response Codes

- 200 – Request successful. Smart Rule in the response body.
- 409 – Conflict: the Smart Rule is currently processing.

For more information, please see "Common Response Codes" on page 17.

DELETE SmartRules/{id}

Purpose

Deletes a Smart Rule by ID.

Required Permissions

Read/Write access to the Smart Rule referenced by ID

URL Parameters

ID: ID of the Smart Rule.

Request Body

None.

Response Body

None.

Response Codes

200 – Request successful.

For more information, please see "Common Response Codes" on page 17.

DELETE SmartRules?title={title}

Purpose

Deletes a Smart Rule by title.

In a multi-tenant environment, assumes global organization.

Required Permissions

Read/Write access to the Smart Rule referenced by title.

Query Parameters

title: Title of the Smart Rule.

Request Body

None.

Response Body

None.

Response Codes

200 – Request successful.

For more information, please see "Common Response Codes" on page 17.

DELETE Organizations/{orgID}/SmartRules?title={title}

Purpose

Deletes a Smart Rule by organization ID and title.

Only valid in a multi-tenant environment.

Required permissions

Read/Write access to the Smart Rule referenced by organization and title.

URL Parameters

orgID: ID of the organization.

Query Parameters

title: Title of the Smart Rule.

Request Body

None.

Response Body

None.

Response Codes

200 – Request successful.

For more information, please see "Common Response Codes" on page 17.

Subscription Delivery (Cloud Only)

Quick Navigation

GET Subscriptions/Delivery

Purpose

Returns a list of IDs for all subscription deliveries that a user has access to. Administrators have access to all deliveries while other users only have access to deliveries they created.

Required Permissions

Analytics and Reporting (Read).

URL Parameters

None.

Request Body

None.

Response Body

Content-Type: application/json

```
[
    {
        int[]
    }
]
```

Response Body Details

A list of ints that reference the **ReportDeliveryId** field for every subscription delivery that the user has access to.

Response Codes

200 – Request successful. Ids in the response body.

For more information, please see "Common Response Codes" on page 17.

POST Subscriptions/Delivery/download?id={id}

Purpose

Returns the subscription delivery for the requested id.

Required Permissions

Analytics and Reporting (Read).

URL Parameters

id: ID of the request for which to retrieve the subscription delivery.

Request Body

None.

Response Body

Content-Type: application/json

```
[
  {
    ReportDeliveryId : int,
    ScheduleId : int,
    Filename : string,
    ApplicationType : string,
    Snapshot : string,
  }
]
```

Response Body Details

- **ReportDeliveryId:** The ID of this subscription delivery in the database.
- **ScheduleId:** Schedule ID of the subscription associated with this subscription delivery.
- **ApplicationType:** The MIME type string identifying the format of the file. Will be one of the following:
    - **application/msword** (Word)
    - **application/vnd.openxmlformats-officedocument.spreadsheetml.sheet** (Excel)

- **application/pdf** (Pdf)
- **image/tiff** (TIFF)
- **text/csv** (CSV)

- **Snapshot:** A Base64 string representing the byte array of the subscription delivery file itself.

Response Codes

200 – Request successful. Subscription delivery in the response body.

For more information, please see "Common Response Codes" on page 17.

User Groups

Quick Navigation

GET UserGroups

Purpose

Returns a list of active and inactive user groups.

Required Permissions

User Accounts Management (Read).

Request Body

None.

Response Body

Content-Type: application/json

```
[
    {
        GroupID : int,
        Name : string,
        DistinguishedName : string,
        Description : string,
        GroupType : string,
        AccountAttribute : string,
        ApplicationRegistrationIDs : string,
        MembershipAttribute : string,
        IsActive : bool
    },
    …
]
```

Response Codes

200 – Request successful. User group in the response body.

For more information, please see "Common Response Codes" on page 17.

GET UserGroups/{id}

Purpose

Returns a user group by ID.

Required Permissions

User Accounts Management (Read).

URL Parameters

id: ID of the user group.

Request Body

None.

Response Body

Content-Type: application/json

```
[
  {
    GroupID : int,
    Name : string,
    DistinguishedName : string,
    Description : string,
    GroupType : string,
    AccountAttribute : string,
    ApplicationRegistrationIDs : string,
    MembershipAttribute : string,
    IsActive : bool
  }
]
```

Response Codes

200 – Request successful. User group in the response body.

For more information, please see "Common Response Codes" on page 17.

GET UserGroups?name={name}

Purpose

Returns a user group by name.

Required Permissions

User Accounts Management (Read).

Query Parameters

name: Name of the user group.

Request Body

None.

Response Body

Content-Type: application/json

```
[
  {
    GroupID : int,
    Name : string,
    DistinguishedName : string,
    GroupType : string,
    AccountAttribute : string,
    ApplicationRegistrationIDs : string,
    MembershipAttribute : string,
    IsActive : bool
  }
]
```

Response Codes

200 – Request successful. User group in the response body.

For more information, please see "Common Response Codes" on page 17.

POST UserGroups

Purpose

Creates a new user group with permissions, and, optionally, Smart Rule access and application registration IDs.

Required Permissions

User Accounts Management (Read/Write).

> ***Note:*** *Creating a user group that has the Secrets Safe feature/permission enabled requires the caller to be an administrator.*

Request Body

The request body differs for the different group types available: **BeyondInsight**, **ActiveDirectory**, **LdapDirectory**.

BeyondInsight Group Type

Request Body

Content-Type: application/json

```
{
    groupType : string = "BeyondInsight",
    groupName : string,
    description : string,
    isActive : bool,
    Permissions : [ { PermissionID: int, AccessLevelID: int }, ... ],
    SmartRuleAccess : [ { SmartRuleID: int, AccessLevelID: int }, ... ],
    ApplicationRegistrationIDs: [ int, … ]
}
```

Request Body Details

- **groupName:** (required) Name of the BeyondInsight user group. Max string length is 200.
- **description:** (required) Description of the user group. Max string length is 255.

> *For more information, please see "Common Request Body Details" on page 125.*

ActiveDirectory Group Type

Request Body

Content-Type: application/json

```
{
    groupType : string = "ActiveDirectory",
    groupName : string,
    forestName : string,
    domainName : string,
    description : string,
    bindUser : string,
    bindPassword : string,
    useSSL : bool,
    isActive : bool,
    ExcludedFromGlobalSync : bool,
    OverrideGlobalSyncSettings : bool,
    Permissions : [ { PermissionID: int,
    AccessLevelID: int }, ... ],
    SmartRuleAccess : [ { SmartRuleID: int, AccessLevelID: int }, ... ],
    ApplicationRegistrationIDs: [ int, … ]
  }
```

Request Body Details

- **groupName:** (required) Name of the Active Directory group. Max string length is 200.
- **domainName:** (required) The directory domain name. Max string length is 250.
- **description:** (required) Description of the user group. Max string length is 255.
- **bindUser:** Username for directory binding. If not given, attempts to use existing credentials for the directory. If specifying an existing credential, you also need **Credential Management – Read**. If specifying a new credential, you also need **Credential Management – Read/Write**.
    - **bindPassword:** Password for directory binding (required if bindUser is given).
    - **forestName:** The directory forest name (required when bindUser is given). Max string length is 300.
- **useSSL:** (default: false) Flag indicating whether to use SSL.
- **ExcludedFromGlobalSync:** (default false) Flag indicating if the Active Directory group uses the global group synchronization settings.
- **OverrideGlobalSyncSettings:** (default false) Flag indicating if the Active Directory group overrides the global group synchronization settings.

For more information, please see "Common Request Body Details" on page 125.

LdapDirectory Group Type

Request Body

Content-Type: application/json

```
{
    groupType : string = "LdapDirectory",
    groupName : string,
    groupDistinguishedName : string,
    hostName : string,
    bindUser : string,
    bindPassword : string,
    port : int,
    useSSL : bool,
    membershipAttribute : string,
    accountAttribute : string,

    isActive : bool,
    Permissions : [ { PermissionID: int,
    AccessLevelID: int }, ... ],
    SmartRuleAccess : [ { SmartRuleID: int, AccessLevelID: int }, ... ],
    ApplicationRegistrationIDs: [ int, … ]
}
```

Request Body Details

- **groupName:** (required) Name of the LDAP group. Max string length is 200.
- **groupDistinguishedName:** (required) Distinguished name of the LDAP group. Max string length is 500.
- **hostName:** (required) The directory server host name or IP. Max string length is 50.
- **bindUser:** Username for directory binding. If not given, attempts to use existing credentials for the directory. If specifying an existing credential, you also need **Credential Management – Read**. If specifying a new credential, you also need **Credential Management – Read/Write**.
    - **bindPassword:** Password for directory binding (Note: required if bindUser is given).
    - **port:** Directory server port (valid range: 1 to 65535) (required if bindUser is given).
    - **useSSL:** (default: false) Flag indicating whether to use SSL (required if bindUser is given).
- **membershipAttribute:** (required) Directory group membership attribute. Max string length is 255.
- **accountAttribute:** (required) Directory account naming attribute. Max string length is 255.

For more information, please see "Common Request Body Details" on page 125.

Common Request Body Details

- **isActive:** (default: true) True if the group should be created as active, otherwise false.
- **Permissions:** One or more permissions and access levels to set for the new user group.

- **SmartRuleAccess:** One or more Smart Rules and access levels to set for the new user group.
- **ApplicationRegistrationIDs:** Zero or more IDs representing the API application registrations to grant the new user group. If given, enables API for the user group.

Response Body

Content-Type: application/json

```
[
  {
    GroupID : int, Name : string,
    DistinguishedName : string,
    Description : string,
    GroupType : string,
    AccountAttribute : string,
    MembershipAttribute : string,
    IsActive : bool
  }
]
```

Response Codes

201 – Request successful. User group in the response body.

For more information, please see "Common Response Codes" on page 17.

DELETE UserGroups/{id}

Purpose

Deletes a user group by ID.

Required Permissions

User Accounts Management (Read/Write).

Note:

- *Deleting a user group that has the Secrets Safe feature/permission enabled requires the caller to be an administrator.*
- *User Groups that have the Secrets Safe feature enabled cannot be deleted if the group has associated secrets.*

URL Parameters

id: ID of the user group.

Request Body

None.

Response Body

None.

Response Codes

200 – Request successful.

For more information, please see "Common Response Codes" on page 17.

DELETE UserGroups?name={name}

Purpose

Deletes a user group by name.

Required Permissions

User Accounts Management (Read/Write).

***Note:** Deleting a user group that has the Secrets Safe feature/permission enabled requires the caller to be an administrator.*

Query Parameters

name: Name of the user group.

Request Body

None.

Response Body

None.

Response Codes

200 – Request successful.

For more information, please see "Common Response Codes" on page 17.

User Group Memberships

Quick Navigation

GET Users/{userID}/UserGroups

Purpose

Returns the user group memberships for an existing user.

Required Permissions

User Accounts Management (Read).

URL Parameters

userID: ID of the user.

Request Body

None.

Response Body

Content-Type: application/json

```
[
    {
        GroupID : int,
        Name : string,
        DistinguishedName : string,
        GroupType : string,
        AccountAttribute : string,
        MembershipAttribute : string,
        IsActive : bool
    },
    …
]
```

Response Codes

200 – Request successful. User group in the response body.

For more information, please see "Common Response Codes" on page 17.

POST Users/{userID}/UserGroups/{userGroupID}

Purpose

Adds an existing user to a user group.

Required Permissions

User Accounts Management (Read/Write).

URL Parameters

- **userID:** ID of the user.
- **userGroupID:** ID of the user group.

Request Body

None.

Response Body

Content-Type: application/json

```
{
    GroupID : int, Name : string,
    DistinguishedName : string,
    GroupType : string,
    AccountAttribute : string,
    MembershipAttribute : string,
    IsActive : bool
}
```

Response Codes

201 – Request successful. User group in the response body.

For more information, please see "Common Response Codes" on page 17.

DELETE Users/{userID}/UserGroups/{userGroupID}

Purpose

Removes a user from a user group.

Required Permissions

User Accounts Management (Read/Write).

URL Parameters

- **userID:** ID of the user.
- **userGroupID:** ID of the user group.

Request Body

None.

Response Codes

200 – Request successful.

For more information, please see "Common Response Codes" on page 17.

User Audits

GET UserAudits

Purpose

Returns a list of user audits.

Required Permissions

User Audit Management (Read).

Query Parameters (Optional)

- **username:** User name.
- **actiontype:** Action type.
- **section:** Section.
- **startdate:** Start date.
- **enddate:** End date.
- **limit:** (default: 1000) Number of records to return.
- **offset:** (default: 0) Number of records to skip before returning records.

Request Body

None.

Response Body

Content-Type: application/json

```
{
    TotalCount : int,
    Data: [
    {
    AuditID : int,
    ActionType : string,
    Section : string,
    UserID : int,
    UserName : string,
    IPAddress : string,
    CreateDate : datetime
    },
    ...
```

```
    ]
}
```

Response Codes

200 – Request successful. User Audits in response body.

Default Sort

By default the records are sorted by **CreateDate** in descending order (latest entries are shown first)

GET UserAudits/{auditId:int}/UserAuditDetails

Purpose

Returns a list of user audit details.

Required Permissions

User Audit Management (Read).

Query Parameters

- **auditid:** Audit ID
- **limit:** (default: 1000) Number of records to return.
- **offset:** (default: 0) Number of records to skip before returning records.

Request Body

None.

Response Body

Content-Type: application/json

```
{
    TotalCount: int,
    Data: [
    {
    AuditDetailsID : int,
    Name: string,
    OldValue : string,
    NewValue : string
```

```
        },
        ...
        ]
}
```

Users

Quick Navigation

GET Users

Purpose

Returns a list of all users if username parameter is not supplied. Otherwise returns the requested user.

> ***Note:*** *Some usernames may be in the format* ***hostname\username****, if not represented by an email address.*

Required Permissions

User Accounts Management (Read).

Query Parameters (Optional)

username: The user to return, in one of following formats:

- **username**: returns the BeyondInsight users.
- **domain\username** or universal principal name: returns Active Directory or LDAP users.

> ***Note:*** *A* ***username*** *search without a domain finds local users; if domain is added to the search, it finds the user for a given domain.*

> ***Note:*** *Use of the optional query parameters results in the supplied value being recorded in the web server log file.*

Request Body

None.

Response Body

Content-Type: application/json

```
[
    {
        UserID : int,
        UserName : string,
        DomainName : string,
        DistinguishedName : string,
        FirstName : string,
        LastName : string,
        EmailAddress : string,
        LastLoginDate : DateTime,
        LastLoginAuthenticationType : string,
        LastLoginConfigurationName : string,
        LastLoginSAMLIDPURL : string,
        LastLoginSSOURL : string,
        IsQuarantined: bool
    },
    …
]
```

Application User Type:

> ***Note: ClientSecret*** *has no value; it can only be retrieved via API by initial creation or recycling it. Please see* *"Users" on page 135**.*

```
{
    ClientID: string,
    ClientSecret: string = null,
    AccessPolicyID: int,
    UserID: int,
    UserType: string = "Application",
    UserName: string,
    DomainName: string = null,
    DistinguishedName: string = null,
    FirstName: string = null,
    LastName: string = null,
    EmailAddress: string = null,
    IsQuarantined: bool
}
```

Response Codes

200 – Request successful. Users in the response body.

For more information, please see "Common Response Codes" on page 17.

GET UserGroups/{userGroupId}/Users

Purpose

Returns a list of users for the user group referenced by ID.

***Note:** For Active Directory, Entra ID, or LDAP user groups, calling this endpoint also triggers the membership synchronization between the directory and BeyondInsight for the group identified by **userGroupId**.*

Required Permissions

User Accounts Management (Read).

URL Parameters

userGroupId: ID of the user group.

Request Body

None.

Response Body

Content-Type: application/json

```
[
    {
        UserID : int,
        UserName : string,
        DomainName : string,
        DistinguishedName : string,
        FirstName : string,
        LastName : string,
        EmailAddress : string,
        LastLoginDate : DateTime,
        LastLoginAuthenticationType : string,
        LastLoginConfigurationName : string,
        LastLoginSAMLIDPURL : string,
```

```
        LastLoginSSOURL : string,
        IsQuarantined: bool
    },
    …
]
```

Response Codes

200 – Request successful. Users in the response body.

> *For more information, please see "Common Response Codes" on page 17.*

GET Users/{id}

Purpose

Returns a user by ID.

Required Permissions

User Accounts Management (Read).

URL Parameters

id: ID of the user.

Request Body

None.

Response Body

Content-Type: application/json

```
[
  {
    UserID : int,
    UserName : string,
    DomainName : string,
    DistinguishedName : string,
    FirstName : string,
    LastName : string,
    EmailAddress : string,
    LastLoginDate : DateTime,
```

```
    LastLoginAuthenticationType : string,
    LastLoginConfigurationName : string,
    LastLoginSAMLIDPURL : string,
    LastLoginSSOURL : string,
    IsQuarantined: bool
  }
]
```

Application User Type

> ***Note: ClientSecret*** *has no value; it can only be retrieved via API by initial creation or recycling it. Please see* *"Users" on page 135**.*

```
{
    ClientID: string,
    ClientSecret: string = null,
    AccessPolicyID: int,
    UserID: int,
    UserType: string = "Application",
    UserName: string,
    DomainName: string = null,
    DistinguishedName: string = null,
    FirstName: string = null,
    LastName: string = null,
    EmailAddress: string = null,
    IsQuarantined: bool
}
```

Response Codes

200 – Request successful. User in the response body.

> *For more information, please see* *"Common Response Codes" on page 17**.*

POST Users

Purpose

Creates a new user with no user group associations.

Required Permissions

User Accounts Management (Read/Write).

Request Body

The request body differs for the different user types available: **BeyondInsight**, **ActiveDirectory**, **LdapDirectory**

BeyondInsight User Type

Content-Type: application/json

```
{
    UserType : string = "BeyondInsight",
    UserName : string,
    FirstName : string,
    LastName : string,
    EmailAddress : string,
    Password : string
}
```

Request Body Details

- **UserName:** (required) Username of the user account. Max string length is 64.
- **FirstName:** (required) First name of the user. Max string length is 64.
- **LastName:** (optional) Last name of the user. Max string length is 64.
- **EmailAddress:** (required must be a properly formatted address) - Email address for the user. Max string length is 255.
- **Password:** (required) The password they would use to login to BeyondInsight.

ActiveDirectory User Type

Content-Type: application/json

```
{
    UserType : string = "ActiveDirectory",
    UserName : string,
    ForestName : string,
    DomainName : string,
    BindUser : string,
    BindPassword : string,
    UseSSL : bool,
}
```

Request Body Details

- **UserName:** (required) Name of the Active Directory user. Max string length is 64.
- **DomainName:** (required) The directory domain name. Max string length is 250.

- **BindUser:** Username for directory binding. If not given, attempts to use existing credentials for the directory.
    - **BindPassword:** Password for directory binding (required when BindUser is given).
    - **ForestName:** The directory forest name (required when BindUser is given). Max string length is 300.
- **UseSSL:** (default: false) Flag indicating whether to use SSL.

LdapDirectory User Type

Content-Type: application/json

```
{
    UserType: string = "LdapDirectory",
    HostName: string,
    DistinguishedName: string,
    AccountNameAttribute: string,
    BindUser: string,
    BindPassword: string,
    Port: int,
    UseSSL: bool
}
```

Request Body Details

- **HostName:** (required) The directory server host name or IP.
- **DistinguishedName:** (required) The DistinguishedName of the user to create. Max string length is 255.
- **AccountNameAttribute:** (required) The LDAP attribute to use for creating the username.
- **BindUser:** Username for directory binding. If not given, attempts to use existing credentials for the directory.
    - **BindPassword:** Password for directory binding. (required if BindUser is given).
    - **Port:** The directory server port. (used when BindUser and BindPassword are given).
    - **UseSSL:** Flag indicating whether to use SSL (used when BindUser and BindPassword are given).

Application User Type

```
{
    UserType: string = "Application",
    UserName: string,
    AccessPolicyID: int
}
```

For more information, please see "Common Request Body Details" on page 125.

Response Body

Content-Type: application/json

```
[
  {
    UserID : int,
    UserName : string,
    DomainName : string,
    DistinguishedName : string,
    FirstName : string,
    LastName : string,
    EmailAddress : string,
    IsQuarantined: bool
  }
]
```

Application User Type

```
{
    ClientID: string,
    ClientSecret: string,
    AccessPolicyID: int,
    UserID: int,
    UserType: string = "Application",
    UserName: string,
    DomainName: string = null,
    DistinguishedName: string = null,
    FirstName: string = null,
    LastName: string = null,
    EmailAddress: string = null,
    IsQuarantined: bool
}
```

Response Codes

200 – Request successful. User in the response body.

For more information, please see "Common Response Codes" on page 17.

POST Users/{id}/Quarantine

Purpose

Quarantines the user referenced by ID.

Required Permissions

Password Safe API Global Quarantine (Read/Write).

URL Parameters

id: ID of the BeyondInsight user.

Request Body

None.

Response Body

Content- Type: application/json

```
[
  {
    UserID : int,
    UserName : string,
    DomainName : string,
    DistinguishedName : string,
    FirstName : string,
    LastName : string,
    EmailAddress : string,
    IsQuarantined: bool
  }
]
```

Response Codes

200 – Request successful. User in the response body.

For more information, please see "Common Response Codes" on page 17.

POST UserGroups/{userGroupId}/Users

Purpose

Creates a user in a BeyondInsight-type user group.

Required Permissions

User Accounts Management (Read/Write).

URL Parameters

userGroupId: ID of the user group.

Request Body

Content-Type: application/json

```
{
    UserName : string,
    FirstName : string,
    LastName : string,
    EmailAddress : string,
    Password : string
}
```

Request Body Details

- **UserName:** (required) Username of the user account. Max string length is 64.
- **FirstName:** (required) First name of the user. Max string length is 64.
- **LastName:** (optional) Last name of the user. Max string length is 64.
- **EmailAddress:** (required and must be a properly formatted address) Email address for the user. Max string length is 255.
- **Password:** (required) The password they would use to login to BeyondInsight.

Response Body

Content-Type: application/json

```
[
  {
    UserID : int,
    UserName : string,
    DomainName : string,
    DistinguishedName : string,
    FirstName : string,
    LastName : string,
    EmailAddress : string,
    IsQuarantined: bool
  }
]
```

Response Codes

201 – Request successful. User in the response body.

For more information, please see "Common Response Codes" on page 17.

POST/{id}/Users/{id}/RecycleClientSecret

> **Note:** *For application user type only.*

Purpose

Recycles the client secret for an application user.

Required Permissions

User Accounts Management (Read/Write) or logged in as the user being affected.

Request Body

None.

Response Body

Content- Type: application/json

```
string
```

Response Codes

200 – Request successful. New client secret in the body.

> *For more information, please see "Common Response Codes" on page 17.*

PUT Users/{id}

Purpose

Updates a BeyondInsight user by ID.

> **Note:** *Cannot update ActiveDirectory or LDAP users.*

Required Permissions

User Accounts Management (Read/Write).

URL Parameters

id: ID of the BeyondInsight user.

Request Body

Content-Type application/json

```
{
    UserName : string,
    FirstName : string,
    LastName : string,
    EmailAddress : string,
    Password: string
}
```

Request Body Details

- **UserName:** (required) Username of the user account.
- **FirstName:** (required) First name of the user.
- **LastName:** (optional) Last name of the user.
- **EmailAddress:** (required and must be a properly formatted address) Email address for the user.
- **Password:** (optional) The password they would use to log in to BeyondInsight. If given, replaces the current password.

Application User Type

```
{
    UserName: string,
    AccessPolicyID: int
}
```

Response Body

Content- Type: application/json

```
[
  {
    UserID : int,
    UserName : string,
    DomainName : string,
    DistinguishedName : string,
    FirstName : string,
    LastName : string,
    EmailAddress : string,
    IsQuarantined: bool
```

```
  }
]
```

Application User Type

> **Note: ClientSecret** *has no value; it can only be retrieved via API by initial creation or recycling it. Please see* *"Users" on page 135*.

```
{
    ClientID: string,
    ClientSecret: string = null,
    AccessPolicyID: int,
    UserID: int,
    UserType: string = "Application",
    UserName: string,
    DomainName: string = null,
    DistinguishedName: string = null,
    FirstName: string = null,
    LastName: string = null,
    EmailAddress: string = null,
    IsQuarantined: bool
}
```

Response Codes

200 – Request successful. User in the response body.

> *For more information, please see* *"Common Response Codes" on page 17*.

DELETE Users/{id}

Purpose

Deletes a user by ID.

Required Permissions

User Accounts Management (Read/Write).

> ***Note:***
> - *Users that have the Secrets Safe feature enabled* ***cannot*** *be deleted if that user is the* ***only*** *owner of at least one secret.*

- *If the user is not the sole owner of any secrets, but is one of multiple owners of a secret, then no error will be presented and the user can be deleted successfully. They will also be removed from the secrets they are part owners to.*

URL Parameters

id: ID of the user.

Request Body

None.

Response Codes

200 – Request successful.

For more information, please see "Common Response Codes" on page 17.

Workgroups

Quick Navigation

GET Workgroups

Purpose

Returns a list of Workgroups to which the current user has permission.

Request Body

None.

Response Body

Content-Type: application/json

```
[
    {
        OrganizationID : string, ID : int,
        Name : string
    },
    …
]
```

Response Codes

200 – Request successful. Workgroups in the response body.

> *For more information, please see "Common Response Codes" on page 17.*

GET Workgroups/{id}

Purpose

Returns a Workgroup by ID.

Required Permissions

- Current user has permission to the Workgroup Organization.
- Asset Management (Read) or Scan Management (Read/Write).

Query Parameters

id: ID of the Workgroup.

Request Body

None.

Response Body

Content-Type: application/json

```
{
    OrganizationID : string,
    ID : int,
    Name : string
}
```

Response Codes

200 – Request successful. Workgroups in the response body.

For more information, please see "Common Response Codes" on page 17.

GET Workgroups?name={name}

Purpose

Returns a Workgroup by name.

Required Permissions

Current user has permission to the Workgroup Organization. Asset Management (Read) or Scan Management (Read/Write).

Query Parameters

name: Name of the Workgroup.

Request Body

None.

Response Body

Content-Type: application/json

```
{
    OrganizationID : string,
    ID : int,
    Name : string
}
```

Response Codes

200 – Request successful. Workgroups in the response body.

For more information, please see "Common Response Codes" on page 17.

POST Workgroups

Purpose

Creates a Workgroup.

Required Permissions

Asset Management (Read/Write).

Request Body

Content-Type: application/json

```
{
    OrganizationID: string,
    Name : string
}
```

Request Body Details

- **Organization ID:** (optional) The ID of the organization in which to place the new Workgroup. If empty, the Workgroup is placed in the default organization.
- **Name:** The name of the Workgroup. Max string length is 256.

Response Body

Content-Type: application/json

```
{
    OrganizationID : string,
    ID : int,
    Name : string
}
```

Response Codes

201 – Request successful. Workgroups in the response body.

For more information, please see "Common Response Codes" on page 17.

Deprecated

The content in this section of the guide has been deprecated and is compatible with earlier versions only.

Quick Navigation

Imports

[deprecated] POST Imports/QueueImportFile

> ***Note:*** *This API has been deprecated and is available for backwards compatibility only. Use* ***POST Imports with Base64FileContents*** *instead.*

Purpose

Queues a Password Safe XML import using multi-part form-data content.

Required Permissions

Scan Management (Read/Write).

Request Body

Content-Type: multipart/form-data

```
{
    Content-type: application/json
    {
        WorkgroupID: int,
        FileName: string
    }
    application/octet-stream
    {
        <string-encoded byte array representing the file>
    }
}
```

Request Body Details

- **WorkgroupID:** ID of the Workgroup to import the assets into.
- **FileName:** Filename (including extension) of the import file.

Response Body

Content-Type: application/json

```
{
    ImportID: int
}
```

Response Codes

- 200 – Request successful. Import ID in the response body.
- 400 – The import file was not found in the body of the request, or a request body validation error has occurred.

Smart Rules

[deprecated] POST SmartRules/FilterSingleAccount

> ***Note:*** *This API has been deprecated and is available for backwards compatibility only. Use* ***QuickRules*** *instead.*

Purpose

Specialized action for creating a Managed Account-type Smart Rule for filtering a single Managed Account by System Name and Account Name.

Required Permissions

Smart Rule Management - Managed Account (Read/Write).

Request Body

Content-type: application/json

```
{
    AccountID: int,
    Title: string
}
```

Request Body Details

- **AccountID:** (required) ID of the managed account you want to filter by parent System Name and Account Name.
- **Title:** (optional) The title/name of the new Smart Rule. If omitted, a unique title is auto-generated.

Response Body

Content-Type: application/json

```
{
    SmartRuleID: int,
    OrganizationID : string, // can be null
    Title: string,
    Description: string,
    Category: string,
    Status: int,
    LastProcessedDate: datetime,
    IsReadOnly: bool,
    RuleType: string
}
```

Response Codes

201 – Request successful. Smart Rule in the response body.

User Groups

[deprecated] GET UserGroups/{name}

> ***Note:*** *This API has been deprecated and is available for backwards compatibility only. Use* ***GET UserGroups?name={name}*** *instead.*

Purpose

Returns a user group by name.

Required Permissions

User Accounts Management (Read).

URL Parameters

name: Name of the user group.

Request Body

None.

Response Body

Content-Type: application/json

```
{
    GroupID : int, Name : string,
    DistinguishedName : string,
    GroupType : string,
    AccountAttribute : string,
    MembershipAttribute : string,
    IsActive : bool
}
```

Response Codes

200 – Request successful. User group in the response body.

[deprecated] DELETE UserGroups/{name}

> ***Note:*** *This API has been deprecated and is available for backwards compatibility only.* ***Use DELETE UserGroups?name={name}*** *instead.*

Purpose

Deletes a user group by name.

Required Permissions

User Accounts Management (Read/Write).

URL Parameters

name: Name of the user group.

Request Body

None.

Response Body

None.

Response Codes

200 – Request successful.

Workgroups

[deprecated] GET Workgroups/{name}

> ***Note:*** *This API has been deprecated and is available for backwards compatibility only. Use* ***GET Workgroups?name={name}*** *instead.*

Purpose

Returns a Workgroup by name.

Required Permissions

Current user has permission to the Workgroup Organization. Asset Management (Read) or Scan Management (Read/Write).

Query Parameters

name: Name of the Workgroup.

Request Body

None.

Response Body

Content-Type: application/json

```
{
    OrganizationID : string,
    ID : int,
    Name : string
}
```

Response Codes

200 – Request successful. Workgroups in the response body.

Password Safe APIs

The Password Safe APIs require a valid Password Safe license.

Access Policies

Quick Navigation

GET AccessPolicies

Purpose

Returns a list of Password Safe access policies.

Required Permissions

Password Safe Role Management (Read).

Request Body

None.

Response Body

Content-Type: application/json

```
[
    {
        AccessPolicyID:int,
        Name:string,
        Description:string,
        Schedules :
        [
            {
                ScheduleID : int,
                RequireReason : bool,
                RequireTicketSystem : bool,
                TicketSystemID : short?,
                AccessTypes :
                [
                    {
                        AccessType : string,
                        IsSession : bool,
                        RecordSession : bool,
                        MinApprovers : int,
                        MaxConcurrent : int
                    },
```

```
                    …
                ]
            },
            …
        ]
    },
    …
]
```

Response Codes

200 - Request successful. Access policies in response body.

For more information, please see "Common Response Codes" on page 17.

POST AccessPolicies/Test

Purpose

Tests access to a managed account and returns a list of Password Safe access policies that are available in the request window.

Required Roles

Requestor role.

Request Body

Content-Type: application/json

```
{
    SystemId: int,
    AccountId: int,
    DurationMinutes : int
}
```

Response Body

Content-Type: application/json

```
[
    {
        AccessPolicyID:int,
        Name:string,
        Description:string,
```

```
        Schedules :
        [
            {
                ScheduleID : int,
                RequireReason : bool,
                RequireTicketSystem : bool,
                TicketSystemID : short?,
                AccessTypes :
                [
                    {
                        AccessType : string,
                        IsSession : bool,
                        RecordSession : bool,
                        MinApprovers : int,
                        MaxConcurrent : int
                    },
                    …
                ]
            },
            …
        ]
    },
    …
]
```

Response Codes

- 200 - Request successful. Access policies in response body.
- 403 - User does not have permissions to request the indicated account or the account does not have API access enabled. Response body contains a status code indicating the reason for this forbidden access:
    - 4031 - User does not have permission to request the account or the account is not valid for the system.

For more information, please see "Common Response Codes" on page 17.

Aliases

Quick Navigation

GET Aliases

Purpose

Returns a list of requestable managed account aliases.

Required Roles

Requestor or Requestor/Approver role for the preferred managed account referenced by the alias.

Query Parameters

- **state** (optional, default: **1**, **2**): Zero or more state values, i.e., **'state=2'**, **'state=1,2'**, **'state=0,1,2'**.
    - **0:** Unmapped
    - **1:** Mapped
    - **2:** Highly Available

> ***Note:*** *Only Aliases with a mapped* ***state*** *of* ***1*** *or* ***2*** *can be used for API* ***POST Aliases/{id}/Requests****.*

Request Body

None.

Response Body

Content-Type: application/json

```
[
    {
        AliasId: int,
        AliasName: string,
        AliasState: int,
```

```
        SystemId: int,
        SystemName: string,
        AccountId: int,
        AccountName: string,
        DomainName: string,
        InstanceName: string,
        DefaultReleaseDuration: int,
        MaximumReleaseDuration: int,
        LastChangeDate: datetime,
        NextChangeDate: datetime,
        IsChanging: bool,
        ChangeState: int,

        MappedAccounts :
        [
            {
                AliasID: int,
                ManagedSystemID: int,
                ManagedAccountID: int,
                Status: string
            },
            …
        ]
    }
    …
]
```

Response Codes

200 - Request successful. Aliases in response body.

For more information, please see "Common Response Codes" on page 17.

GET Aliases/{id}

Purpose

Returns a requestable managed account alias by ID.

Required Roles

Requestor or Requestor/Approver role for the preferred managed account referenced by the alias.

URL Parameters

id: ID of the managed account alias.

Request Body

None.

Response Body

Content-Type: application/json

```
{
    AliasId: int,
    AliasName: string,
    AliasState: int,
    SystemId: int,
    SystemName: string,
    AccountId: int,
    AccountName: string,
    DomainName: string,
    InstanceName: string,
    DefaultReleaseDuration: int,
    MaximumReleaseDuration: int,
    LastChangeDate: datetime,
    NextChangeDate: datetime,
    IsChanging: bool,
    ChangeState: int,

    MappedAccounts :
    [
        {
            AliasID: int,
            ManagedSystemID: int,
            ManagedAccountID: int,
            Status: string
        },
        …
    ]
}
```

Response Codes

200 - Request successful. Alias in response body.

For more information, please see "Common Response Codes" on page 17.

GET Aliases?name={name}

Purpose

Returns a requestable managed account alias by name.

Required Roles

Requestor or Requestor/Approver role for the preferred managed account referenced by the alias.

URL Parameters

name: Name of the managed account alias.

Request Body

None.

Response Body

Content-Type: application/json

```
{
    AliasId: int,
    AliasName: string,
    AliasState: int,
    SystemId: int,
    SystemName: string,
    AccountId: int,
    AccountName: string,
    DomainName: string,
    InstanceName: string,
    DefaultReleaseDuration: int,
    MaximumReleaseDuration: int,
    LastChangeDate: datetime,
    NextChangeDate: datetime,
    IsChanging: bool,
    ChangeState: int,

    MappedAccounts :
    [
        {
            AliasID: int,
            ManagedSystemID: int,
            ManagedAccountID: int,
            Status: string
        },
        …
    ]
}
```

Response Codes

200 - Request successful. Alias in response body.

For more information, please see "Common Response Codes" on page 17.

Applications

Quick Navigation

GET Applications

Purpose

Returns a list of applications.

Required Permissions

Password Safe Account Management (Read).

Request Body

None.

Response Body

Content-Type: application/json

```
[
    {
        ApplicationID : int,
        Name : string,
        DisplayName : string,
        Version : string,
        Command : string,
        Parameters : string,
        Publisher : string,
        ApplicationType : string,
        FunctionalAccountID : int, // can be null
        ManagedSystemID : int, // can be null
        IsActive : bool,
     SmartRuleID : int // can be null
    }
    …
]
```

Response Codes

200 - Request successful. Applications in response body.

For more information, please see "Common Response Codes" on page 17.

GET Applications/{id}

Purpose

Returns an application by ID.

Required Permissions

Password Safe Account Management (Read).

URL Parameters

id: ID of the application.

Request Body

None.

Response Body

Content-Type: application/json

```
{
    ApplicationID : int,
    Name : string,
    DisplayName : string,
    Version : string,
    Command : string,
    Parameters : string,
    Publisher : string,
    ApplicationType : string,
    FunctionalAccountID : int, // can be null
    ManagedSystemID : int, // can be null
    IsActive : bool,
    SmartRuleID : int // can be null
}
```

Response Codes

200 - Request successful. Application in response body.

For more information, please see "Common Response Codes" on page 17.

Attributes

Quick Navigation

GET ManagedAccounts/{managedAccountID}/Attributes

Purpose

Returns a list of attributes by managed account ID.

Required Permissions

Password Safe Account Management (Read), Attribute Management (Read).

URL Parameters

managedAccountID: ID of the managed account.

Request Body

None.

Response Body

Content-Type: application/json

```
[
    {
        AttributeID : int,
        AttributeTypeID : int,
        ParentAttributeID : int, // can be null
        ShortName : string,
        LongName : string,
```

```
        Description : string, ValueInt : int, // can be null
        IsReadOnly: bool
    },
    …
]
```

Response Codes

201 - Request successful. Attributes associated with the asset in the response body.

For more information, please see "Common Response Codes" on page 17.

GET ManagedSystems/{managedSystemID}/Attributes

Purpose

Returns a list of attributes by managed system ID.

Required Permissions

Password Safe System Management (Read), Attribute Management (Read).

URL Parameters

managedSystemID: ID of the managed system.

Request Body

None.

Response Body

Content-Type: application/json

```
[
    {
        AttributeID : int,
        AttributeTypeID : int,
        ParentAttributeID : int, // can be null
        ShortName : string,
        LongName : string,
        Description : string,
        ValueInt : int, // can be null
        IsReadOnly: bool
```

```
    },
…
]
```

Response Codes

200 - Request successful. Attributes associated with the Managed System in the response body.

> *For more information, please see "Common Response Codes" on page 17.*

POST ManagedAccounts/{managedAccountID}/Attributes/{attributeID}

Purpose

Assigns an attribute to a managed account.

Required Permissions

Password Safe Account Management (Read/Write), Attribute Management (Read/Write).

URL Parameters

- **managedAccountID:** ID of the managed account.
- **attributeID:** ID of the attribute.

Request Body

None.

Response Body

Content-Type: application/json

```
[
    {
        AttributeID : int,
        AttributeTypeID : int,
        ParentAttributeID : int, // can be null
        ShortName : string,
        LongName : string,
        Description : string, ValueInt : int, // can be null
        IsReadOnly: bool
    },
```

```
    ...
]
```

Response Codes

201 - Request successful. Attribute in the response body.

> *For more information, please see "Common Response Codes" on page 17.*

POST ManagedSystems/{managedSystemID}/Attributes/{attributeID}

Purpose

Assigns an attribute to a managed system.

Required Permissions

Password Safe System Management (Read/Write), Attribute Management (Read/Write).

URL Parameters

managedSystemID: ID of the managed system.

attributeID: ID of the attribute.

Request Body

None.

Response Body

Content-Type: application/json

```
[
    {
        AttributeID : int,
        AttributeTypeID : int,
        ParentAttributeID : int, // can be null
        ShortName : string,
        LongName : string,
        Description : string,
        ValueInt : int, // can be null
        IsReadOnly: bool
    },
```

```
    ...
]
```

Response Codes

201 - Request successful. Attribute in the response body.

For more information, please see "Common Response Codes" on page 17.

DELETE ManagedAccounts/{managedAccountID}/Attributes

Purpose

Deletes all managed account attributes by managed account ID.

Required Permissions

Password Safe Account Management (Read/Write), Attribute Management (Read/Write).

URL Parameters

managedAccountID: ID of the managed account.

Request Body

None.

Response Body

None.

Response Codes

200 - Request successful.

For more information, please see "Common Response Codes" on page 17.

DELETE ManagedAccounts/{managedAccountID}/Attributes/{attributeID}

Purpose

Deletes a managed account attribute by managed account ID and attribute ID.

Required Permissions

Password Safe Account Management (Read/Write), Attribute Management (Read/Write).

URL Parameters

- **managedAccountID:** ID of the managed account.
- **attributeID:** ID of the attribute.

Request Body

None.

Response Body

None.

Response Codes

200 - Request successful.

For more information, please see "Common Response Codes" on page 17.

DELETE ManagedSystems/{managedSystemID}/Attributes

Purpose

Deletes all managed system attributes by managed system ID.

Required Permissions

Password Safe System Management (Read/Write), Attribute Management (Read/Write).

URL Parameters

managedSystemID: ID of the managed system.

Request Body

None.

Response Body

None.

Response Codes

200 - Request successful.

For more information, please see "Common Response Codes" on page 17.

DELETE ManagedSystems/{managedSystemID}/Attributes/{attributeID}

Purpose

Deletes a managed system attribute by managed system ID and attribute ID.

Required Permissions

Password Safe System Management (Read/Write), Attribute Management (Read/Write).

URL Parameters

managedSystemID: ID of the managed system.

attributeID: ID of the attribute.

Request Body

None.

Response Body

None.

Response Codes

200 - Request successful.

For more information, please see "Common Response Codes" on page 17.

Credentials

Quick Navigation

For more information on related topics, please see:

- *"Requests" on page 376*
- *"Aliases" on page 163*
- *"Managed Accounts" on page 225*

GET Credentials/{requestId}

Purpose

Retrieves the credentials for an approved and active (not expired) credentials release request.

Required Permissions

None.

URL Parameters

requestId: ID of the request for which to retrieve the credentials.

Query Parameters

- **type:** (optional, default: password) Type of credentials to retrieve.
  - **password:** Returns the password in the response body.
  - **dsskey:** Returns the DSS private key in the response body.

Note: *The key is returned in the state in which it was set. For example, an encrypted key is returned encrypted.*

  - **passphrase:** Returns the DSS key passphrase in the response body.

Note: passphrase *supported only for encrypted DSS keys.*

Request Body

None.

Response Body

```
Credentials: string
```

Response Codes

- 200 - Request successful. Credentials in the response body.
- 403 - User does not have permissions to request credentials for the indicated account or the account does not have API access enabled.
    - 4031 - User does not have permission to request credentials. 4034 - Request is not yet approved.
- 404 - Could not find the request to release. The specified request ID may have already been released or has expired.

For more information, please see "Common Response Codes" on page 17.

GET Aliases/{aliasId}/Credentials/{requestId}

Purpose

Retrieves the credentials and alias details for an approved and active (not expired) credentials release request for an alias.

Required Permissions

None.

URL Parameters

- **aliasId:** ID of the alias.
- **requestId:** ID of the request for which to retrieve the credentials.

Query Parameters

- **type:** (optional, default: password) Type of credentials to retrieve.
- **password:** Returns the password in response body property **Password**.
- **dsskey:** Returns the DSS private key in response body property **PrivateKey**.

> **Note:** *The key is returned in the state in which it was set. For example, an encrypted key is returned encrypted.*

- **passphrase:** returns the DSS key passphrase in response body property **Passphrase**.

> ***Note: passphrase** supported only for encrypted DSS keys.*

Request Body

None.

Response Body

Content-Type: application/json

```
{
            AliasID: int,
            AliasName: string,
            SystemID: int,
            SystemName: string,
            AccountID: int,
            AccountName: string,
            DomainName: string,
            Password: string,
            PrivateKey: string,
            Passphrase: string
        }
```

Response Codes

- 200 - Request successful. Account details and credentials in the response body.
- 403 - User does not have permissions to request credentials for the indicated alias or the account referenced by the alias does not have API access enabled.
    - 4031 - User does not have permission to request credentials.
    - 4034 - Request is not yet approved.
- 404 - Could not find the request to release. The specified request ID may have already been released or has expired.

> *For more information, please see "Common Response Codes" on page 17.*

Custom Platforms

Administrators have the ability to to export the custom platform configuration data from a customer's on-premises Password Safe instance and import the configuration data into a Password Safe Cloud instance.

Quick Navigation

GET CustomPlatforms

Purpose

Returns a list of platforms for managed systems.

Required Permissions

Password Safe Configuration Management (Read).

Request Body

None.

Response Body

Content-Type: application/json

```
[
    {
        PlatformID : int,
        Name : string
    },
    …
]
```

Response Body Details

- **PlatformID**: Platform ID.
- **Name**: Platform Name.

Response Codes

200 – Request successful.

For more information, please see "Common Response Codes" on page 17.

GET CustomPlatforms/{id}

Purpose

Returns a custom platform by ID.

Required Permissions

Password Safe Configuration Management (Read).

URL Parameters

id: ID of the platform.

Request Body

None.

Response Body

Content-Type: application/json

```
[
    {
        PlatformID : int,
        Name : string
    },
    …
]
```

Response Body Details

- **PlatformID**: Platform ID.
- **Name**: Platform Name.

Response Codes

200 – Request successful.

For more information, please see "Common Response Codes" on page 17.

POST CustomPlatforms/Import

Purpose

Imports a custom platform.

Required Permissions

Password Safe Configuration Management (Read/Write).

URL Parameters

None.

Request Body

```
{

    CustomPlatform : string


}
```

Response Body

Content-Type: application/json

```
[
    {
    PlatformId : int,

    },
    …
]
```

Response Body Details

- **PlatformId**: The ID of the custom platform.

Response Codes

200 – Request successful.

For more information, please see "Common Response Codes" on page 17.

POST CustomPlatforms/{id}/Export

Purpose

Exports a particular custom platform.

Required Permissions

Password Safe Configuration Management (Read).

URL Parameters

id: ID of the custom platform.

Request Body

None.

Response Body

Content-Type: application/xml

Response Body Details

The custom platform XML data is returned in the response..

Response Codes

200 – Request successful.

For more information, please see "Common Response Codes" on page 17.

Directories

Quick Navigation

For more information on related topics, please see "Managed Systems" on page 284.

GET Directories

Purpose

Returns a list of directories.

Required Permissions

One of: Password Safe System Management (Read), Password Safe Domain Management (Read).

Request Body

None.

Response Body

```
Content-type: application/json [
    {
        DirectoryID : int,
        WorkgroupID : int,
        PlatformID : int,
        DomainName : string,
        ForestName : string,
        NetBiosName : string,
        UseSSL : bool,
        Port : int, // can be null
        Timeout : short,
        Description : string,
        ContactEmail : string,
        PasswordRuleID : int,
        ReleaseDuration : int,
```

```
        MaxReleaseDuration : int,
        ISAReleaseDuration : int,
        AccountNameFormat : int,
        AutoManagementFlag : bool,
        FunctionalAccountID : int, // can be null
        CheckPasswordFlag : bool,
        ChangePasswordAfterAnyReleaseFlag : bool,
        ResetPasswordOnMismatchFlag : bool,
        ChangeFrequencyType : string,
        ChangeFrequencyDays : int,
    }
]
```

Response Codes

200 - Request successful. Directory in response body.

For more information, please see "Common Response Codes" on page 17.

GET Directories/{id}

Purpose

Returns a directory by ID.

Required Permissions

One of: Password Safe System Management (Read), Password Safe Domain Management (Read).

URL Parameters

id: ID of the directory.

Request Body

None.

Response Body

Content-Type: application/json

```
{
    DirectoryID : int,
    WorkgroupID : int,
```

```
    PlatformID : int,
    DomainName : string,
    ForestName : string,
    NetBiosName : string,
    UseSSL : bool,
    Port : int, // can be null
    Timeout : short,
    Description : string,
    ContactEmail : string,
    PasswordRuleID : int,
    ReleaseDuration : int,
    MaxReleaseDuration : int,
    ISAReleaseDuration : int,
    AccountNameFormat : int,
    AutoManagementFlag : bool,
    FunctionalAccountID : int, // can be null
    CheckPasswordFlag : bool,
    ChangePasswordAfterAnyReleaseFlag : bool,
    ResetPasswordOnMismatchFlag : bool,
    ChangeFrequencyType : string,
    ChangeFrequencyDays : int,
    ChangeTime : string,
}
```

POST Workgroups/{id}/Directories

Purpose

Creates a new directory in the Workgroup referenced by ID.

Required Permissions

One of: Password Safe System Management (Read/Write), Password Safe Domain Management (Read/Write).

URL Parameters

id: ID of the Workgroup.

Request Body

Content-Type: application/json

```
{
    PlatformID : int,
    DomainName : string,
    ForestName : string,
    NetBiosName : string,
    UseSSL : bool,
```

```
    Port : int, // can be null
    Timeout : short,
    Description : string,
    ContactEmail : string,
    PasswordRuleID : int,
    ReleaseDuration : int,
    MaxReleaseDuration : int,
    ISAReleaseDuration : int,
    AccountNameFormat : int,
    AutoManagementFlag : bool,
    FunctionalAccountID : int, // can be null
    CheckPasswordFlag : bool,
    ChangePasswordAfterAnyReleaseFlag : bool,
    ResetPasswordOnMismatchFlag : bool,
    ChangeFrequencyType : string,
    ChangeFrequencyDays : int,
    ChangeTime : string,
}
```

Request Body Details

- **PlatformID:** (required) ID of the platform
- **DomainName:** (required) Name of the domain. Max string length is 128.
- **ForestName:** (required for Active Directory only, not applicable to LDAP) Name of the directory forest. Max string length is 64.
- **NetBiosName:** (required for Active Directory, optional for LDAP) NetBIOS name of the directory. Max string length is 15.
- **UseSSL:** (default: false) True to use an SSL connection, otherwise false.
- **Port:** (set automatically for Active Directory, optional for LDAP) The port used to connect to the host. If null and the related Platform is LDAP, Password Safe uses **Platform.DefaultPort**.
- **Timeout:** (seconds, default: 30) Connection timeout. Length of time in seconds before a slow or unresponsive connection to the system fails.
- **Description:** (optional) Description of the directory. Max string length is 255.
- **ContactEmail:** Max string length is 1000.
- **PasswordRuleID:** (default: 0) ID of the default password rule assigned to managed accounts created under this managed system.
- **ReleaseDuration:** (minutes: 1-525600, default: 120) Default release duration.
- **MaxReleaseDuration:** (minutes: 1-525600, default: 525600) Default maximum release duration.
- **ISAReleaseDuration:** (minutes: 1-525600, default: 120) Default Information Systems Administrator (ISA) release duration.
- **AccountNameFormat:** (Active Directory only, default: 0) Account Name format to use:
    - **0:** Domain and Account. Use **ManagedAccount.DomainName\ManagedAccount.AccountName**
    - **1:** UPN. Use the Managed Account UPN
    - **2:** SAM. Use the Managed Account SAM Account Name
- **AutoManagementFlag:** (default: false) True if password auto-management is enabled, otherwise false. Can be set if **Platform.AutoManagementFlag** is true.
    - **FunctionalAccountID:** (required if **AutoManagementFlag** is true) ID of the functional account used for managed account password changes. **FunctionalAccount.PlatformID** must match the **PlatformID**.

- **CheckPasswordFlag:** True to enable password testing, otherwise false.
- **ChangePasswordAfterAnyReleaseFlag:** True to change passwords on release of a request, otherwise false.
- **ResetPasswordOnMismatchFlag:** True to queue a password change when scheduled password test fails, otherwise false.
- **ChangeFrequencyType:** (default: first) The change frequency for scheduled password changes:
  - **first:** Changes scheduled for the first day of the month
  - **last:** Changes scheduled for the last day of the month
  - **xdays:** Changes scheduled every x days (see ChangeFrequencyDays)
- **ChangeFrequencyDays:** (days: 1-999, required if **ChangeFrequencyType** is **xdays**) When **ChangeFrequencyType** is **xdays**, password changes take place this configured number of days.
- **ChangeTime:** (24hr format: 00:00-23:59, default: 23:30) UTC time of day scheduled password changes take place.

Response Body

Content-Type: application/json

```
{
    DirectoryID : int,
    WorkgroupID : int,
    PlatformID : int,
    DomainName : string,
    ForestName : string,
    NetBiosName : string,
    UseSSL : bool,
    Port : int, // can be null
    Timeout : short,
    Description : string,
    ContactEmail : string,
    PasswordRuleID : int,
    ReleaseDuration : int,
    MaxReleaseDuration : int,
    ISAReleaseDuration : int,
    AccountNameFormat : int,
    AutoManagementFlag : bool,
    FunctionalAccountID : int, // can be null
    CheckPasswordFlag : bool,
    ChangePasswordAfterAnyReleaseFlag : bool,
    ResetPasswordOnMismatchFlag : bool,
    ChangeFrequencyType : string,
    ChangeFrequencyDays : int,
    ChangeTime : string,
}
```

Response Codes

201 - Request successful. Directory in response body.

For more information, please see "Common Response Codes" on page 17.

PUT Directories/{id}

Purpose

Updates an existing directory by ID.

Required Permissions

One of: Password Safe System Management (Read/Write), Password Safe Domain Management (Read/Write).

URL Parameters

id: ID of the directory.

Request Body

Content-Type: application/json

```
{
    PlatformID : int,
    WorkgroupID : int,
    DomainName : string,
    ForestName : string,
    NetBiosName : string,
    UseSSL : bool,
    Port : int, // can be null
    Timeout : short,
    Description : string,
    ContactEmail : string,
    PasswordRuleID : int,
    ReleaseDuration : int,
    MaxReleaseDuration : int,
    ISAReleaseDuration : int,
    AccountNameFormat : int,
    AutoManagementFlag : bool,
    FunctionalAccountID : int, // can be null
    CheckPasswordFlag : bool,
    ChangePasswordAfterAnyReleaseFlag : bool,
    ResetPasswordOnMismatchFlag : bool,
    ChangeFrequencyType : string,
    ChangeFrequencyDays : int,
    ChangeTime : string,
}
```

Request Body Details

- **WorkgroupID:** (required) ID of the Workgroup.
- **PlatformID:** (required) ID of the platform.

- **DomainName:** (required) Name of the domain. Max string length is 128.
- **ForestName:** (required for Active Directory only, not applicable to LDAP) Name of the directory forest. Max string length is 64..
- **NetBiosName:** (required for Active Directory, optional for LDAP) NetBIOS Name of the directory. Max string length is 15.
- **UseSSL:** (default: false) True to use an SSL connection, otherwise false.
- **Port:** (set automatically for Active Directory, optional for LDAP) The port used to connect to the host. If null and the related Platform is LDAP, Password Safe uses **Platform.DefaultPort**.
- **Timeout:** (seconds, default: 30) Connection timeout. Length of time in seconds before a slow or unresponsive connection to the system fails.
- **Description:** (optional) Description of the directory. Max string length is 255.
- **ContactEmail:** Max string length is 1000.
- **PasswordRuleID:** (default: 0) ID of the default password rule assigned to managed accounts created under this managed system.
- **ReleaseDuration:** (minutes: 1-525600, default: 120) Default release duration.
- **MaxReleaseDuration:** (minutes: 1-525600, default: 525600) Default maximum release duration.
- **ISAReleaseDuration:** (minutes: 1-525600, default: 120) Default Information Systems Administrator (ISA) release duration.
- **AccountNameFormat:** (Active Directory only, default: 0) Account name format to use:
    - **0:** Domain and Account. Use **ManagedAccount.DomainName\ManagedAccount.AccountName**
    - **1:** UPN. Use the Managed Account UPN
    - **2:** SAM. Use the Managed Account SAM Account Name
- **AutoManagementFlag:** (default: false) True if password auto-management is enabled, otherwise false. Can be set if **Platform.AutoManagementFlag** is true.
    - **FunctionalAccountID:** (required if **AutoManagementFlag** is true) ID of the functional account used for managed account password changes. **FunctionalAccount.PlatformID** must match the **PlatformID**.
    - **CheckPasswordFlag:** True to enable password testing, otherwise false.
    - **ChangePasswordAfterAnyReleaseFlag:** True to change passwords on release of a request, otherwise false.
    - **ResetPasswordOnMismatchFlag:** True to queue a password change when scheduled password test fails, otherwise false.
    - **ChangeFrequencyType:** (default: first) The change frequency for scheduled password changes:
        - **first:** Changes scheduled for the first day of the month
        - **last:** Changes scheduled for the last day of the month
        - **xdays:** Changes scheduled every x days (see **ChangeFrequencyDays**)
    - **ChangeFrequencyDays:** (days: 1-999, required if **ChangeFrequencyType** is **xdays**) When **ChangeFrequencyType** is **xdays**, password changes take place this configured number of days.
    - **ChangeTime:** (24hr format: 00:00-23:59, default: 23:30) UTC time of day scheduled password changes take place.

Response Body

Content-Type: application/json

```
{
    DirectoryID : int,
```

```
    WorkgroupID : int,
    PlatformID : int,
    DomainName : string,
    ForestName : string,
    NetBiosName : string,
    UseSSL : bool,
    Port : int, // can be null
    Timeout : short,
    Description : string,
    ContactEmail : string,
    PasswordRuleID : int,
    ReleaseDuration : int,
    MaxReleaseDuration : int,
    ISAReleaseDuration : int,
    AccountNameFormat : int,
    AutoManagementFlag : bool,
    FunctionalAccountID : int, // can be null
    CheckPasswordFlag : bool,
    ChangePasswordAfterAnyReleaseFlag : bool,
    ResetPasswordOnMismatchFlag : bool,
    ChangeFrequencyType : string,
    ChangeFrequencyDays : int,
    ChangeTime : string,
}
```

Response Codes

200 - Request successful. Directory in response body.

For more information, please see "Common Response Codes" on page 17.

DELETE Directories

Purpose

Deletes a directory by ID.

Required Permissions

One of: Password Safe System Management (Read/Write), Password Safe Domain Management (Read/Write).

URL Parameters

id: ID of the directory.

Request Body

None.

Response Body

None.

Response Codes

200 – Request successful.

For more information, please see "Common Response Codes" on page 17.

Oracle Internet Directories

Quick Navigation

GET OracleInternetDirectories

Purpose

Returns a list of Oracle Internet Directories.

Required Permissions

Password Safe System Management (Read).

Request Body

None.

Response Body

Content-type: application/json

```
[{
    OrganizationID : Guid,
    OracleInternetDirectoryID : Guid,
    Name : string,
    Description : string,
},
…]
```

Response Codes

200 – Request successful. Oracle Internet Directories in response body.

For more information, please see "Common Response Codes" on page 17.

GET OracleInternetDirectories/{id}

Purpose

Returns an Oracle Internet Directory by ID.

Required Permissions

Password Safe System Management (Read).

URL Parameters

id: ID of the Oracle Internet Directory.

Request Body

None.

Response Body

Content-Type: application/json

```
{
    OrganizationID : Guid,
    OracleInternetDirectoryID : Guid,
    Name : string,
    Description : string,
}
```

Response Codes

200 – Request successful. Oracle Internet Directory in response body.

For more information, please see "Common Response Codes" on page 17.

GET Organizations/{id}/OracleInternetDirectories

Purpose

Returns a list of Oracle Internet Directories by organization ID.

Required Permissions

Password Safe System Management (Read).

URL Parameters

id: ID of the organization.

Request Body

None.

Response Body

Content-Type: application/json

```
[{
    OrganizationID : Guid,
    OracleInternetDirectoryID : Guid,
    Name : string,
    Description : string,
},
…]
```

Response Codes

200 – Request successful. Oracle Internet Directories in response body.

For more information, please see "Common Response Codes" on page 17.

POST OracleInternetDirectories/{id}/Services/Query

Purpose

Queries and returns DB Services for an Oracle Internet Directory by ID.

Required Permissions

Password Safe System Management (Read/Write).

URL Parameters

id: ID of the Oracle Internet Directory.

Request Body

None.

Response Body

Content-Type: application/json

```
{
    Success : bool,
    Message : string,
    Services : [{
    Name : string,
},
…]
}
```

Response Codes

200 - Request successful. Oracle Internet Directory query result in response body.

For more information, please see "Common Response Codes" on page 17.

POST OracleInternetDirectories/{id}/Test

Purpose

Tests the connection to an Oracle Internet Directory by ID.

Required Permissions

Password Safe System Management (Read/Write).

URL Parameters

id: ID of the Oracle Internet Directory.

Request Body

None.

Response Body

Content-Type: application/json

```
{
    Success : bool,
}
```

Response Codes

200 – Request successful. Oracle Internet Directory test result in response body.

For more information, please see "Common Response Codes" on page 17.

DSS Key Policies

> ***Note:*** *DSS Key Policies are formerly known as DSS Key Rules but the API remains* ***DSSKeyRules*** *to be compatible with earlier versions.*

Quick Navigation

- "GET DSSKeyRules" on page 200
- "GET DSSKeyRules/{id}" on page 201

GET DSSKeyRules

Purpose

Returns a list of DSS Key Rules.

Required Permissions

Password Safe System Management (Read).

Request Body

None.

Response Body

Content-Type: application/json

```
[
    {
        DSSKeyRuleID: int,
        Name: string,
        Description: string,
        KeyType: string,
        KeySize: int,
        EncryptionType: char,
        PasswordRuleID: int, // can be null
    },
    …
]
```

Response Body Details

- **KeyType:** (RSA, DSA) The type of key to generate.
- **EncryptionType:** The type of key encryption to use:
  - **A:** Auto-managed passphrase, generated using the associated password rule (see **PasswordRuleID**).
  - **N:** No encryption.
- **PasswordRuleID:** (given when **EncryptionType** is **A**) ID of the password rule used to auto-generate the passphrase for DSS key encryption.

Response Codes

200 - Request successful. DSS Key Rules in the response body.

For more information, please see "Common Response Codes" on page 17.

GET DSSKeyRules/{id}

Purpose

Returns a DSS Key Rule by ID.

Required Permissions

Password Safe System Management (Read).

URL Parameters

id: ID of the DSS Key Rule.

Request Body

None.

Response Body

Content-Type: application/json

```
{
    DSSKeyRuleID: int,
    Name: string,
    Description: string,
    KeyType: string,
```

```
    KeySize: int,
    EncryptionType: char,
    PasswordRuleID: int, // can be null
}
```

Response Body Details

- **KeyType:** The type of key to generate (RSA, DSA).
- **EncryptionType:** The type of key encryption to use:
    - **A:** Auto-managed passphrase, generated using the associated password rule (see **PasswordRuleID**).
    - **N:** No encryption.
- **PasswordRuleID:** (given when **EncryptionType** is **A**) ID of the password rule used to auto-generate the passphrase for DSS key encryption.

Response Codes

200 - Request successful. DSS Key Rule in the response body.

For more information, please see "Common Response Codes" on page 17.

Entity Types

Entity types define the types of entities within Password Safe (for example, asset, database, directory, and cloud).

For more information on related topics, please see "Platforms" on page 352.

GET EntityTypes

Purpose

Returns a list of entity types.

Required Permissions

None.

Request Body

None.

Response Body

Content-Type: application/json

```
[
    {
        EntityTypeID: int,
        Name: string,
        Description: string,
    },
    …
]
```

Response Codes

200 - Request successful. Entity types in the response body.

For more information, please see "Common Response Codes" on page 17.

Functional Accounts

Quick Navigation

GET FunctionalAccounts

Purpose

Returns a list of functional accounts.

Required Permissions

Password Safe Account Management (Read).

Request Body

None.

Response Body

Content-Type: application/json

```
[
    {
        FunctionalAccountID : int,
        PlatformID : int,
        DomainName : string,
        AccountName : string,
        DisplayName : string,
        Description : string,
        ElevationCommand : string,
        SystemReferenceCount : int,
        TenantID : string,
        ObjectID : string
    },
    …
]
```

Response Body Details

- **PlatformID:** ID of the platform to which the account belongs.
- **DomainName:** Domain name of the account.
- **AccountName:** Name of the account (does not include domain name).
- **DisplayName:** The display name or alias for the account.
- **Description:** Description of the account.
- **ElevationCommand:** Elevation command used for SSH connections (**sudo**, **pbrun**, **pmrun**).
- **SystemReferenceCount:** The count of managed systems that reference the functional account.
- **TenantID:** TenantID of the account (if applicable).
- **ObjectID:** ObjectID of the account (if applicable).

Response Codes

200 - Request successful. Functional account in the response body.

For more information, please see "Common Response Codes" on page 17.

GET FunctionalAccounts/{id}

Purpose

Returns a functional account by ID.

Required Permissions

Password Safe Account Management (Read).

URL Parameters

id: ID of the functional account.

Request Body

None.

Response Body

Content-Type: application/json

```
{
    FunctionalAccountID : int,
    PlatformID: int, DomainName : string,
    AccountName : string,
    DisplayName : string,
    Description : string,
    ElevationCommand : string,
    SystemReferenceCount : int,
    TenantID : string,
    ObjectID : string
}
```

Response Body Details

- **PlatformID:** ID of the platform to which the account belongs.
- **DomainName:** Domain name of the account.
- **AccountName:** Name of the account (does not include domain name).
- **DisplayName:** The display name or alias for the account.
- **Description:** Description of the account.
- **ElevationCommand:** Elevation command used for SSH connections (**sudo**, **pbrun**, **pmrun**).
- **SystemReferenceCount:** The count of managed systems that reference the functional account.
- **TenantID:** TenantID of the account (if applicable).
- **ObjectID:** ObjectID of the account (if applicable).

Response Codes

200 - Request successful. Functional Account in the response body.

For more information, please see "Common Response Codes" on page 17.

POST FunctionalAccounts

Purpose

Creates a functional account.

Required Permissions

Password Safe Account Management (Read/Write).

Request Body

Content-Type: application/json

```
{
    PlatformID : int,
    DomainName : string,
    AccountName : string,
    DisplayName : string,
    Password : string,
    PrivateKey : string,
    Passphrase : string,
    Description : string,
    ElevationCommand : string,
    TenantID : string,
    ObjectID : string,
    Secret : string
}
```

Request Body Details

- **PlatformID:** (required) ID of the platform to which the account belongs.
- **DomainName:** (optional) Domain name of the account. Can be set if **Platform.DomainNameFlag** is true. Max string length is 50.
- **AccountName:** (required) Name of the account (do not include domain name). Max string length is 245.
- **DisplayName:** (optional) The display name or alias for the account. If not given, uses the **AccountName**. Must be unique for the platform. Max string length is 100.
- **Password:** (required when **Platform.RequiresSecret** is false) The current account password.
- **PrivateKey:** (optional) DSS private key. Can be set if **Platform.DSSFlag** is true.
- **Passphrase:** (required when **PrivateKey** is an encrypted DSS key) DSS passphrase. Can be set if **Platform.DSSFlag** is true.
- **Description:** (optional) Description of the account. Max string length is 1000.
- **ElevationCommand:** (optional) Elevation command to use for SSH connections. Can be set if **Platform.SupportsElevationFlag** is true (**sudo**, **pbrun**, **pmrun**). Max string length is 80.
- **TenantID:** string (required when **Platform.RequiresTenantID** is true). Max string length is 36.
- **ObjectID:** string (required when **Platform.RequiresObjectID** is true). Max string length is 36.
- **Secret: string:** (required when **Platform.RequiresSecret** is true). Max string length is 255.

Response Body

Content-Type: application/json

```
{
    FunctionalAccountID : int,
    PlatformID : int,
    DomainName : string,
    AccountName : string,
    DisplayName : string,
    Description : string,
    ElevationCommand : string,
    SystemReferenceCount : int,
    TenantID : string,
```

```
    ObjectID : string
}
```

Response Body Details

- **PlatformID:** ID of the platform to which the account belongs.
- **DomainName:** Domain name of the account.
- **AccountName:** Name of the account (does not include domain name).
- **DisplayName:** The display name or alias for the account.
- **Description:** Description of the account.
- **ElevationCommand:** Elevation command used for SSH connections (**sudo**, **pbrun**, **pmrun**).
- **SystemReferenceCount:** The count of managed systems that reference the functional account.
- **TenantID:** TenantID of the account (if applicable).
- **ObjectID:** ObjectID of the account (if applicable).

Response Codes

201 - Request successful. Functional Account in the response body.

For more information, please see "Common Response Codes" on page 17.

DELETE FunctionalAccounts/{id}

Purpose

Deletes a functional account by ID.

Required Permissions

Password Safe Account Management (Read/Write).

Other Requirements

The functional account cannot be referenced by any managed systems.

URL Parameters

id: ID of the functional account.

Request Body

None.

Response Body

None.

Response Codes

200 - Request successful.

For more information, please see "Common Response Codes" on page 17.

ISA Requests

The ISARequests endpoint is for Information Systems Administrator (ISA) role access.

> *For more information on Requestor and Requestor/Approver role access, please see "POST Requests" on page 377.*

POST ISARequests

Purpose

Creates a new Information Systems Administrator (ISA) release request and returns the requested credentials.

Similar to **POST Requests (AccessType=View)** and **GET Credentials** in a single call.

Required Roles

ISA Role to managed account referenced by ID.

Query Parameters

- **type:** (optional, default: password) Type of credentials to retrieve.
  - **password:** Returns the password in the response body.
  - **dsskey:** Returns the DSS private key in the response body.

> ***Note:** The key is returned in the state in which it was set. For example, an encrypted key is returned encrypted.*

  - **passphrase:** Returns the DSS key passphrase in the response body.

> ***Note: passphrase** supported only for encrypted DSS keys.*

Request Body

Content-Type: application/json

```
{
    SystemID: int,
    AccountID: int,
    DurationMinutes: int, // can be null
    Reason: string
}
```

Request Body Details

- **SystemID:** (required) ID of the managed system to request.
- **AccountID:** (required) ID of the managed account to request.
- **DurationMinutes:** (optional) The request duration (in minutes). If omitted, uses the value **ManagedAccount.ISAReleaseDuration**.
- **Reason:** (optional) The reason for the request.

Response Body

```
{
    Credentials: string
}
```

Response Codes

201 - Request successful. Credentials in the response body.

For more information, please see "Common Response Codes" on page 17.

ISA Sessions

The ISASessions endpoint is for Information Systems Administrator (ISA) role access.

> *For more information on Requestor and Requestor/Approver role access, please see the following:*
>
> - *"POST Requests" on page 377*
> - *"POST Requests/{requestID}/Sessions" on page 399*

POST ISASessions

Purpose

Creates a new Information Systems Administrator (ISA) release request and returns the requested session.

Similar to **POST Requests** and **POST Sessions** in a single call.

Required Roles

- ISA role to managed account referenced by ID.

Request Body

Content-Type: application/json

```
{
    SessionType : string,
    SystemID: int,
    AccountID: int,
    DurationMinutes : int, // can be null
    ApplicationID: int, // can be null
    Reason : string
}
```

Request Body Details

- **SessionType:** (required) The type of session to create.
- **SystemID:** (required) ID of the managed system to request.
- **AccountID:** (required) ID of the managed account to request.
- **DurationMinutes:** (optional) The request duration (in minutes). If omitted, uses the value **ManagedAccount.ISAReleaseDuration**.
- **ApplicationID:** (required when **AccessType** = **App** or **AccessType** = **AppFile**) ID of the application to request.
- **Reason:** (optional) The reason for the request.

Response Body (SSH or sshticket)

Content-Type: application/json

```
{
    ID : string,
    Ticket : string,
    Host : string,
    Port : string,
    TicketAtHost : string,
    Link : string,
    Command : string
}
```

Response Body (RDP or rdpticket)

Content-Type: application/json

```
{
    ID : string,
    Ticket : string,
    Host : string,
    Port : string
}
```

Response Body (rdpfile or appfile)

RDP file as an attachment.

Response Codes

201- Request successful. Session details or RDP file in the response body.

For more information, please see "Common Response Codes" on page 17.

Keystrokes

Quick Navigation

GET Sessions/{sessionId:int}/Keystrokes

Purpose

Returns a list of keystrokes by session ID.

Required Roles

Password Safe Auditor role, ISA role, or a member of BeyondInsight Administrators group.

URL Parameters

sessionId: ID of recorded RDP/SSH session.

Response Body

Content-Type: application/json

```
[
    {
        KeystrokeID: long,
        SessionID: int,
        TimeMarker: long,
        Type: byte,
        Data: string
    },
    …
]
```

Response Codes

200 - Request successful. Keystrokes are in response body.

> *For more information, please see "Common Response Codes" on page 17.*

GET Keystrokes/{id:long}

Purpose

Returns a keystroke by ID.

Required Roles

Password Safe Auditor role, ISA role, or a member of BeyondInsight Administrators group.

URL Parameters

id: ID of a keystroke.

Response Body

Content-Type: application/json

```
{
    KeystrokeID: long,
    SessionID: int,
    TimeMarker: long,
    Type: byte ,
    Data: string
}
```

Response Codes

200 - Request successful. Keystroke in response body.

For more information, please see "Common Response Codes" on page 17.

POST Keystrokes/Search

Purpose

Search for keystrokes.

Required Roles

Password Safe Auditor role, ISA role, or a member of BeyondInsight Administrators group.

Request Body

Content-Type: application/json

```
{
    Data: string,
    Type: byte
}
```

Request Body Details

- **Data:** (required) Keyword(s) for which to search.
- **Type:** (default: **0**) Type of keystrokes:
    - **0:** All
    - **1:** StdIn
    - **2:** StdOut
    - **4:** Window Event
    - **5:** User Event

Response Body

Content-Type: application/json

```
[
    {
        KeystrokeID: long,
        SessionID: int,
        TimeMarker: long,
        Type: byte,
        Data: string
    },
    …
]
```

Response Codes

200 - Request successful. Keystrokes are in response body.

For more information, please see "Common Response Codes" on page 17.

Linked Accounts

Linked accounts are Directory managed accounts that are linked to asset-based managed systems.

> **Note:** *Directory accounts can be linked only to managed assets and managed databases.*

Quick Navigation

GET ManagedSystems/{systemID}/LinkedAccounts

Purpose

Returns a list of linked directory managed accounts by managed system ID.

Required Permissions

Password Safe System Management (Read).

URL Parameters

systemID: ID of the managed system.

Request Body

None.

Response Body

Content-Type: application/json

```
[
    {
        ManagedAccountID : int,
        ManagedSystemID : int,
        DomainName : string,
        AccountName : string,
        DistinguishedName : string,
```

```
        PasswordFallbackFlag : bool,
        LoginAccountFlag : bool,
        Description : string,
        PasswordRuleID : int,
        ApiEnabled : bool,
        ReleaseNotificationEmail : string,
        ChangeServicesFlag : bool,
        RestartServicesFlag : bool,
        ReleaseDuration : int,
        MaxReleaseDuration : int,
        ISAReleaseDuration : int,
        MaxConcurrentRequests : int,

        AutoManagementFlag : bool,
        DSSAutoManagementFlag : bool,
        CheckPasswordFlag : bool,
        ResetPasswordOnMismatchFlag : bool,
        ChangePasswordAfterAnyReleaseFlag : bool,
        ChangeFrequencyType : string,
        ChangeFrequencyDays : int,
        ChangeTime : string,

        ParentAccountID : int, // can be null
        IsSubscribedAccount : bool,
        LastChangeDate : datetime, // can be null
        NextChangeDate : datetime, // can be null
        IsChanging : bool,
        ChangeState : int,
        UseOwnCredentials : bool,
        ChangeIISAppPoolFlag : bool,
        RestartIISAppPoolFlag : bool,
        WorkgroupID : int, // can be null

        ChangeWindowsAutoLogonFlag : bool,
        ChangeComPlusFlag : bool,
        ChangeDComFlag : bool,
        ChangeSComFlag : bool,
        },
    …
]
```

Response Body Details

- **DomainName:** The domain name for a domain-type account.
- **AccountName:** The name of the account.
- **DistinguishedName:** The distinguished name of an LDAP managed account.
- P**asswordFallbackFlag:** True if failed DSS authentication can fall back to password authentication, otherwise false.
- **LoginAccountFlag:** True if the account should use the managed system login account for SSH sessions, otherwise false.
- **Description:** A description of the account.
- **PasswordRuleID:** ID of the password rule assigned to this managed account.
- **ApiEnabled:** True if the account can be requested through the API, otherwise false.

- **ReleaseNotificationEmail:** Email address used for notification emails related to this managed account.
- **ChangeServicesFlag:** True if services run as this user should be updated with the new password after a password change, otherwise false.
- **RestartServicesFlag:** True if services should be restarted after the run as password is changed (see **ChangeServicesFlag**), otherwise false.
- **ReleaseDuration:** (minutes: 1-525600) Default release duration.
- **MaxReleaseDuration:** (minutes: 1-525600) Default maximum release duration.
- **ISAReleaseDuration:** (minutes: 1-525600) Default Information Systems Administrator (ISA) release duration.
- **MaxConcurrentRequests:** (0-999, 0 means unlimited) Maximum number of concurrent password requests for this account.
- **AutoManagementFlag:** True if password auto-management is enabled, otherwise false.
    - **DSSAutoManagementFlag:** True if DSS key auto-management is enabled, otherwise false.
    - **CheckPasswordFlag:** True to enable password testing, otherwise false.
    - **ChangePasswordAfterAnyReleaseFlag:** True to change passwords on release of a request, otherwise false.
    - **ResetPasswordOnMismatchFlag:** True to queue a password change when scheduled password test fails, otherwise false.
    - **ChangeFrequencyType:** The change frequency for scheduled password changes:
        - **first:** Changes scheduled for the first day of the month.
        - **last:** Changes scheduled for the last day of the month.
        - **xdays:** Changes scheduled every x days (see **ChangeFrequencyDays**).
    - **ChangeFrequencyDays:** (days: 1-999) When **ChangeFrequencyType** is **xdays**, password changes take place this configured number of days.
    - **ChangeTime:** (24hr format: 00:00-23:59) UTC time of day scheduled password changes take place.
- **ParentAccountID:** If this is a subscribed account (see **IsSubscribedAccount**), this is the ID of the parent managed account.
- **IsSubscribedAccount:** True if the account is a synced or subscribed account, otherwise false.
- **LastChangeDate:** The date and time of the last password change.
- **NextChangeDate:** The date and time of the next scheduled password change.
- **IsChanging:** True if the account credentials are in the process of changing, otherwise false.
- **ChangeState:** The change state of the account credentials:
    - **0:** Idle / no change taking place or scheduled within 5 minutes.
    - **1:** Changing / managed account credential currently changing.
    - **2:** Queued / managed account credential is queued to change or scheduled to change within 5 minutes.

For more information, please see Configure Subscriber Accounts at https://www.beyondtrust.com/docs/beyondinsight-password-safe/ps/admin/managed-accounts.htm#ConfigureAccounts.

Response Codes

200 - Request successful. Linked managed account in the response body.

For more information, please see "Common Response Codes" on page 17.

POST ManagedSystems/{systemID}/LinkedAccounts/{accountID}

Purpose

Links a directory managed account to the managed system referenced by ID.

Required Permissions

Password Safe System Management (Read/Write).

URL Parameters

- **systemID:** ID of the managed system.
- **accountID:** ID of the directory managed account.

Request Body

None.

Response Body

Content-Type: application/json

```
{
    ManagedAccountID : int,
    ManagedSystemID : int,
    DomainName : string,
    AccountName : string,
    DistinguishedName : string,
    PasswordFallbackFlag : bool,
    LoginAccountFlag : bool,
    Description : string,
    PasswordRuleID : int,
    ApiEnabled : bool,
    ReleaseNotificationEmail : string,
    ChangeServicesFlag : bool,
    RestartServicesFlag : bool,
    ReleaseDuration : int,
    MaxReleaseDuration : int,
    ISAReleaseDuration : int,
    MaxConcurrentRequests : int,

    AutoManagementFlag : bool,
    DSSAutoManagementFlag : bool,
    CheckPasswordFlag : bool,
    ResetPasswordOnMismatchFlag : bool,
    ChangePasswordAfterAnyReleaseFlag : bool,
    ChangeFrequencyType : string,
```

```
    ChangeFrequencyDays : int,
    ChangeTime : string,

    ParentAccountID : int, // can be null
    IsSubscribedAccount : bool,
    LastChangeDate : datetime, // can be null
    NextChangeDate : datetime, // can be null
    IsChanging: bool,
    ChangeState : int,
    UseOwnCredentials : bool,
    ChangeIISAppPoolFlag : bool,
    RestartIISAppPoolFlag : bool,
    WorkgroupID : int, // can be null

    ChangeWindowsAutoLogonFlag : bool,
    ChangeComPlusFlag : bool,
    ChangeDComFlag : bool,
    ChangeSComFlag : bool,
}
```

Response Body Details

- **AccountName:** The name of the account.
- **PasswordFallbackFlag:** True if failed DSS authentication can fall back to password authentication, otherwise false.
- **LoginAccountFlag:** True if the account should use the managed system login account for SSH sessions, otherwise false.
- **Description:** A description of the account.
- **PasswordRuleID:** ID of the password rule assigned to this managed account.
- **ApiEnabled:** True if the account can be requested through the API, otherwise false.
- **ReleaseNotificationEmail:** Email address used for notification emails related to this managed account.
- **ChangeServicesFlag:** True if services run as this user should be updated with the new password after a password change, otherwise false.
- **RestartServicesFlag:** True if services should be restarted after the run as password is changed (see **ChangeServicesFlag**), otherwise false.
- **ReleaseDuration:**(minutes: 1-525600) Default release duration.
- **MaxReleaseDuration:** (minutes: 1-525600) Default maximum release duration.
- **ISAReleaseDuration:** (minutes: 1-525600) Default Information Systems Administrator (ISA) release duration.
- **MaxConcurrentRequests:** (0-999, 0 is unlimited) Maximum number of concurrent password requests for this account.
- **AutoManagementFlag:** True if password auto-management is enabled, otherwise false.
    - **DSSAutoManagementFlag:** True if DSS key auto-management is enabled, otherwise false.
    - **CheckPasswordFlag:** True to enable password testing, otherwise false.
    - **ChangePasswordAfterAnyReleaseFlag:** True to change passwords on release of a request, otherwise false.
    - **ResetPasswordOnMismatchFlag:** True to queue a password change when scheduled password test fails, otherwise false.

- **ChangeFrequencyType:** The change frequency for scheduled password changes:
  - **first:** Changes scheduled for the first day of the month.
  - **last:** Changes scheduled for the last day of the month.
  - **xdays:** Changes scheduled every x days (**ChangeFrequencyDays**).
- **ChangeFrequencyDays:** (days: 1-999) When **ChangeFrequencyType** is **xdays**, password changes take place this configured number of days.
- **ChangeTime:** (24hr format: 00:00-23:59) UTC time of day scheduled password changes take place.

- **ParentAccountID:** If this is a subscribed account (**IsSubscribedAccount**), this is the ID of the parent managed account.
- **IsSubscribedAccount:** True if the account is a synced or subscribed account, otherwise false.
- **LastChangeDate:** The date and time of the last password change.
- **NextChangeDate:** The date and time of the next scheduled password change.
- **IsChanging:** True if the account credentials are in the process of changing, otherwise false.
- **ChangeState:** The change state of the account credentials:
  - **0:** Idle / no change taking place or scheduled within 5 minutes.
  - **1:** Changing / managed account credential currently changing.
  - **2:** Queued / managed account credential is queued to change or scheduled to change within 5 minutes.

For more information, please see Configure Subscriber Accounts at https://www.beyondtrust.com/docs/beyondinsight-password-safe/ps/admin/managed-accounts.htm#ConfigureAccounts.

Response Codes

- 200 - Account was already linked. Directory Managed Account in the response body.
- 201 - Account was linked successfully. Directory Managed Account in the response body.

For more information, please see "Common Response Codes" on page 17.

DELETE ManagedSystems/{systemID}/LinkedAccounts

Purpose

Unlinks all directory managed accounts from the managed system by ID.

Required Permissions

Password Safe System Management (Read/Write).

URL Parameters

systemID: ID of the managed system.

Request Body

None.

Response Body

None.

Response Codes

200 - Request successful.

For more information, please see "Common Response Codes" on page 17.

DELETE ManagedSystems/{systemID}/LinkedAccounts/{accountID}

Purpose

Unlinks a directory managed account from the managed system by ID.

Required Permissions

Password Safe System Management (Read/Write).

URL Parameters

- **systemID:** ID of the managed system.
- **accountID:** ID of the directory managed account.

Request Body

None.

Response Body

None.

Response Codes

200 - Request successful.

For more information, please see "Common Response Codes" on page 17.

Managed Accounts

There are two different ways to interact with managed accounts:

1. **Role-based:Requestor**, **Requestor/Approver**, or **ISA** role assigned for requesting access to a specific managed account.
2. **Permission-based**: A user with appropriate **Password Safe Account Management** permission for provisioning accounts and viewing the definition of a managed account.

Role-based Access

Quick Navigation

- "GET ManagedAccounts" on page 225
- "GET ManagedAccounts?systemName={systemName}&accountName={accountName}" on page 229

For more information on related topics, please see:

- *"Managed Systems" on page 284*
- *"Requests" on page 376*
- *"Quick Rules" on page 364*
- *"Smart Rules" on page 107*

GET ManagedAccounts

Note: *When specifying a directory managed account name in the* **GET ManagedAccounts** *API call, the account name must be in the UPN or Domain\AccountName format, even if the option* **type=domainlinked** *is specified.*

For example:

```
GET managedaccounts?accountname=domain\directoryAccount&type=domainlinked
```

type=domainlinked *is not necessary in the example above.*

type=domainlinked *can be used to limit the returned results to domain accounts when an account name is not included in the call.* **type=domainlinked** *can also be useful when you want to exclude local accounts when specifying the systemname.*

If a managed account name is not specified, then **type=domainlinked** *can be used to get all the domain linked accounts that the logged-in user has access to.*

Purpose

Returns a list of managed accounts (or a single managed account depending on the query parameters provided) that can be requested by the current user.

Required Roles

Requestor, Requestor/Approver, or ISA role.

Other Requirements

Only managed accounts with the **Enable for API Access** setting enabled are returned.

Query Parameters

- **systemName:** (optional) Name of the managed system.
- **accountName:** (optional) Name of the managed account.
- **systemID:** (optional) ID of the Managed System.
- **workgroupName:** (optional) Name of the Workgroup.
- **applicationDisplayName:** (optional, when given, type must be application) Display name of the application.
- **ipAddress:** (optional, when given type must be one of system, domainlinked, or database) IP Address of the managed asset.
- **type:** (optional/recommended) Type of the managed account to return.
    - **system:** Returns local accounts.
    - **recent**: Returns recently used accounts.
    - **domainlinked:** Returns domain accounts linked to systems.
    - **database:** Returns database accounts.
    - **cloud:** Returns cloud system accounts.
    - **application:** Returns application accounts
- **limit:** (optional) (default: 1000) Number of records to return
- **offset:** (optional) (default: 0) Number of records to skip before returning <limit> records

Request Body

None

Response Body (when both systemName or systemID, and accountName are given)

Content-Type: application/json

```
{
    PlatformID : int,
    SystemId : int,
    SystemName : string,
    DomainName : string,
    AccountId : int,
    AccountName : string,
```

```
    InstanceName : string,
    UserPrincipalName : string,
    ApplicationID : int,
    ApplicationDisplayName : string,
    DefaultReleaseDuration : int,
    MaximumReleaseDuration : int,
    LastChangeDate : datetime,
    NextChangeDate : datetime,
    IsChanging : bool,
    ChangeState : int,
    IsISAAccess : bool,
    PreferredNodeID : string
}
```

Response Body (all other combinations of query parameters)

Content-Type: application/json

```
[
    {
    PlatformID : int,
    SystemId : int,
    SystemName : string,
    DomainName : string,
    AccountId : int,
    AccountName : string,
    InstanceName : string,
    UserPrincipalName : string,
    ApplicationID : int,
    ApplicationDisplayName : string,
    DefaultReleaseDuration : int,
    MaximumReleaseDuration : int,
    LastChangeDate : datetime,
    NextChangeDate : datetime,
    IsChanging : bool,
    ChangeState : int,
    IsISAAccess : bool,
    PreferredNodeID : string
    },
    …
]
```

Response Body Details

- **PlatformID:** ID of the managed system platform.
- **SystemId:** ID of the managed system.
- **SystemName:** Name of the managed system.
- **DomainName:** The domain name for a domain-type account.
- **AccountId:** ID of the managed account.
- **AccountName:** Name of the managed account.

- **InstanceName:** Database instance name of a database-type managed system, or empty for the default instance.
- **UserPrincipalName:** User Principal Name of the managed account.
- **ApplicationID:** ID of the application for application-based access.
- **ApplicationDisplayName:** Display name of the application for application-based access.
- **DefaultReleaseDuration (minutes):** Default release duration.
- **MaximumReleaseDuration (minutes):** Maximum release duration.
- **LastChangeDate:** The date and time of the last password change.
- **NextChangeDate:** The date and time of the next password change.
- **IsChanging:** True if the account credentials are in the process of changing, otherwise false.
- **IsISAAccess:** True if the account is for Information Systems Administrator (ISA) access, otherwise false.

***Note:** If **true**, credential access is through **POST ISARequests** and session access is through **POST ISASessions**.*

*If **false**, credential access is through **POST Requests** and **GET Credentials**; session access is through **POST Requests** and **POST Sessions**.*

- **ChangeState:** The change state of the account credentials:
  - **0:** Idle / no change taking place or scheduled within 5 minutes.
  - **1:** Changing / managed account credential currently changing.
  - **2:** Queued / managed account credential is queued to change or scheduled to change within 5 minutes.
- **PreferredNodeID:** ID of the node that is preferred for establishing sessions. If no node is preferred, returns the local node ID.

For more information, please see the following:

- *"ISA Requests" on page 210*
- *"ISA Sessions" on page 212*
- *"POST Requests" on page 377*
- *"Credentials" on page 179*
- *"POST Requests/{requestID}/Sessions" on page 399*

Response Codes

200 - Request successful. Requestable Account(s) in the response body.

For more information, please see "Common Response Codes" on page 17.

GET ManagedAccounts?systemName={systemName}&accountName={accountName}

Note: *This API has been replaced by optional query parameters on* ***GET ManagedAccounts****.*

For more information, please see "GET ManagedAccounts" on page 225.

Provisioning

Quick Navigation

GET ManagedAccounts/{id}

Purpose

Returns a managed account by ID.

Required Permissions

Password Safe Account Management (Read).

URL Parameters

id: ID of the managed account.

Request Body

None.

Response Body

Content-Type: application/json

```
{
    ManagedAccountID : int,
    ManagedSystemID : int,
    DomainName : string,
    AccountName : string,
    DistinguishedName : string,
    PasswordFallbackFlag : bool,
    UserPrincipalName : string,
    SAMAccountName : string,
    LoginAccountFlag : bool,
    Description : string,
    PasswordRuleID : int,
    ApiEnabled : bool,
    ReleaseNotificationEmail : string,
    ChangeServicesFlag : bool,
    RestartServicesFlag : bool,
    ChangeTasksFlag : bool,
    ReleaseDuration : int,
    MaxReleaseDuration : int,
    ISAReleaseDuration : int,
    MaxConcurrentRequests : int,

    AutoManagementFlag : bool,
    DSSAutoManagementFlag : bool,
    CheckPasswordFlag : bool,
    ResetPasswordOnMismatchFlag : bool,
```

```
    ChangePasswordAfterAnyReleaseFlag : bool,
    ChangeFrequencyType : string,
    ChangeFrequencyDays : int,
    ChangeTime : string,

    ParentAccountID : int, // can be null
    IsSubscribedAccount : bool,
    LastChangeDate: datetime, // can be null
    NextChangeDate: datetime, // can be null
    IsChanging: bool
    ChangeState : int,
    UseOwnCredentials: bool,
    WorkgroupID : int // can be null
    ChangeIISAppPoolFlag : bool,
    RestartIISAppPoolFlag : bool,
    ObjectID : string
}
```

Response Body Details

- **DomainName:** The domain name for a domain-type account.
- **AccountName:** The name of the account.
- **DistinguishedName:** The distinguished name of an LDAP managed account.
- **PasswordFallbackFlag:** True if failed DSS authentication can fall back to password authentication, otherwise false.
- **UserPrincipalName:** (Active Directory managed systems only) The account user principal name of an Active Directory account.
- **SAMAccountName:** (Active Directory managed systems only) The account SAM account name of an Active Directory account.
- **LoginAccountFlag:** True if the account should use the managed system login account for SSH sessions, otherwise false.
- **Description:** A description of the account.
- **PasswordRuleID:** ID of the password rule assigned to this managed account.
- **ApiEnabled:** True if the account can be requested through the API, otherwise false.
- **ReleaseNotificationEmail:** Email address used for notification emails related to this managed account.
- **ChangeServicesFlag:** True if services run as this user should be updated with the new password after a password change, otherwise false.
- **RestartServicesFlag:** True if services should be restarted after the run as password is changed (**ChangeServicesFlag**), otherwise false.
- **ChangeTasksFlag:** True if scheduled tasks run as this user should be updated with the new password after a password change, otherwise false.
- **ReleaseDuration:** (minutes: 1-525600) Default release duration.
- **MaxReleaseDuration:** (minutes: 1-525600) Default maximum release duration.
- **ISAReleaseDuration:** (minutes: 1-525600) Default Information Systems Administrator (ISA) release duration.
- **MaxConcurrentRequests:** (0-999, default: 1) Maximum number of concurrent password requests for this account. A value of zero denotes unlimited requests.
- **AutoManagementFlag:** True if password auto-management is enabled, otherwise false.
    - **DSSAutoManagementFlag:** True if DSS key auto-management is enabled, otherwise false.
    - **CheckPasswordFlag:** True to enable password testing, otherwise false.

  - **ChangePasswordAfterAnyReleaseFlag:** True to change passwords on release of a request, otherwise false.
  - **ResetPasswordOnMismatchFlag:** True to queue a password change when scheduled password test fails, otherwise false.
  - **ChangeFrequencyType:** The change frequency for scheduled password changes:
    - **first:** Changes scheduled for the first day of the month.
    - **last:** Changes scheduled for the last day of the month.
    - **xdays:** Changes scheduled every x days (**ChangeFrequencyDays**).
  - **ChangeFrequencyDays:** (days: 1-999) When **ChangeFrequencyType** is **xdays**, password changes take place this configured number of days.
  - **ChangeTime:** (24hr format: 00:00-23:59) UTC time of day scheduled password changes take place.
- **ParentAccountID:** If this is a subscribed account (**IsSubscribedAccount**), this is the ID of the parent managed account.
- **IsSubscribedAccount:** True if the account is a synced or subscribed account, otherwise false.
- **LastChangeDate:** The date and time of the last password change.
- **NextChangeDate:** The date and time of the next scheduled password change.
- **IsChanging:** True if the account credentials are in the process of changing, otherwise false.
- **ChangeState:** The change state of the account credentials:
  - **0:** Idle / No change taking place or scheduled within 5 minutes.
  - **1:** Changing / Managed Account Credential currently changing.
  - **2:** Queued / Managed Account Credential is queued to change or scheduled to change within 5 minutes.
- **UseOwnCredentials:** True if the current account credentials should be used during change operations, otherwise false.
- **WorkgroupID:** ID of the assigned Workgroup.
- **ObjectID:** (required when **Platform.RequiresObjectID** is true). ObjectID of the account (if applicable).

For more information, please see Configure Subscriber Accounts at https://www.beyondtrust.com/docs/beyondinsight-password-safe/ps/admin/managed-accounts.htm#ConfigureAccounts.

Response Code

200 - Request successful. Managed Account in the response body.

For more information, please see "Common Response Codes" on page 17.

GET ManagedSystems/{systemID}/ManagedAccounts

Purpose

Returns a list of managed accounts by managed system ID.

Required Permissions

Password Safe Account Management (Read).

URL Parameters

systemID: ID of the managed system.

Request Body

None.

Response Body

Content-Type: application/json

```
[
{
    ManagedAccountID : int,
    ManagedSystemID : int,
    DomainName : string,
    AccountName : string,
    DistinguishedName : string,
    PasswordFallbackFlag : bool,
    UserPrincipalName : string,
    SAMAccountName : string,
    LoginAccountFlag : bool,
    Description : string,
    PasswordRuleID : int,
    ApiEnabled : bool,
    ReleaseNotificationEmail : string,
    ChangeServicesFlag : bool,
    RestartServicesFlag : bool,
    ChangeTasksFlag : bool,
    ReleaseDuration : int,
    MaxReleaseDuration : int,
    ISAReleaseDuration : int,
    MaxConcurrentRequests : int,

    AutoManagementFlag : bool,
    DSSAutoManagementFlag : bool,
    CheckPasswordFlag : bool,
```

```
    ResetPasswordOnMismatchFlag : bool,
    ChangePasswordAfterAnyReleaseFlag : bool,
    ChangeFrequencyType : string,
    ChangeFrequencyDays : int,
    ChangeTime : string,

    ParentAccountID : int, // can be null
    IsSubscribedAccount : bool,
    LastChangeDate : datetime, // can be null
    NextChangeDate : datetime, // can be null
    IsChanging : bool,
    ChangeState : int,
    UseOwnCredentials : bool,
    WorkgroupID : int // can be null
    ChangeIISAppPoolFlag : bool,
    RestartIISAppPoolFlag : bool,
    WorkgroupID : int, // can be null
    ChangeWindowsAutoLogonFlag : bool,
    ChangeComPlusFlag : bool,
    ChangeDComFlag : bool,
    ChangeSComFlag : bool,

    },
    …
]
```

Response Body Details

- **DomainName:** The domain name for a domain-type account.
- **AccountName:** The name of the account.
- **DistinguishedName:** The distinguished name of an LDAP managed account.
- **PasswordFallbackFlag:** True if failed DSS authentication can fall back to password authentication, otherwise false.
- **UserPrincipalName:** (Active Directory managed systems only) The account user principal name of an Active Directory account.
- **SAMAccountName:** (Active Directory managed systems only) The account SAM account name of an Active Directory account.
- **LoginAccountFlag:** True if the account should use the managed system login account for SSH sessions, otherwise false.
- **Description:** A description of the account.
- **PasswordRuleID:** ID of the password rule assigned to this managed account.
- **ApiEnabled:** True if the account can be requested through the API, otherwise false.
- **ReleaseNotificationEmail:** Email address used for notification emails related to this managed account.
- **ChangeServicesFlag:** True if services run as this user should be updated with the new password after a password change, otherwise false.
- **RestartServicesFlag:** True if services should be restarted after the run as password is changed (**ChangeServicesFlag**), otherwise false.
- **ChangeTasksFlag:** True if scheduled tasks run as this user should be updated with the new password after a password change, otherwise false.
- **ReleaseDuration:** (minutes: 1-525600) Default release duration.
- **MaxReleaseDuration:** (minutes: 1-525600) Default maximum release duration.
- **ISAReleaseDuration:** (minutes: 1-525600) Default Information Systems Administrator (ISA) release duration.

- **MaxConcurrentRequests:** (0-999, default: 1) Maximum number of concurrent password requests for this account. A value of zero denotes unlimited requests.
- **AutoManagementFlag:** True if password auto-management is enabled, otherwise false.
    - **DSSAutoManagementFlag:** True if DSS key auto-management is enabled, otherwise false.
    - **CheckPasswordFlag:** True to enable password testing, otherwise false.
    - **ChangePasswordAfterAnyReleaseFlag:** True to change passwords on release of a request, otherwise false.
    - **ResetPasswordOnMismatchFlag:** True to queue a password change when scheduled password test fails, otherwise false.
    - **ChangeFrequencyType:** The change frequency for scheduled password changes:
        - **first:** Changes scheduled for the first day of the month.
        - **last:** Changes scheduled for the last day of the month.
        - **xdays:** Changes scheduled every x days (**ChangeFrequencyDays**).
    - **ChangeFrequencyDays:** (days: 1-999) When **ChangeFrequencyType** is **xdays**, password changes take place this configured number of days.
    - **ChangeTime:** (24hr format: 00:00-23:59) UTC time of day scheduled password changes take place.
- **ParentAccountID:** If this is a subscribed account (**IsSubscribedAccount**), this is the ID of the parent managed account.
- **IsSubscribedAccount:** True if the account is a synced or subscribed account, otherwise false.
- **LastChangeDate:** The date and time of the last password change.
- **NextChangeDate:** The date and time of the next scheduled password change.
- **IsChanging:** True if the account credentials are in the process of changing, otherwise false.
- **ChangeState:** The change state of the account credentials:
    - **0:** Idle / no change taking place or scheduled within 5 minutes.
    - **1:** Changing / managed account credential currently changing.
    - **2:** Queued / managed account credential is queued to change or scheduled to change within 5 minutes.
- **WorkgroupID:** ID of the assigned Workgroup.

> *For more information, please see Configure Subscriber Accounts at https://www.beyondtrust.com/docs/beyondinsight-password-safe/ps/admin/managed-accounts.htm#ConfigureAccounts.*

Response Codes

200 - Request successful. Managed Account in the response body.

> *For more information, please see "Common Response Codes" on page 17.*

GET ManagedSystems/{systemID}/ManagedAccounts?name={name}

Purpose

Returns a managed account by managed system ID and managed account name.

Required Permissions

Password Safe Account Management (Read).

URL Parameters

systemID: ID of the managed system.

Query Parameters

name: Name of the managed account.

Request Body

None.

Response Body

Content-Type: application/json

```
{
    ManagedAccountID : int,
    ManagedSystemID : int,
    DomainName : string,
    AccountName : string,
    DistinguishedName : string,
    PasswordFallbackFlag : bool,
    UserPrincipalName : string,
    SAMAccountName : string,
    LoginAccountFlag : bool,
    Description : string,
    PasswordRuleID : int,
    ApiEnabled : bool,
    ReleaseNotificationEmail : string,
    ChangeServicesFlag : bool,
    RestartServicesFlag : bool,
    ChangeTasksFlag : bool,
    ReleaseDuration : int,
    MaxReleaseDuration : int,
    ISAReleaseDuration : int,
    MaxConcurrentRequests : int,
```

```
    AutoManagementFlag : bool,
    DSSAutoManagementFlag : bool,
    CheckPasswordFlag : bool,
    ResetPasswordOnMismatchFlag : bool,
    ChangePasswordAfterAnyReleaseFlag : bool,
    ChangeFrequencyType : string,
    ChangeFrequencyDays : int,
    ChangeTime : string,

    ParentAccountID : int, // can be null
    IsSubscribedAccount : bool,
    LastChangeDate: datetime, // can be null
    NextChangeDate: datetime, // can be null
    IsChanging: bool
    ChangeState : int,
    UseOwnCredentials: bool,
    WorkgroupID : int // can be null
    ChangeIISAppPoolFlag : bool,
    RestartIISAppPoolFlag : bool,
}
```

Response Body Details

- **DomainName:** The domain name for a domain-type account.
- **AccountName:** The name of the account.
- **DistinguishedName:** The distinguished name of an LDAP managed account.
- **PasswordFallbackFlag:** True if failed DSS authentication can fall back to password authentication, otherwise false.
- **UserPrincipalName:** (Active Directory managed systems only) The account user principal name of an Active Directory account.
- **SAMAccountName:** (Active Directory managed systems only) The account SAM account name of an Active Directory account.
- **LoginAccountFlag:** True if the account should use the managed system login account for SSH sessions, otherwise false.
- **Description:** A description of the account.
- **PasswordRuleID:** ID of the password rule assigned to this managed account.
- **ApiEnabled:** True if the account can be requested through the API, otherwise false.
- **ReleaseNotificationEmail:** Email address used for notification emails related to this managed account.
- **ChangeServicesFlag:** True if services run as this user should be updated with the new password after a password change, otherwise false.
- **RestartServicesFlag:** True if services should be restarted after the run as password is changed (**ChangeServicesFlag**), otherwise false.
- **ChangeTasksFlag:** True if scheduled tasks run as this user should be updated with the new password after a password change, otherwise false.
- **ReleaseDuration:** (minutes: 1-525600) Default release duration.
- **MaxReleaseDuration:** (minutes: 1-525600) Default maximum release duration.
- **ISAReleaseDuration:** (minutes: 1-525600) Default Information Systems Administrator (ISA) release duration.
- **MaxConcurrentRequests:** (0-999, default: 1) Maximum number of concurrent password requests for this account. A value of zero denotes unlimited requests.

- **AutoManagementFlag:** True if password auto-management is enabled, otherwise false.
    - **DSSAutoManagementFlag:** True if DSS key auto-management is enabled, otherwise false.
    - **CheckPasswordFlag:** True to enable password testing, otherwise false.
    - **ChangePasswordAfterAnyReleaseFlag:** True to change passwords on release of a request, otherwise false.
    - **ResetPasswordOnMismatchFlag:** True to queue a password change when scheduled password test fails, otherwise false.
    - **ChangeFrequencyType:** The change frequency for scheduled password changes:
        - **first:** Changes scheduled for the first day of the month.
        - **last:** Changes scheduled for the last day of the month.
        - **xdays:** Changes scheduled every x days (**ChangeFrequencyDays**).
    - **ChangeFrequencyDays:** (days: 1-999) When **ChangeFrequencyType** is **xdays**, password changes take place this configured number of days.
    - **ChangeTime:** (24hr format: 00:00-23:59) UTC time of day scheduled password changes take place.
- **ParentAccountID:** If this is a subscribed account (**IsSubscribedAccount**), this is the ID of the parent managed account.
- **IsSubscribedAccount:** True if the account is a synced or subscribed account, otherwise false.
- **LastChangeDate:** The date and time of the last password change.
- **NextChangeDate:** The date and time of the next scheduled password change.
- **IsChanging:** True if the account credentials are in the process of changing, otherwise false.
- **ChangeState:** The change state of the account credentials:
    - **0:** Idle / No change taking place or scheduled within 5 minutes.
    - **1:** Changing / Managed Account Credential currently changing.
    - **2:** Queued / Managed Account Credential is queued to change or scheduled to change within 5 minutes.
- **UseOwnCredentials:** True if the current account credentials should be used during change operations, otherwise false.
- **WorkgroupID:** ID of the assigned Workgroup.

> *For more information, please see Configure Subscriber Accounts at https://www.beyondtrust.com/docs/beyondinsight-password-safe/ps/admin/managed-accounts.htm#ConfigureAccounts.*

Response Codes

200 - Request successful. Managed Account in the response body.

PUT ManagedAccounts/{id}

Purpose

Updates an existing managed account by ID.

Required Permissions

Password Safe Account Management (Read/Write).

URL Parameters

- **id:** ID of the managed account.
- **version**: (optional, default: 3.0) Request body model version (3.0, 3.1, 3.2, 3.3, 3.4, 3.5).

Request Body (version 3.0)

Content-Type: application/json

```
{
    AccountName : string,
    ManagedSystemID: int,
    Password : string,
    PrivateKey : string,
    Passphrase : string,
    PasswordFallbackFlag : bool,
    LoginAccountFlag : bool,
    Description : string,
    PasswordRuleID : int,
    ApiEnabled : bool,
    ReleaseNotificationEmail : string,
    ChangeServicesFlag : bool,
    RestartServicesFlag : bool,
    ChangeTasksFlag : bool,
    ReleaseDuration : int,
    MaxReleaseDuration : int,
    ISAReleaseDuration : int,
    MaxConcurrentRequests : int,

    AutoManagementFlag : bool,
    DSSAutoManagementFlag : bool,
    CheckPasswordFlag : bool,
    ResetPasswordOnMismatchFlag : bool,
    ChangePasswordAfterAnyReleaseFlag : bool,
    ChangeFrequencyType : string,
    ChangeFrequencyDays : int,
    ChangeTime : string,
    NextChangeDate : date-formatted string
}
```

Request Body (version 3.1)

Content-Type: application/json

```
{
    AccountName : string,
    Password : string,
    DomainName : string,
    UserPrincipalName : string,
    SAMAccountName : string,
    DistinguishedName : string,
    PrivateKey : string,
    Passphrase : string,
    PasswordFallbackFlag : bool,
    LoginAccountFlag : bool,
    Description : string,
    PasswordRuleID : int,
    ApiEnabled : bool,
    ReleaseNotificationEmail : string,
    ChangeServicesFlag : bool,
    RestartServicesFlag : bool,
    ChangeTasksFlag : bool,
    ReleaseDuration : int,
    MaxReleaseDuration : int,
    ISAReleaseDuration : int,
    MaxConcurrentRequests : int,

    AutoManagementFlag : bool,
    DSSAutoManagementFlag : bool,
    CheckPasswordFlag : bool,
    ResetPasswordOnMismatchFlag : bool,
    ChangePasswordAfterAnyReleaseFlag : bool,
    ChangeFrequencyType : string,
    ChangeFrequencyDays : int,
    ChangeTime : string,
    NextChangeDate : date-formatted string,
    UseOwnCredentials : bool
}
```

Request Body (version 3.2)

Content-Type: application/json

```
{
    AccountName : string,
    Password : string,
    DomainName : string,
    UserPrincipalName : string,
    SAMAccountName : string,
    DistinguishedName : string,
    PrivateKey : string,
    Passphrase : string,
```

```
    PasswordFallbackFlag : bool,
    LoginAccountFlag : bool,
    Description : string,
    PasswordRuleID : int,
    ApiEnabled : bool,
    ReleaseNotificationEmail : string,
    ChangeServicesFlag : bool,
    RestartServicesFlag : bool,
    ChangeTasksFlag : bool,
    ReleaseDuration : int,
    MaxReleaseDuration : int,
    ISAReleaseDuration : int,
    MaxConcurrentRequests : int,

    AutoManagementFlag : bool,
    DSSAutoManagementFlag : bool,
    CheckPasswordFlag : bool,
    ResetPasswordOnMismatchFlag : bool,
    ChangePasswordAfterAnyReleaseFlag : bool,
    ChangeFrequencyType : string,
    ChangeFrequencyDays : int,
    ChangeTime : string,
    NextChangeDate : date-formatted string,
    UseOwnCredentials : bool,
    ChangeIISAppPoolFlag : bool,
    RestartIISAppPoolFlag : bool
}
```

Request Body (version 3.3)

Content-Type: application/json

```
{
    AccountName : string,
    Password : string,
    DomainName : string,
    UserPrincipalName : string,
    SAMAccountName : string,
    DistinguishedName : string,
    PrivateKey : string,
    Passphrase : string,
    PasswordFallbackFlag : bool,
    LoginAccountFlag : bool,
    Description : string,
    PasswordRuleID : int,
    ApiEnabled : bool,
    ReleaseNotificationEmail : string,
    ChangeServicesFlag : bool,
    RestartServicesFlag : bool,
    ChangeTasksFlag : bool,
    ReleaseDuration : int,
    MaxReleaseDuration : int,
    ISAReleaseDuration : int,
```

```
    MaxConcurrentRequests : int,

    AutoManagementFlag : bool,
    DSSAutoManagementFlag : bool,
    CheckPasswordFlag : bool,
    ResetPasswordOnMismatchFlag : bool,
    ChangePasswordAfterAnyReleaseFlag : bool,
    ChangeFrequencyType : string,
    ChangeFrequencyDays : int,
    ChangeTime : string,
    NextChangeDate : date-formatted string,
    UseOwnCredentials : bool,
    ChangeIISAppPoolFlag : bool,
    RestartIISAppPoolFlag : bool,
    WorkgroupID : int // can be null
}
```

Request Body (version 3.4)

Content-Type: application/json

```
{
    AccountName : string,
    Password : string,
    DomainName : string,
    UserPrincipalName : string,
    SAMAccountName : string,
    DistinguishedName : string,
    PrivateKey : string,
    Passphrase : string,
    PasswordFallbackFlag : bool,
    LoginAccountFlag : bool,
    Description : string,
    PasswordRuleID : int,
    ApiEnabled : bool,
    ReleaseNotificationEmail : string,
    ChangeServicesFlag : bool,
    RestartServicesFlag : bool,
    ChangeTasksFlag : bool,
    ReleaseDuration : int,
    MaxReleaseDuration : int,
    ISAReleaseDuration : int,
    MaxConcurrentRequests : int,

    AutoManagementFlag : bool,
    DSSAutoManagementFlag : bool,
    CheckPasswordFlag : bool,
    ResetPasswordOnMismatchFlag : bool,
    ChangePasswordAfterAnyReleaseFlag : bool,
    ChangeFrequencyType : string,
    ChangeFrequencyDays : int,
    ChangeTime : string,
    NextChangeDate : date-formatted string,
```

```
    UseOwnCredentials : bool,
    ChangeIISAppPoolFlag : bool,
    RestartIISAppPoolFlag : bool,
    WorkgroupID : int // can be null,
    ChangeWindowsAutoLogonFlag : bool,
    ChangeComPlusFlag : bool,
    ChangeDComFlag : bool,
    ChangeSComFlag : bool,

}
```

Request Body (version 3.5)

Content-Type: application/json

```
{
    AccountName : string,
    Password : string,
    DomainName : string,
    UserPrincipalName : string,
    SAMAccountName : string,
    DistinguishedName : string,

    PrivateKey : string,
    Passphrase : string,
    PasswordFallbackFlag : bool,
    LoginAccountFlag : bool,
    Description : string,
    PasswordRuleID : int,
    ApiEnabled : bool,
    ReleaseNotificationEmail : string,
    ChangeServicesFlag : bool,
    RestartServicesFlag : bool,
    ChangeTasksFlag : bool,
    ReleaseDuration : int,
    MaxReleaseDuration : int,
    ISAReleaseDuration : int,
    MaxConcurrentRequests : int,

    AutoManagementFlag : bool,
        DSSAutoManagementFlag : bool,
        CheckPasswordFlag : bool,
        ResetPasswordOnMismatchFlag : bool,
        ChangePasswordAfterAnyReleaseFlag : bool,
        ChangeFrequencyType : string,
        ChangeFrequencyDays : int,
        ChangeTime : string,
        NextChangeDate : date-formatted string,

    UseOwnCredentials : bool,
    ChangeIISAppPoolFlag : bool,
    RestartIISAppPoolFlag : bool,
    WorkgroupID : int // can be null,
```

```
    ChangeWindowsAutoLogonFlag : bool,
    ChangeComPlusFlag : bool,
    ChangeDComFlag : bool,
    ChangeSComFlag : bool,

    ObjectID : string
}
```

Request Body Details

- **AccountName:** (required) The name of the account. Must be unique on the system. Max string length is 245.
- **ManagedSystemID:** (required) ID of the managed system.
- **Password:** (required if **AutoManagementFlag** is false) The account password.
- **DomainName:** (optional) This can be given but it must be exactly the same as the directory. If empty or null, it is automatically populated from the parent managed system/directory. Max string length is 50.
- **UserPrincipalName:** (required for Active Directory managed systems only) The Active Directory user principal name. Max string length is 500.
- **SAMAccountName:** (required for Active Directory managed systems only) The Active Directory SAM account name (maximum 20 characters). Max string length is 20.
- **DistinguishedName:** (required for LDAP Directory managed systems only) The LDAP distinguished name. Max string length is 1000.
- **PrivateKey:** DSS private key. Can be set if **Platform.DSSFlag** is true.
- **Passphrase:** (required when **PrivateKey** is an encrypted DSS key) DSS passphrase. Can be set if **Platform.DSSFlag** is true.
- **PasswordFallbackFlag:** (default: false) True if failed DSS authentication can fall back to password authentication, otherwise false. Can be set if **Platform.DSSFlag** is true.
- **LoginAccountFlag:** True if the account should use the managed system login account for SSH sessions, otherwise false. Can be set when the **ManagedSystem.LoginAccountID** is set.
- **Description:** A description of the account. Max string length is 1024.
- **PasswordRuleID:** (default: 0) ID of the password rule assigned to this managed account.
- **ApiEnabled:** (default: false) True if the account can be requested through the API, otherwise false.
- **ReleaseNotificationEmail:** Email address used for notification emails related to this managed account. Max string length is 255.
- **ChangeServicesFlag:** (default: false) True if services run as this user should be updated with the new password after a password change, otherwise false.
- **RestartServicesFlag:** (default: false) True if services should be restarted after the run as password is changed (**ChangeServicesFlag**), otherwise false.
- **ChangeTasksFlag:** (default: false) True if scheduled tasks run as this user should be updated with the new password after a password change, otherwise false.
- **ReleaseDuration:** (minutes: 1-525600, default: 120) Default release duration.
- **MaxReleaseDuration:** (minutes: 1-525600, default: 525600) Default maximum release duration.
- **ISAReleaseDuration:** (minutes: 1-525600, default: 120) Default Information Systems Administrator (ISA) release duration.
- **MaxConcurrentRequests:** (0-999, 0 is unlimited, default: 1) Maximum number of concurrent password requests for this account.
- **AutoManagementFlag:** (default: false) True if password auto-management is enabled, otherwise false.
    - **DSSAutoManagementFlag:** (default: false) True if DSS key auto-management is enabled, otherwise false. If set to true, and no **PrivateKey** is provided, immediately attempts to generate and set a new public key on the server. Can be set if

Platform.DSSAutoManagementFlag is true.

- **CheckPasswordFlag:** (default: false) True to enable password testing, otherwise false.
- **ChangePasswordAfterAnyReleaseFlag:** (default: false) True to change passwords on release of a request, otherwise false.
- **ResetPasswordOnMismatchFlag:** (default: false) True to queue a password change when scheduled password test fails, otherwise false.
- **ChangeFrequencyType:** (default: first) The change frequency for scheduled password changes:
  - **first:** Changes scheduled for the first day of the month.
  - **last:** Changes scheduled for the last day of the month.
  - **xdays:** Changes scheduled every x days (**ChangeFrequencyDays**).
- **ChangeFrequencyDays:** (days: 1-999) When **ChangeFrequencyType** is **xdays**, password changes take place this configured number of days.
- **ChangeTime:** (24hr format: 00:00-23:59, default: 23:30) UTC time of day scheduled password changes take place.
- **NextChangeDate:** (date format: YYYY-MM-DD) UTC date when next scheduled password change occurs. If the **NextChangeDate** + **ChangeTime** is in the past, password change occurs at the nearest future **ChangeTime**.

- **UseOwnCredentials:** (version 3.1+) True if the current account credentials should be used during change operations, otherwise false.
- **ChangeIISAppPoolFlag:** (version 3.2 only) True if IIS Application Pools run, as this user should be updated with the new password after a password change, otherwise false.
- **RestartIISAppPoolFlag:** (version 3.2 only) True if IIS Application Pools should be restarted after the run as password is changed (**ChangeIISAppPoolFlag**), otherwise false.
- **WorkgroupID:** ID of the assigned Workgroup.
- **ChangeWindowsAutoLogonFlag:** (default: false) True if Windows Auto Logon should be updated with the new password after a password change, otherwise false.
- **ChangeComPlusFlag:** (default: false) True if COM+ Apps should be updated with the new password after a password change, otherwise false.
- **ChangeDComFlag:** (default: false) True if DCOM Apps should be updated with the new password after a password change, otherwise false.
- **ChangeSComFlag:** (default: false) True if SCOM Identities should be updated with the new password after a password change, otherwise false.
- **ObjectID:** (required when **Platform.RequiresObjectID** is true). ObjectID of the account (if applicable). Max string length is 36.

Response Body

Content-Type: application/json

```
{
    ManagedAccountID : int,
    ManagedSystemID : int,
    DomainName : string,
    AccountName : string,
    DistinguishedName : string,
    PasswordFallbackFlag : bool,
    LoginAccountFlag : bool,
    Description : string,
```

```
    PasswordRuleID : int,
    ApiEnabled : bool,
    ReleaseNotificationEmail : string,
    ChangeServicesFlag : bool,
    RestartServicesFlag : bool,
    ChangeTasksFlag : bool,
    ReleaseDuration : int,
    MaxReleaseDuration : int,
    ISAReleaseDuration : int,
    MaxConcurrentRequests : int,

    AutoManagementFlag : bool,
    DSSAutoManagementFlag : bool,
    CheckPasswordFlag : bool,
    ResetPasswordOnMismatchFlag : bool,
    ChangePasswordAfterAnyReleaseFlag : bool,
    ChangeFrequencyType : string,
    ChangeFrequencyDays : int,
    ChangeTime : string,

    ParentAccountID : int, // can be null
    IsSubscribedAccount : bool,
    LastChangeDate: datetime, // can be null
    NextChangeDate: datetime, // can be null
    IsChanging: bool,
    ChangeState : int,
    UseOwnCredentials : bool,
    ChangeIISAppPoolFlag : bool,
    RestartIISAppPoolFlag : bool,
    WorkgroupID : int, // can be null
    ChangeWindowsAutoLogonFlag : bool,
    ChangeComPlusFlag : bool,
    ChangeDComFlag : bool,
    ChangeSComFlag : bool,
    ObjectID : string
}
```

Response Codes

200 - Request successful. Managed Account in the response body.

For more information, please see "Common Response Codes" on page 17.

POST ManagedSystems/{systemID}/ManagedAccounts

Purpose

Creates a new managed account in the managed system referenced by ID.

Required Permissions

Password Safe Account Management (Read/Write).

URL Parameters

systemID: ID of the managed system.

Query Parameters

version: (optional, default: 3.0) Request body model version (3.0, 3.1, 3.2, 3.3, 3.4, 3.5).

Request Body (version 3.0)

Content-Type: application/json

```
{
    AccountName : string,
    Password : string,
    DomainName : string,
    UserPrincipalName : string,
    SAMAccountName : string,
    DistinguishedName : string,
    PrivateKey : string,
    Passphrase : string,
    PasswordFallbackFlag : bool,
    LoginAccountFlag : bool,
    Description : string,
    PasswordRuleID : int,
    ApiEnabled : bool,
    ReleaseNotificationEmail : string,
    ChangeServicesFlag : bool,
    RestartServicesFlag : bool,
    ChangeTasksFlag : bool,
    ReleaseDuration : int,
    MaxReleaseDuration : int,
    ISAReleaseDuration : int,
    MaxConcurrentRequests : int,

    AutoManagementFlag : bool,
    DSSAutoManagementFlag : bool,
    CheckPasswordFlag : bool,
```

```
    ResetPasswordOnMismatchFlag : bool,
    ChangePasswordAfterAnyReleaseFlag : bool,
    ChangeFrequencyType : string,
    ChangeFrequencyDays : int,
    ChangeTime : string,
    NextChangeDate : date-formatted string
}
```

Request Body (version 3.1)

Content-Type: application/json

```
{
    AccountName : string,
    Password : string,
    DomainName : string,
    UserPrincipalName : string,
    SAMAccountName : string,
    DistinguishedName : string,
    PrivateKey : string,
    Passphrase : string,
    PasswordFallbackFlag : bool,
    LoginAccountFlag : bool,
    Description : string,
    PasswordRuleID : int,
    ApiEnabled : bool,
    ReleaseNotificationEmail : string,
    ChangeServicesFlag : bool,
    RestartServicesFlag : bool,
    ChangeTasksFlag : bool,
    ReleaseDuration : int,
    MaxReleaseDuration : int,
    ISAReleaseDuration : int,
    MaxConcurrentRequests : int,

    AutoManagementFlag : bool,
    DSSAutoManagementFlag : bool,
    CheckPasswordFlag : bool,
    ResetPasswordOnMismatchFlag : bool,
    ChangePasswordAfterAnyReleaseFlag : bool,
    ChangeFrequencyType : string,
    ChangeFrequencyDays : int,
    ChangeTime : string,
    NextChangeDate : date-formatted string,
    UseOwnCredentials : bool
}
```

Request Body (version 3.2)

Content-Type: application/json

```
{
    AccountName : string,
    Password : string,
    DomainName : string,
    UserPrincipalName : string,
    SAMAccountName : string,
    DistinguishedName : string,
    PrivateKey : string,
    Passphrase : string,
    PasswordFallbackFlag : bool,
    LoginAccountFlag : bool,
    Description : string,
    PasswordRuleID : int,
    ApiEnabled : bool,
    ReleaseNotificationEmail : string,
    ChangeServicesFlag : bool,
    RestartServicesFlag : bool,
    ChangeTasksFlag : bool,
    ReleaseDuration : int,
    MaxReleaseDuration : int,
    ISAReleaseDuration : int,
    MaxConcurrentRequests : int,

    AutoManagementFlag : bool,
    DSSAutoManagementFlag : bool,
    CheckPasswordFlag : bool,
    ResetPasswordOnMismatchFlag : bool,
    ChangePasswordAfterAnyReleaseFlag : bool,
    ChangeFrequencyType : string,
    ChangeFrequencyDays : int,
    ChangeTime : string,
    NextChangeDate : date-formatted string,
    UseOwnCredentials : bool,
    ChangeIISAppPoolFlag : bool,
    RestartIISAppPoolFlag : bool
}
```

Request Body (version 3.3)

Content-Type: application/json

```
{
    AccountName : string,
    Password : string,
    DomainName : string,
    UserPrincipalName : string,
    SAMAccountName : string,
    DistinguishedName : string,
    PrivateKey : string,
    Passphrase : string,
    PasswordFallbackFlag : bool,
    LoginAccountFlag : bool,
    Description : string,
```

```
    PasswordRuleID : int,
    ApiEnabled : bool,
    ReleaseNotificationEmail : string,
    ChangeServicesFlag : bool,
    RestartServicesFlag : bool,
    ChangeTasksFlag : bool,
    ReleaseDuration : int,
    MaxReleaseDuration : int,
    ISAReleaseDuration : int,
    MaxConcurrentRequests : int,

    AutoManagementFlag : bool,
    DSSAutoManagementFlag : bool,
    CheckPasswordFlag : bool,
    ResetPasswordOnMismatchFlag : bool,
    ChangePasswordAfterAnyReleaseFlag : bool,
    ChangeFrequencyType : string,
    ChangeFrequencyDays : int,
    ChangeTime : string,
    NextChangeDate : date-formatted string,
    UseOwnCredentials : bool,
    ChangeIISAppPoolFlag : bool,
    RestartIISAppPoolFlag : bool,
    WorkgroupID : int // can be null
}
```

Request Body (version 3.4)

Content-Type: application/json

```
{
    AccountName : string,
    Password : string,
    DomainName : string,
    UserPrincipalName : string,
    SAMAccountName : string,
    DistinguishedName : string,
    PrivateKey : string,
    Passphrase : string,
    PasswordFallbackFlag : bool,
    LoginAccountFlag : bool,
    Description : string,
    PasswordRuleID : int,
    ApiEnabled : bool,
    ReleaseNotificationEmail : string,
    ChangeServicesFlag : bool,
    RestartServicesFlag : bool,
    ChangeTasksFlag : bool,
    ReleaseDuration : int,
    MaxReleaseDuration : int,
    ISAReleaseDuration : int,
    MaxConcurrentRequests : int,
```

```
    AutoManagementFlag : bool,
    DSSAutoManagementFlag : bool,
    CheckPasswordFlag : bool,
    ResetPasswordOnMismatchFlag : bool,
    ChangePasswordAfterAnyReleaseFlag : bool,
    ChangeFrequencyType : string,
    ChangeFrequencyDays : int,
    ChangeTime : string,
    NextChangeDate : date-formatted string,
    UseOwnCredentials : bool,
    ChangeIISAppPoolFlag : bool,
    RestartIISAppPoolFlag : bool,
    WorkgroupID : int // can be null,
    ChangeWindowsAutoLogonFlag : bool,
    ChangeComPlusFlag : bool,
    ChangeDComFlag : bool,
    ChangeSComFlag : bool,

}
```

Request Body (version 3.5)

Content-Type: application/json

```
{
    AccountName : string,
    Password : string,
    DomainName : string,
    UserPrincipalName : string,
    SAMAccountName : string,
    DistinguishedName : string,

    PrivateKey : string,
    Passphrase : string,
    PasswordFallbackFlag : bool,
    LoginAccountFlag : bool,
    Description : string,
    PasswordRuleID : int,
    ApiEnabled : bool,
    ReleaseNotificationEmail : string,
    ChangeServicesFlag : bool,
    RestartServicesFlag : bool,
    ChangeTasksFlag : bool,
    ReleaseDuration : int,
    MaxReleaseDuration : int,
    ISAReleaseDuration : int,
    MaxConcurrentRequests : int,

    AutoManagementFlag : bool,
        DSSAutoManagementFlag : bool,
        CheckPasswordFlag : bool,
        ResetPasswordOnMismatchFlag : bool,
        ChangePasswordAfterAnyReleaseFlag : bool,
```

```
        ChangeFrequencyType : string,
        ChangeFrequencyDays : int,
        ChangeTime : string,
        NextChangeDate : date-formatted string,

    UseOwnCredentials : bool,
    ChangeIISAppPoolFlag : bool,
    RestartIISAppPoolFlag : bool,
    WorkgroupID : int // can be null,
    ChangeWindowsAutoLogonFlag : bool,
    ChangeComPlusFlag : bool,
    ChangeDComFlag : bool,
    ChangeSComFlag : bool,

    ObjectID : string
}
```

Request Body Details

- **AccountName:** (required) The name of the account. Must be unique on the system. Max string length is 245.
- **Password:** (required if **AutoManagementFlag** is false) The account password.
- **DomainName:** (optional) This can be given but it must be exactly the same as the directory. If empty or null, it is automatically populated from the parent managed system/directory. Max string length is 50.
- **UserPrincipalName:** (required for Active Directory and Entra ID managed systems only) The Active Directory user principal name. Max string length is 500.
- **SAMAccountName:** (required for Active Directory managed systems, optional for Entra ID managed systems) The Active Directory SAM account name (Maximum 20 characters). Max string length is 20.
- **DistinguishedName:** (required for LDAP Directory managed systems only) The LDAP distinguished name. Max string length is 1000.
- **PrivateKey:** DSS private key. Can be set if **Platform.DSSFlag** is true.
- **Passphrase:** (required when **PrivateKey** is an encrypted DSS key) DSS passphrase. Can be set if **Platform.DSSFlag** is true.
- **PasswordFallbackFlag:** (default: false) True if failed DSS authentication can fall back to password authentication, otherwise false. Can be set if **Platform.DSSFlag** is true.
- **LoginAccountFlag:** True if the account should use the managed system login account for SSH sessions, otherwise false. Can be set when the **ManagedSystem.LoginAccountID** is set.
- **Description:** A description of the account. Max string length is 1024.
- **PasswordRuleID:** (default: 0) ID of the password rule assigned to this managed account.
- **ApiEnabled:** (default: false) True if the account can be requested through the API, otherwise false.
- **ReleaseNotificationEmail:** Email address used for notification emails related to this managed account. Max string length is 255.
- **ChangeServicesFlag:** (default: false) True if services run as this user should be updated with the new password after a password change, otherwise false.
- **RestartServicesFlag:** (default: false) True if services should be restarted after the run as password is changed (**ChangeServicesFlag**), otherwise false.
- **ChangeTasksFlag:** (default: false) True if scheduled tasks run as this user should be updated with the new password after a password change, otherwise false.
- **ReleaseDuration:** (minutes: 1-525600, default: 120) Default release duration.

- **MaxReleaseDuration:** (minutes: 1-525600, default: 525600) Default maximum release duration.
- **ISAReleaseDuration:** (minutes: 1-525600, default: 120) Default Information Systems Administrator (ISA) release duration.
- **MaxConcurrentRequests:** (0-999, 0 is unlimited, default: 1) Maximum number of concurrent password requests for this account.
- **AutoManagementFlag:** (default: false) True if password auto-management is enabled, otherwise false.
    - **DSSAutoManagementFlag:** (default: false) True if DSS key auto-management is enabled, otherwise false. If set to true, and no **PrivateKey** is provided, immediately attempts to generate and set a new public key on the server. Can be set if **Platform.DSSAutoManagementFlag** is true.
    - **CheckPasswordFlag:** (default: false) True to enable password testing, otherwise false.
    - **ChangePasswordAfterAnyReleaseFlag:** (default: false) True to change passwords on release of a request, otherwise false.
    - **ResetPasswordOnMismatchFlag:** (default: false) True to queue a password change when scheduled password test fails, otherwise false.
    - **ChangeFrequencyType:** (default: first) The change frequency for scheduled password changes:
        - **first:** Changes scheduled for the first day of the month.
        - **last:** Changes scheduled for the last day of the month.
        - **xdays:** Changes scheduled every x days (**ChangeFrequencyDays**).
    - **ChangeFrequencyDays:** (days: 1-999) When **ChangeFrequencyType** is **xdays**, password changes take place this configured number of days.
    - **ChangeTime:** (24hr format: 00:00-23:59, default: 23:30) UTC time of day scheduled password changes take place.
    - **NextChangeDate:** (date format: YYYY-MM-DD) UTC date when next scheduled password change occurs. If the **NextChangeDate** + **ChangeTime** is in the past, password change occurs at the nearest future **ChangeTime**.
- **UseOwnCredentials:** (version 3.1+) True if the current account credentials should be used during change operations, otherwise false.
- **ChangeIISAppPoolFlag:** (version 3.2 only) True if IIS application pools run as this user should be updated with the new password after a password change, otherwise false.
- **RestartIISAppPoolFlag:** (version 3.2 only) True if IIS application pools should be restarted after the run as password is changed (**ChangeIISAppPoolFlag**), otherwise false.
- **WorkgroupID:** ID of the assigned Workgroup.
- **ChangeWindowsAutoLogonFlag:** (default: false) True if Windows Auto Logon should be updated with the new password after a password change, otherwise false.
- **ChangeComPlusFlag:** (default: false) True if COM+ Apps should be updated with the new password after a password change, otherwise false.
- **ChangeDComFlag:** (default: false) True if DCOM Apps should be updated with the new password after a password change, otherwise false.
- **ChangeSComFlag:** (default: false) True if SCOM Identities should be updated with the new password after a password change, otherwise false.
- **ObjectID:** (required when **Platform.RequiresObjectID** is true). ObjectID of the account (if applicable). Max string length is 36.

Response Body

Content-Type: application/json

```
{
    ManagedAccountID : int,
    ManagedSystemID : int,
    DomainName : string,
    AccountName : string,
    DistinguishedName : string,
    PasswordFallbackFlag : bool,
    UserPrincipalName : string,
    SAMAccountName : string,
    LoginAccountFlag : bool,
    Description : string,
    PasswordRuleID : int,
    ApiEnabled : bool,
    ReleaseNotificationEmail : string,
    ChangeServicesFlag : bool,
    RestartServicesFlag : bool,
    ChangeTasksFlag : bool,
    ReleaseDuration : int,
    MaxReleaseDuration : int,
    ISAReleaseDuration : int,
    MaxConcurrentRequests : int,

    AutoManagementFlag : bool,
    DSSAutoManagementFlag : bool,
    CheckPasswordFlag : bool,
    ResetPasswordOnMismatchFlag : bool,
    ChangePasswordAfterAnyReleaseFlag : bool,
    ChangeFrequencyType : string,
    ChangeFrequencyDays : int,
    ChangeTime : string,

    ParentAccountID : int, // can be null
    IsSubscribedAccount : bool,
    LastChangeDate : datetime, // can be null
    NextChangeDate : datetime, // can be null
    IsChanging : bool,
    ChangeState : int,
    UseOwnCredentials : bool,
    ChangeIISAppPoolFlag : bool,
    RestartIISAppPoolFlag : bool,
    WorkgroupID : int, // can be null
    ChangeWindowsAutoLogonFlag : bool,
    ChangeComPlusFlag : bool,
    ChangeDComFlag : bool,
    ChangeSComFlag : bool,
    ObjectID : string
}
```

Response Body Details

- **AccountName:** The name of the account.
- **PasswordFallbackFlag:** True if failed DSS authentication can fall back to password authentication, otherwise false.
- **UserPrincipalName:** (Active Directory and Entra ID managed systems only) The account user principal name of an Active Directory account.

- **SAMAccountName:** (Active Directory managed systems, optional for Entra ID managed systems) The account SAM account name of an Active Directory account.
- **LoginAccountFlag:** True if the account should use the managed system login account for SSH sessions, otherwise false.
- **Description:** A description of the account.
- **PasswordRuleID:** ID of the password rule assigned to this managed account.
- **ApiEnabled:** True if the account can be requested through the API, otherwise false.
- **ReleaseNotificationEmail:** Email address used for notification emails related to this managed account.
- **ChangeServicesFlag:** True if services run as this user should be updated with the new password after a password change, otherwise false.
- **RestartServicesFlag:** True if services should be restarted after the run as password is changed (**ChangeServicesFlag**), otherwise false.
- **ChangeTasksFlag:** True if scheduled tasks run as this user should be updated with the new password after a password change, otherwise false.
- **ReleaseDuration:** (minutes: 1-525600) Default release duration.
- **MaxReleaseDuration:** (minutes: 1-525600) Default maximum release duration.
- **ISAReleaseDuration:** (minutes: 1-525600) Default Information Systems Administrator (ISA) release duration.
- **MaxConcurrentRequests:** (0-999, 0 means unlimited) Maximum number of concurrent password requests for this account.
- **AutoManagementFlag:** True if password auto-management is enabled, otherwise false.
    - **DSSAutoManagementFlag:** True if DSS key auto-management is enabled, otherwise false.
    - **CheckPasswordFlag:** True to enable password testing, otherwise false.
    - **ChangePasswordAfterAnyReleaseFlag:** True to change passwords on release of a request, otherwise false.
    - **ResetPasswordOnMismatchFlag:** True to queue a password change when scheduled password test fails, otherwise false.
    - **ChangeFrequencyType:** The change frequency for scheduled password changes:
        - **first:** Changes scheduled for the first day of the month.
        - **last:** Changes scheduled for the last day of the month.
        - **xdays:** Changes scheduled every x days (**ChangeFrequencyDays**).
    - **ChangeFrequencyDays:** (days: 1-999) When **ChangeFrequencyType** is **xdays**, password changes take place this configured number of days.
    - **ChangeTime:** (24hr format: 00:00-23:59) UTC time of day scheduled password changes take place.
- **ParentAccountID:** If this is a subscribed account, this is the ID of the parent managed account.
- **IsSubscribedAccount:** True if the account is a synced or subscribed account, otherwise false.
- **LastChangeDate:** The date and time of the last password change.
- **NextChangeDate:** The date and time of the next scheduled password change.
- **IsChanging:** True if the account credentials are in the process of changing, otherwise false.
- **ChangeState:** The change state of the account credentials:
    - **0:** Idle / no change taking place or scheduled within 5 minutes.
    - **1:** Changing / managed account credential currently changing.
    - **2:** Queued / managed account credential is queued to change or scheduled to change within 5 minutes.
- **UseOwnCredentials:** True if the current account credentials should be used during change operations, otherwise false.

- **ChangeIISAppPoolFlag:** True if IIS application pools run as this user should be updated with the new password after a password change, otherwise false.
- **RestartIISAppPoolFlag:** True if IIS application pools should be restarted after the run as password is changed, otherwise false.
- **WorkgroupID:** ID of the assigned Workgroup.
- **ChangeWindowsAutoLogonFlag:** True if Windows auto logon should be updated with the new password after a password change, otherwise false.
- **ChangeComPlusFlag:** True if COM+ apps should be updated with the new password after a password change, otherwise false.
- **ChangeDComFlag:** True if DCOM apps should be updated with the new password after a password change, otherwise false.
- **ChangeSComFlag:** True if SCOM identities should be updated with the new password after a password change, otherwise false.
- **ObjectID:** ObjectID of the account (if applicable).

For more information, please see Configure Subscriber Accounts at https://www.beyondtrust.com/docs/beyondinsight-password-safe/ps/admin/managed-accounts.htm#ConfigureAccounts.

Response Codes

201 - Request successful. Managed Account in the response body.

For more information, please see "Common Response Codes" on page 17.

DELETE ManagedAccounts/{id}

Purpose

Deletes a managed account by ID.

Required Permissions

Password Safe Account Management (Read/Write).

URL Parameters

id: ID of the managed account.

Request Body

None.

Response Body

None.

Response Codes

200 - Request successful.

For more information, please see "Common Response Codes" on page 17.

DELETE ManagedSystems/{systemID}/ManagedAccounts/{accountName}

Purpose

Deletes a managed account by managed system ID and managed account name.

Required Permissions

Password Safe Account Management (Read/Write).

URL Parameters

- **systemID:** ID of the managed system.
- **accountName:** Name of the managed account.

Request Body

None.

Response Body

None.

Response Codes

200 - Request successful.

For more information, please see "Common Response Codes" on page 17.

DELETE ManagedSystems/{id}/ManagedAccounts

Purpose

Deletes all managed accounts on the managed system by ID.

Required Permissions

Password Safe Account Management (Read/Write).

URL Parameters

- **id**: ID of the managed system.

Request Body

None.

Response Body

None.

Response Codes

200 - Request successful.

For more information, please see "Common Response Codes" on page 17.

Managed Account Credentials

Quick Navigation

PUT ManagedAccounts/{managedAccountID}/Credentials

Purpose

Updates the credentials for a managed account, optionally applying the change to the managed system.

Required Permissions

Requires one of the following:

- Password Safe Account Management (Read/Write).
- ISA Role or Credentials Manager Role on a Smart Rule referencing the account.

URL Parameters

managedAccountID: ID of the managed account for which to set the credentials.

Request Body

Content-Type: application/json

```
{
    Password: string,
    PublicKey: string,
    PrivateKey: string,
    Passphrase: string,
    UpdateSystem: bool
}
```

Request Body Details

- **Password:** (optional) The new password to set. If not given, generates a new random password.
- **PublicKey:** (required if **PrivateKey** is given and **updateSystem** = true) The new public key to set on the host.

- **PrivateKey:** The private key to set (provide passphrase if encrypted).
- **Passphrase:** (optional) The passphrase to use for an encrypted private key.
- **UpdateSystem:** (default: true) Whether to update the credentials on the referenced system.

Response Body

None.

Response Codes

204 - Request successful. No content in body.

For more information, please see "Common Response Codes" on page 17.

PUT Credentials?workgroupName={workgroupName}&assetName={assetName}&accountName={accountName}

Purpose

Updates the credentials for a managed account by Workgroup name, asset name, and managed account name, optionally applying the change to the managed system.

Required Permissions

Requires one of the following:

- Password Safe Account Management (Read/Write).
- ISA Role or Credentials Manager Role on a Smart Rule referencing the account.

Query Parameters

- **workgroupName:** Name of the Workgroup.
- **assetName:** Name of the asset.
- **accountName:** Name of the managed account for which to set the credentials.

Request Body

Content-Type: application/json

```
{
    Password: string,
    PublicKey: string,
```

```
    PrivateKey: string,
    Passphrase: string,
    UpdateSystem: bool
}
```

Request Body Details

- **Password:** (optional) The new password to set. If not given, generates a new random password.
- **PublicKey:** (required if **PrivateKey** is given and **updateSystem** = true) The new public key to set on the host.
- **PrivateKey:** The private key to set (provide passphrase if encrypted).
- **Passphrase:** (optional) The passphrase to use for an encrypted private key.
- **UpdateSystem:** (default: true) Whether to update the credentials on the referenced system.

Response Body

None.

Response Codes

204 - Request Successful. No Response Body.

For more information, please see "Common Response Codes" on page 17.

POST ManagedAccounts/{managedAccountID}/Credentials/Test

Purpose

Tests the current credentials of a managed account.

Required Permissions

Password Safe Account Management (Read/Write).

URL Parameters

managedAccountID: ID of the managed account.

Request Body

None.

Response Body

Content-Type: application/json

```
{
    Success : bool
}
```

Response Body Details

Success: True if the credential test succeeded, otherwise false.

Response Codes

200 - Request Successful.

For more information, please see "Common Response Codes" on page 17.

POST ManagedAccounts/{managedAccountID}/Credentials/Change

Purpose

Changes the current credentials of a managed account.

Required Permissions

Password Safe Account Management (Read/Write).

URL Parameters

managedAccountID: ID of the managed account.

Request Body (optional)

Content-Type: application/json

```
{
    Queue : bool
}
```

Request Body Details

Queue: (default: false) True to queue the change for background processing, otherwise false. When **Queue** is false the credentials change is immediate.

Response Body

None.

Response Codes

204 - Request successful. No content in body.

For more information, please see "Common Response Codes" on page 17.

POST ManagedSystems/{systemId}/ManagedAccounts/Credentials/Change

Purpose

Queues credentials' changes for all active managed accounts for a managed system.

Required Permissions

Password Safe API Global Quarantine (Read/Write).

URL Parameters

systemId: ID of the managed system.

Request Body

None.

Response Body

None.

Response Codes

204 - Request successful. No content in body.

For more information, please see "Common Response Codes" on page 17.

Quick Rule Managed Accounts

Quick Navigation

GET QuickRules/{quickRuleID}/ManagedAccounts

Purpose

Returns a list of managed accounts by Quick Rule ID.

Required Permissions

Read access to the Quick Rule.

URL Parameters

quickRuleID: ID of the Quick Rule.

Request Body

None.

Response Body

Content-Type: application/json

```
[
    {
        ManagedAccountID : int,
        ManagedSystemID : int,
        DomainName : string,
        AccountName : string,
        DistinguishedName : string,
        PasswordFallbackFlag : bool,
        LoginAccountFlag : bool,
        Description : string,
        PasswordRuleID : int,
        ApiEnabled : bool,
        ReleaseNotificationEmail : string,
```

```
        ChangeServicesFlag : bool,
        RestartServicesFlag : bool,
        ChangeTasksFlag : bool,
        ReleaseDuration : int,
        MaxReleaseDuration : int,
        ISAReleaseDuration : int,
        MaxConcurrentRequests : int,

        AutoManagementFlag : bool,
        DSSAutoManagementFlag : bool,
        CheckPasswordFlag : bool,
        ResetPasswordOnMismatchFlag : bool,
        ChangePasswordAfterAnyReleaseFlag : bool,
        ChangeFrequencyType : string,
        ChangeFrequencyDays : int,
        ChangeTime : string,

        ParentAccountID : int, // can be null
        IsSubscribedAccount : bool,
        LastChangeDate : datetime, // can be null
        NextChangeDate : datetime, // can be null
        IsChanging : bool,
        ChangeState : int,
        UseOwnCredentials : bool,
        ChangeIISAppPoolFlag : bool,
        RestartIISAppPoolFlag : bool,
        WorkgroupID : int // can be null
        ChangeWindowsAutoLogonFlag : bool,
        ChangeComPlusFlag : bool,
        ChangeDComFlag : bool,
        ChangeSComFlag : bool,
    },
    …
]
```

Response Body Details

- **DomainName:** The domain name for a domain-type account.
- **AccountName:** The name of the account.
- **DistinguishedName:** The distinguished name of an LDAP managed account.
- **PasswordFallbackFlag:** True if failed DSS authentication can fall back to password authentication, otherwise false.
- **LoginAccountFlag:** True if the account should use the managed system login account for SSH sessions, otherwise false.
- **Description:** A description of the account.
- **PasswordRuleID:** ID of the password rule assigned to this managed account.
- **ApiEnabled:** True if the account can be requested through the API, otherwise false.
- **ReleaseNotificationEmail:** Email address used for notification emails related to this managed account.
- **ChangeServicesFlag:** True if services run as this user should be updated with the new password after a password change, otherwise false.
- **RestartServicesFlag:** True if services should be restarted after the run as password is changed (**ChangeServicesFlag**), otherwise false.

- **ChangeTasksFlag:** True if scheduled tasks run as this user should be updated with the new password after a password change, otherwise false.
- **ReleaseDuration:** (minutes: 1-525600) Default release duration.
- **MaxReleaseDuration:** (minutes: 1-525600) Default maximum release duration.
- **ISAReleaseDuration:** (minutes: 1-525600) Default Information Systems Administrator (ISA) release duration.
- **MaxConcurrentRequests:** (0-999, 0 is unlimited) Maximum number of concurrent password requests for this account.
- **AutoManagementFlag:** True if password auto-management is enabled, otherwise false.
    - **DSSAutoManagementFlag:** True if DSS key auto-management is enabled, otherwise false.
    - **CheckPasswordFlag:** True to enable password testing, otherwise false.
    - **ChangePasswordAfterAnyReleaseFlag:** True to change passwords on release of a request, otherwise false.
    - **ResetPasswordOnMismatchFlag:** True to queue a password change when scheduled password test fails, otherwise false.
    - **ChangeFrequencyType:** The change frequency for scheduled password changes:
        - **first:** Changes scheduled for the first day of the month.
        - **last:** Changes scheduled for the last day of the month.
        - **xdays:** Changes scheduled every x days (**ChangeFrequencyDays**).
    - **ChangeFrequencyDays:** (days: 1-999) When **ChangeFrequencyType** is **xdays**, password changes take place this configured number of days.
    - **ChangeTime:** (24hr format: 00:00-23:59) UTC time of day scheduled password changes take place.
- **ParentAccountID:** If this is a subscribed account (**IsSubscribedAccount**), this is the ID of the parent managed account.
- **IsSubscribedAccount:** True if the account is a synced or subscribed account, otherwise false.
- **LastChangeDate:** The date and time of the last password change.
- **NextChangeDate:** The date and time of the next scheduled password change.
- **IsChanging:** True if the account credentials are in the process of changing, otherwise false.
- **ChangeState:** The change state of the account credentials:
    - **0:** Idle / no change taking place or scheduled within 5 minutes.
    - **1:** Changing / managed account credential currently changing.
    - **2:** Queued / managed account credential is queued to change or scheduled to change within 5 minutes.
- **UseOwnCredentials:** True if the current account credentials should be used during change operations, otherwise false.
- **ChangeIISAppPoolFlag:** True if IIS application pools run as this user should be updated with the new password after a password change, otherwise false.
- **RestartIISAppPoolFlag:** True if IIS application pools should be restarted after the run as password is changed, otherwise false.
- **WorkgroupID:** ID of the assigned Workgroup.

> *For more information, please see Configure Subscriber Accounts at https://www.beyondtrust.com/docs/beyondinsight-password-safe/ps/admin/managed-accounts.htm#ConfigureAccounts.*

Response Codes

200 – Request successful. Managed Accounts in the response body.

For more information, please see "Common Response Codes" on page 17.

PUT QuickRules/{quickRuleID}/ManagedAccounts

Purpose

Updates the entire list of managed accounts in a Quick Rule by removing all **Managed Account Fields - Quick Group ID** filters and adding a new one with the managed accounts referenced by ID.

Required Permissions

- Password Safe Account Management (Read).
- Read/Write access to the Quick Rule.

URL Parameters

quickRuleID: ID of the Quick Rule.

Request Body

Content-Type: application/json

```
{
    AccountIDs: [ int, …]
}
```

Response Body

Content-Type: application/json

```
[
    {
        ManagedAccountID : int,
        ManagedSystemID : int,
        DomainName : string,
        AccountName : string,
        DistinguishedName : string,
        PasswordFallbackFlag : bool,
        LoginAccountFlag : bool,
        Description : string,
        PasswordRuleID : int,
        ApiEnabled : bool,
        ReleaseNotificationEmail : string,
        ChangeServicesFlag : bool,
        RestartServicesFlag : bool,
```

```
        ChangeTasksFlag : bool,
        ReleaseDuration : int,
        MaxReleaseDuration : int,
        ISAReleaseDuration : int,
        MaxConcurrentRequests : int,

        AutoManagementFlag : bool,
        DSSAutoManagementFlag : bool,
        CheckPasswordFlag : bool,
        ResetPasswordOnMismatchFlag : bool,
        ChangePasswordAfterAnyReleaseFlag : bool,
        ChangeFrequencyType : string,
        ChangeFrequencyDays : int,
        ChangeTime : string,
        ParentAccountID : int, // can be null

        IsSubscribedAccount : bool,
        LastChangeDate: datetime, // can be null
        NextChangeDate: datetime, // can be null
        IsChanging: bool,
        ChangeState : int,
        UseOwnCredentials : bool,
        ChangeIISAppPoolFlag : bool,
        RestartIISAppPoolFlag : bool,
        WorkgroupID : int // can be null
        ChangeWindowsAutoLogonFlag : bool,
        ChangeComPlusFlag : bool,
        ChangeDComFlag : bool,
        ChangeSComFlag : bool,
    },
    …
]
```

Response Body Details

- **DomainName:** The domain name for a domain-type account.
- **AccountName:** The name of the account.
- **DistinguishedName:** The distinguished name of an LDAP managed account.
- **PasswordFallbackFlag:** True if failed DSS authentication can fall back to password authentication, otherwise false.
- **LoginAccountFlag:** True if the account should use the managed system login account for SSH sessions, otherwise false.
- **Description:** A description of the account.
- **PasswordRuleID:** ID of the password rule assigned to this managed account.
- **ApiEnabled:** True if the account can be requested through the API, otherwise false.
- **ReleaseNotificationEmail:** Email address used for notification emails related to this managed account.
- **ChangeServicesFlag:** True if services run as this user should be updated with the new password after a password change, otherwise false.
- **RestartServicesFlag:** True if services should be restarted after the run as password is changed (**ChangeServicesFlag**), otherwise false.
- **ChangeTasksFlag:** True if scheduled tasks run as this user should be updated with the new password after a password change, otherwise false.

- **ReleaseDuration:** (minutes: 1-525600) Default release duration.
- **MaxReleaseDuration:** (minutes: 1-525600) Default maximum release duration.
- **ISAReleaseDuration:** (minutes: 1-525600) Default Information Systems Administrator (ISA) release duration.
- **MaxConcurrentRequests:** (0-999, 0 is unlimited) Maximum number of concurrent password requests for this account.
- **AutoManagementFlag:** True if password auto-management is enabled, otherwise false.
    - **DSSAutoManagementFlag:** True if DSS key auto-management is enabled, otherwise false.
    - **CheckPasswordFlag:** True to enable password testing, otherwise false.
    - **ChangePasswordAfterAnyReleaseFlag:** True to change passwords on release of a request, otherwise false.
    - **ResetPasswordOnMismatchFlag:** True to queue a password change when scheduled password test fails, otherwise false.
    - **ChangeFrequencyType:** The change frequency for scheduled password changes:
        - **first:** Changes scheduled for the first day of the month.
        - **last:** Changes scheduled for the last day of the month.
        - **xdays:** Changes scheduled every x days (**ChangeFrequencyDays**).
    - **ChangeFrequencyDays:** (days: 1-999) When **ChangeFrequencyType** is **xdays**, password changes take place this configured number of days.
    - **ChangeTime:** (24hr format: 00:00-23:59) UTC time of day scheduled password changes take place.
- **ParentAccountID:** If this is a subscribed account (**IsSubscribedAccount**), this is the ID of the parent managed account.
- **IsSubscribedAccount:** True if the account is a synced or subscribed account, otherwise false.
- **LastChangeDate:** The date and time of the last password change.
- **NextChangeDate:** The date and time of the next scheduled password change.
- **IsChanging:** True if the account credentials are in the process of changing, otherwise false.
- **ChangeState:** The change state of the account credentials:
    - **0:** Idle / no change taking place or scheduled within 5 minutes.
    - **1:** Changing / managed account credential currently changing.
    - **2:** Queued / managed account credential is queued to change or scheduled to change within 5 minutes.
- **UseOwnCredentials:** True if the current account credentials should be used during change operations, otherwise false.
- **ChangeIISAppPoolFlag:** True if IIS application pools run as this user should be updated with the new password after a password change, otherwise false.
- **RestartIISAppPoolFlag:** True if IIS application pools should be restarted after the run as password is changed, otherwise false.
- **WorkgroupID:** ID of the assigned Workgroup.

For more information, please see Configure Subscriber Accounts at https://www.beyondtrust.com/docs/beyondinsight-password-safe/ps/admin/managed-accounts.htm#ConfigureAccounts.

Response Codes

200 – Request successful. Managed Accounts in the response body.

For more information, please see "Common Response Codes" on page 17.

POST QuickRules/{quickRuleID}/ManagedAccounts/{accountID}

Purpose

Adds the managed account referenced by ID to the Quick Rule by adding it to the first **Managed Account Fields - Quick Group ID** filter found.

Required Permissions

- Password Safe Account Management (Read).
- Read/Write access to the Quick Rule.

URL Parameters

- **quickRuleID:** ID of the Quick Rule.
- **accountID:** ID of the managed account.

Request Body

None.

Response Body

Content-Type: application/json

```
[
    {
        ManagedAccountID : int,
        ManagedSystemID : int,
        DomainName : string,
        AccountName : string,
        DistinguishedName : string,
        PasswordFallbackFlag : bool,
        LoginAccountFlag : bool,
        Description : string,
        PasswordRuleID : int,
        ApiEnabled : bool,
        ReleaseNotificationEmail : string,
        ChangeServicesFlag : bool,
        RestartServicesFlag : bool,
        ChangeTasksFlag : bool,
        ReleaseDuration : int,
        MaxReleaseDuration : int,
        ISAReleaseDuration : int,
        MaxConcurrentRequests : int,

        AutoManagementFlag : bool,
```

```
        DSSAutoManagementFlag : bool,
        CheckPasswordFlag : bool,
        ResetPasswordOnMismatchFlag : bool,
        ChangePasswordAfterAnyReleaseFlag : bool,
        ChangeFrequencyType : string,
        ChangeFrequencyDays : int,
        ChangeTime : string,

        ParentAccountID : int, // can be null
        IsSubscribedAccount : bool,
        LastChangeDate : datetime, // can be null
        NextChangeDate : datetime, // can be null
        IsChanging : bool,
        ChangeState : int,
        UseOwnCredentials : bool,
        ChangeIISAppPoolFlag : bool,
        RestartIISAppPoolFlag : bool,
        WorkgroupID : int, // can be null
        ChangeWindowsAutoLogonFlag : bool,
        ChangeComPlusFlag : bool,
        ChangeDComFlag : bool,
        ChangeSComFlag : bool,
    },
    …
]
```

Response Body Details

- **DomainName:** The domain name for a domain-type account.
- **AccountName:** The name of the account.
- **DistinguishedName:** The distinguished name of an LDAP managed account.
- **PasswordFallbackFlag:** True if failed DSS authentication can fall back to password authentication, otherwise false.
- **LoginAccountFlag:** True if the account should use the managed system login account for SSH sessions, otherwise false.
- **Description:** A description of the account.
- **PasswordRuleID:** ID of the password rule assigned to this managed account.
- **ApiEnabled:** True if the account can be requested through the API, otherwise false.
- **ReleaseNotificationEmail:** Email address used for notification emails related to this managed account.
- **ChangeServicesFlag:** True if services run as this user should be updated with the new password after a password change, otherwise false.
- **RestartServicesFlag:** True if services should be restarted after the run as password is changed (**ChangeServicesFlag**), otherwise false.
- **ChangeTasksFlag:** True if scheduled tasks run as this user should be updated with the new password after a password change, otherwise false.
- **ReleaseDuration:** (minutes: 1-525600) Default release duration.
- **MaxReleaseDuration:** (minutes: 1-525600) Default maximum release duration.
- **ISAReleaseDuration:** (minutes: 1-525600) Default Information Systems Administrator (ISA) release duration.
- **MaxConcurrentRequests:** (0-999, 0 means unlimited) Maximum number of concurrent password requests for this account.

- **AutoManagementFlag:** True if password auto-management is enabled, otherwise false.
  - **DSSAutoManagementFlag:** True if DSS key auto-management is enabled, otherwise false.
  - **CheckPasswordFlag:** True to enable password testing, otherwise false.
  - **ChangePasswordAfterAnyReleaseFlag:** True to change passwords on release of a request, otherwise false.
  - **ResetPasswordOnMismatchFlag:** True to queue a password change when scheduled password test fails, otherwise false.
  - **ChangeFrequencyType:** The change frequency for scheduled password changes:
    - **first:** Changes scheduled for the first day of the month.
    - **last:** Changes scheduled for the last day of the month.
    - **xdays:** Changes scheduled every x days (**ChangeFrequencyDays**).
  - **ChangeFrequencyDays:** (days: 1-999) When **ChangeFrequencyType** is **xdays**, password changes take place this configured number of days.
  - **ChangeTime:** (24hr format: 00:00-23:59) UTC time of day scheduled password changes take place.
- **ParentAccountID:** If this is a subscribed account (**IsSubscribedAccount**), this is the ID of the parent managed account.
- **IsSubscribedAccount:** True if the account is a synced or subscribed account, otherwise false.
- **LastChangeDate:** The date and time of the last password change.
- **NextChangeDate:** The date and time of the next scheduled password change.
- **IsChanging:** True if the account credentials are in the process of changing, otherwise false.
- **ChangeState:** The change state of the account credentials:
  - **0:** Idle / no change taking place or scheduled within 5 minutes.
  - **1:** Changing / managed account credential currently changing.
  - **2:** Queued / managed account credential is queued to change or scheduled to change within 5 minutes.

For more information, please see Configure Subscriber Accounts at https://www.beyondtrust.com/docs/beyondinsight-password-safe/ps/admin/managed-accounts.htm#ConfigureAccounts.

Response Codes

200 – Request successful. Managed Accounts in the response body.

For more information, please see "Common Response Codes" on page 17.

DELETE QuickRules/{quickRuleID}/ManagedAccounts/{accountID}

Purpose

Removes the managed account referenced by ID from the Quick Rule by removing it from all **Managed Account Fields - Quick Group ID** filters found.

IMPORTANT!

A rule cannot be left in an invalid state. If removing the account would result in an empty filter, the filter itself will be removed. If there are no filters left in the rule, a "400 Bad Request" is returned.

- *If you intend to replace all accounts in the rule, see "PUT QuickRules/{quickRuleID}/ManagedAccounts" on page 270.*
- *If you intend to delete the rule, see "DELETE QuickRules/{id}" on page 369.*

Required Permissions

- Read/Write access to the Quick Rule.

URL Parameters

- **quickRuleID:** ID of the Quick Rule.
- **accountID:** ID of the managed account.

Request Body

None.

Response Codes

200 – Request successful.

For more information, please see "Common Response Codes" on page 17.

Smart Rule Managed Accounts

GET SmartRules/{smartRuleID}/ManagedAccounts

Purpose

Returns a list of managed accounts by Smart Rule ID.

Required Permissions

Read access to the Smart Rule.

URL Parameters

smartRuleID: ID of the Smart Rule.

Request Body

None.

Response Body

Content-Type: application/json

```
[
    {
        ManagedAccountID : int,
        ManagedSystemID : int,
        DomainName : string,
        AccountName : string,
        DistinguishedName : string,
        PasswordFallbackFlag : bool,
        LoginAccountFlag : bool,
        Description : string,
        PasswordRuleID : int,
        ApiEnabled : bool,
        ReleaseNotificationEmail : string,
        ChangeServicesFlag : bool,
        RestartServicesFlag : bool,
        ChangeTasksFlag : bool,
        ReleaseDuration : int,
        MaxReleaseDuration : int,
        ISAReleaseDuration : int,
        MaxConcurrentRequests : int,

        AutoManagementFlag : bool,
        DSSAutoManagementFlag : bool,
```

```
        CheckPasswordFlag : bool,
        ResetPasswordOnMismatchFlag : bool,
        ChangePasswordAfterAnyReleaseFlag : bool,
        ChangeFrequencyType : string,
        ChangeFrequencyDays : int,
        ChangeTime : string,

        ParentAccountID : int, // can be null
        IsSubscribedAccount : bool,
        LastChangeDat e: datetime, // can be null
        NextChangeDate : datetime, // can be null
        IsChanging : bool,
        ChangeState : int,
        UseOwnCredentials : bool,
        ChangeIISAppPoolFlag : bool,
        RestartIISAppPoolFlag : bool,
        WorkgroupID : int // can be null

    },
    …
]
```

Response Body Details

- **DomainName:** The domain name for a domain-type account.
- **AccountName:** The name of the account.
- **DistinguishedName:** The distinguished name of an LDAP managed account.
- **PasswordFallbackFlag:** True if failed DSS authentication can fall back to password authentication, otherwise false.
- **LoginAccountFlag:** True if the account should use the managed system login account for SSH sessions, otherwise false.
- **Description:** A description of the account.
- **PasswordRuleID:** ID of the password rule assigned to this managed account.
- **ApiEnabled:** True if the account can be requested through the API, otherwise false.
- **ReleaseNotificationEmail:** Email address used for notification emails related to this managed account.
- **ChangeServicesFlag:** True if services run as this user should be updated with the new password after a password change, otherwise false.
- **RestartServicesFlag:** True if services should be restarted after the run as password is changed (**ChangeServicesFlag**), otherwise false.
- **ChangeTasksFlag:** True if scheduled tasks run as this user should be updated with the new password after a password change, otherwise false.
- **ReleaseDuration:** (minutes: 1-525600) Default release duration.
- **MaxReleaseDuration:** (minutes: 1-525600) Default maximum release duration.
- **ISAReleaseDuration:** (minutes: 1-525600) Default Information Systems Administrator (ISA) release duration.
- **MaxConcurrentRequests:** (0-999, 0 means unlimited) Maximum number of concurrent password requests for this account.
- **AutoManagementFlag:** True if password auto-management is enabled, otherwise false.
    - **DSSAutoManagementFlag:** True if DSS key auto-management is enabled, otherwise false.
    - **CheckPasswordFlag:** True to enable password testing, otherwise false.

  - **ChangePasswordAfterAnyReleaseFlag:** True to change passwords on release of a request, otherwise false.
  - **ResetPasswordOnMismatchFlag:** True to queue a password change when scheduled password test fails, otherwise false.
  - **ChangeFrequencyType:** The change frequency for scheduled password changes:
    - **first:** Changes scheduled for the first day of the month.
    - **last:** Changes scheduled for the last day of the month.
    - **xdays:** Changes scheduled every x days (**ChangeFrequencyDays**).
  - **ChangeFrequencyDays:** (days: 1-999) When **ChangeFrequencyType** is **xdays**, password changes take place this configured number of days.
  - **ChangeTime:** (24hr format: 00:00-23:59) UTC time of day scheduled password changes take place.
- **ParentAccountID:** If this is a subscribed account (**IsSubscribedAccount**), this is the ID of the parent managed account.
- **IsSubscribedAccount:** True if the account is a synced or subscribed account, otherwise false.
- **LastChangeDate:** The date and time of the last password change.
- **NextChangeDate:** The date and time of the next scheduled password change.
- **IsChanging:** True if the account credentials are in the process of changing, otherwise false.
- **ChangeState:** The change state of the account credentials:
  - **0:** Idle / No change taking place or scheduled within 5 minutes.
  - **1:** Changing / Managed Account Credential currently changing.
  - **2:** Queued / Managed Account Credential is queued to change or scheduled to change within 5 minutes.
- **WorkgroupID:** ID of the assigned Workgroup.

> *For more information, please see Configure Subscriber Accounts at https://www.beyondtrust.com/docs/beyondinsight-password-safe/ps/admin/managed-accounts.htm#ConfigureAccounts.*

Response Codes

200 - Request successful. Managed Accounts in the response body.

> *For more information, please see "Common Response Codes" on page 17.*

Managed Account Applications

Quick Navigation

GET ManagedAccounts/{accountID}/Applications

Purpose

Returns a list of applications assigned to a managed account.

Required Permissions

Password Safe Account Management (Read).

URL Parameters

accountID: ID of the managed account.

Request Body

None.

Response Body

Content-Type: application/json

```
[
    {
        ApplicationID : int,
        Name : string,
        DisplayName : string,
        Version : string,
        Command : string,
        Parameters : string,
        Publisher : string,
        ApplicationType : string,
        FunctionalAccountID : int, // can be null
        ManagedSystemID : int, // can be null
        IsActive : bool,
```

```
      SmartRuleID : int // can be null
    }
    …
]
```

Response Codes

200 - Request successful. Applications in response body.

For more information, please see "Common Response Codes" on page 17.

POST ManagedAccounts/{accountID}/Applications/{applicationID}

Purpose

Assigns an application to a managed account.

Required Permissions

Password Safe Account Management (Read/Write).

URL Parameters

- **accountID:** ID of the managed account.
- **applicationID:** ID of the application.

Request Body

None.

Response Body

Content-Type: application/json

```
{
    ApplicationID : int,
    Name : string,
    DisplayName : string,
    Version : string,
    Command : string,
    Parameters : string,
    Publisher : string,
    ApplicationType : string,
```

```
    FunctionalAccountID : int, // can be null
    ManagedSystemID : int, // can be null
    IsActive : bool,
    SmartRuleID : int // can be null
}
```

Response Codes

201 - Request successful. Application in response body.

For more information, please see "Common Response Codes" on page 17.

DELETE ManagedAccounts/{accountID}/Applications/{applicationID}

Purpose

Unassigns an application from a managed account by managed account ID and application ID.

Required Permissions

Password Safe Account Management (Read/Write).

URL Parameters

- **accountID:** ID of the managed account.
- **applicationID:** ID of the application.

Request Body

None.

Response Body

None.

Response Codes

200 - Request successful.

> *For more information, please see "Common Response Codes" on page 17.*

DELETE ManagedAccounts/{accountID}/Applications

Purpose

Unassigns all managed account applications by managed account ID.

Required Permissions

Password Safe Account Management (Read/Write).

URL Parameters

- **accountID:** ID of the managed account.
- **applicationID:** ID of the application.

Request Body

None.

Response Body

None.

Response Codes

200 - Request successful.

> *For more information, please see "Common Response Codes" on page 17.*

Managed Systems

Quick Navigation

For more information on related topics, please see:

- *"Assets" on page 54*
- *"Managed Accounts" on page 225*
- *"Password Policies" on page 347*
- *"DSS Key Policies" on page 200*
- *"Platforms" on page 352*

GET ManagedSystems/{id}

Purpose

Returns a managed system by ID.

Required Permissions

Password Safe System Management (Read).

URL Parameters

id: ID of the managed system.

Request Body

None.

Response Body

Content-Type: application/json

```
[
    {
        WorkgroupID : int

        HostName : string

        IPAddress : string
        DNSName : string
        InstanceName : string
        IsDefaultInstance : bool // can be null
        Template : string
        ForestName : string
        UseSSL : bool // can be null

        ManagedSystemID : int,
        EntityTypeID : int,
        AssetID : int, // can be null
        DatabaseID : int, // can be null
        DirectoryID : int, // can be null
        CloudID : int, // can be null
        SystemName : string,
        Timeout : short,
        PlatformID: int,
        NetBiosName : string,
        ContactEmail : string,
        Description : string,
```

```
        Port : int, // can be null
        Timeout : short,
        SshKeyEnforcementMode : int, // can be null
        PasswordRuleID : int,
        DSSKeyRuleID : int, // can be null
        LoginAccountID : int, // can be null
        AccountNameFormat : int,
        OracleInternetDirectoryID : guid, // can be null
        OracleInternetDirectoryServiceName : string,
        ReleaseDuration : int,
        MaxReleaseDuration : int,
        ISAReleaseDuration : int,

        AutoManagementFlag : bool,
        FunctionalAccountID : int, // can be null
        ElevationCommand : string, // can be null
        CheckPasswordFlag : bool,
        ChangePasswordAfterAnyReleaseFlag : bool,
        ResetPasswordOnMismatchFlag : bool,
        ChangeFrequencyType : string,
        ChangeFrequencyDays : int,
        ChangeTime : string,
        RemoteClientType : string,
        ApplicationHostID : int, // can be null
        IsApplicationHost : bool,
        AccessURL : string
    },
    …
]
```

Response Body Details

- **ManagedSystemID:** ID of the managed system.
- **AssetD:** Asset ID; set if the managed system is an asset or a database.
- **DatabaseID:** Database ID; set if the managed system is a database.
- **DirectoryID:** Directory ID; set if the managed system is a directory.
- **CloudID:** Cloud system ID; set if the managed system is a cloud system.
- **SystemName:** Name of the related entity (asset, directory, database, or cloud).
- **PlatformID:** ID of the managed system platform.
- **NetBiosName:** (Managed domains only) Domain NetBIOS name. Setting this value will allow Password Safe to fall back to the NetBIOS name if needed.
- **Port:** The port used to connect to the host. If null and the related **Platform.PortFlag** is true, Password Safe uses **Platform.DefaultPort** for communication.
- **Timeout:** (seconds) Connection timeout. Length of time in seconds before a slow or unresponsive connection to the system fails.
- **SshKeyEnforcementMode:** Enforcement mode for SSH host keys.
    - **0:** None.
    - **1:** Auto. Auto accept initial key.
    - **2:** Strict. Manually accept keys.

- **PasswordRuleID:** ID of the default password rule assigned to managed accounts created under this managed system.
- **DSSKeyRuleID:** ID of the default DSS key rule assigned to managed accounts created under this managed system.
- **LoginAccountID:** ID of the functional account used for SSH session logins.
- **ReleaseDuration:** (minutes: 1-525600) Default release duration.
- **MaxReleaseDuration:** (minutes: 1-525600) Default maximum release duration.
- **ISAReleaseDuration:** (minutes: 1-525600) Default Information Systems Administrator (ISA) release duration.
- **AutoManagementFlag:** True if password auto-management is enabled, otherwise false.
    - **FunctionalAccountID:** ID of the functional account used for local managed account password changes.
    - **ElevationCommand:** Elevation command to use (**sudo**, **pbrun**, **pmrun**).
    - **CheckPasswordFlag:** True to enable password testing, otherwise false.
    - **ChangePasswordAfterAnyReleaseFlag:** True to change passwords on release of a request, otherwise false.
    - **ResetPasswordOnMismatchFlag:** True to queue a password change when scheduled password test fails, otherwise false.
    - **ChangeFrequencyType:** The change frequency for scheduled password changes:
        - **first:** Changes scheduled for the first day of the month.
        - **last:** Changes scheduled for the last day of the month.
        - **xdays:** Changes scheduled every x days (see **ChangeFrequencyDays**).
    - **ChangeFrequencyDays:** (days: 1-90) When **ChangeFrequencyType** is **xdays**, password changes take place this configured number of days.
    - **ChangeTime:** (24hr format: 00:00-23:59) UTC time of day scheduled password changes take place.
- **RemoteClientType:** The type of remote client to use.
    - **None:** No remote client.
    - **EPM:** Endpoint Privilege Management.
- **ApplicationHostID:** Managed system ID of the target application host. Must be an ID of a managed system whose IsApplicationHost = true.
- **IsApplicationHost:** True if the managed system can be used as an application host, otherwise false. Can be set when the Platform.ApplicationHostFlag = true, and cannot be set when ApplicationHostID has a value.
- **AccessURL:** The URL used for cloud access (applies to cloud systems only).

Response Codes

200 - Request successful. Managed System in response body.

For more information, please see "Common Response Codes" on page 17.

GET ManagedSystems

Purpose

Returns a list of managed systems.

Required Permissions

Password Safe System Management (Read).

Query Parameters (Optional)

- **type:** The entity type of the managed system.
- **name:** The name of the managed system.
- **limit:** (default: 100000) Number of records to return.
- **offset:** (default: 0) Number of records to skip before returning records (can only be used in conjunction with **limit**).

Request Body

None.

Response Body (when limit is not given)

Content-Type: application/json

```
[
    {
        WorkgroupID : int

        HostName : string

        IPAddress : string
        DNSName : string
        InstanceName : string
        IsDefaultInstance : bool // can be null
        Template : string
        ForestName : string
        UseSSL : bool // can be null

        ManagedSystemID : int,
        EntityTypeID : int,
        AssetID : int, // can be null
        DatabaseID : int, // can be null
        DirectoryID : int, // can be null
        CloudID : int, // can be null
        SystemName : string,
        Timeout : short,
```

```
        PlatformID: int,
        NetBiosName : string,
        ContactEmail : string,
        Description : string,
        Port : int, // can be null
        Timeout : short,
        SshKeyEnforcementMode : int, // can be null
        PasswordRuleID : int,
        DSSKeyRuleID : int, // can be null
        LoginAccountID : int, // can be null
        AccountNameFormat : int,
        OracleInternetDirectoryID : guid, // can be null
        OracleInternetDirectoryServiceName : string,
        ReleaseDuration : int,
        MaxReleaseDuration : int,
        ISAReleaseDuration : int,

        AutoManagementFlag : bool,
        FunctionalAccountID : int, // can be null
        ElevationCommand : string, // can be null
        CheckPasswordFlag : bool,
        ChangePasswordAfterAnyReleaseFlag : bool,
        ResetPasswordOnMismatchFlag : bool,
        ChangeFrequencyType : string,
        ChangeFrequencyDays : int,
        ChangeTime : string,
        RemoteClientType : string,
        ApplicationHostID : int, // can be null
        IsApplicationHost : bool,
        AccessURL : string
    },
    …
]
```

Response Body (when limit is given)

Content-Type: application/json

```
[
    {
        TotalCount : int,
        Data : [{
        WorkgroupID : int

        HostName : string

        IPAddress : string
        DNSName : string
        InstanceName : string
        IsDefaultInstance : bool // can be null
        Template : string
        ForestName : string
        UseSSL : bool // can be null
```

```
        ManagedSystemID : int,
        EntityTypeID : int,
        AssetID : int, // can be null
        DatabaseID : int, // can be null
        DirectoryID : int, // can be null
        CloudID : int, // can be null
        SystemName : string,
        Timeout : short,
        PlatformID: int,
        NetBiosName : string,
        ContactEmail : string,
        Description : string,
        Port : int, // can be null
        Timeout : short,
        SshKeyEnforcementMode : int, // can be null
        PasswordRuleID : int,
        DSSKeyRuleID : int, // can be null
        LoginAccountID : int, // can be null
        AccountNameFormat : int,
        OracleInternetDirectoryID : guid, // can be null
        OracleInternetDirectoryServiceName : string,
        ReleaseDuration : int,
        MaxReleaseDuration : int,
        ISAReleaseDuration : int,

        AutoManagementFlag : bool,
        FunctionalAccountID : int, // can be null
        ElevationCommand : string, // can be null
        CheckPasswordFlag : bool,
        ChangePasswordAfterAnyReleaseFlag : bool,
        ResetPasswordOnMismatchFlag : bool,
        ChangeFrequencyType : string,
        ChangeFrequencyDays : int,
        ChangeTime : string,
        RemoteClientType : string,
        ApplicationHostID : int, // can be null
        IsApplicationHost : bool,
        AccessURL : string
        },
    …]
}
```

Response Body Details

- **ManagedSystemID:** ID of the managed system.
- **AssetD:** Asset ID; set if the managed system is an asset or a database.
- **DatabaseID:** Database ID; set if the managed system is a database.
- **DirectoryID:** Directory ID; set if the managed system is a directory.
- **CloudID:** Cloud system ID; set if the managed system is a cloud system.
- **SystemName:** Name of the related entity (asset, directory, database, or cloud).
- **PlatformID:** ID of the managed system platform.

- **NetBiosName:** (Managed domains only) Domain NetBIOS name. Setting this value will allow Password Safe to fall back to the NetBIOS name if needed.
- **Port:** The port used to connect to the host. If null and the related **Platform.PortFlag** is true, Password Safe uses **Platform.DefaultPort** for communication.
- **Timeout:** (seconds) Connection timeout. Length of time in seconds before a slow or unresponsive connection to the system fails.
- **SshKeyEnforcementMode:** Enforcement mode for SSH host keys.
    - **0:** None.
    - **1:** Auto. Auto accept initial key.
    - **2:** Strict. Manually accept keys.
- **PasswordRuleID:** ID of the default password rule assigned to managed accounts created under this managed system.
- **DSSKeyRuleID:** ID of the default DSS key rule assigned to managed accounts created under this managed system.
- **LoginAccountID:** ID of the functional account used for SSH session logins.
- **ReleaseDuration:** (minutes: 1-525600) Default release duration.
- **MaxReleaseDuration:** (minutes: 1-525600) Default maximum release duration.
- **ISAReleaseDuration:** (minutes: 1-525600) Default Information Systems Administrator (ISA) release duration.
- **AutoManagementFlag:** True if password auto-management is enabled, otherwise false.
    - **FunctionalAccountID:** ID of the functional account used for local managed account password changes.
    - **ElevationCommand:** Elevation command to use (**sudo**, **pbrun**, **pmrun**).
    - **CheckPasswordFlag:** True to enable password testing, otherwise false.
    - **ChangePasswordAfterAnyReleaseFlag:** True to change passwords on release of a request, otherwise false.
    - **ResetPasswordOnMismatchFlag:** True to queue a password change when scheduled password test fails, otherwise false.
    - **ChangeFrequencyType:** The change frequency for scheduled password changes:
        - **first:** Changes scheduled for the first day of the month.
        - **last:** Changes scheduled for the last day of the month.
        - **xdays:** Changes scheduled every x days (see **ChangeFrequencyDays**).
    - **ChangeFrequencyDays:** (days: 1-90) When **ChangeFrequencyType** is **xdays**, password changes take place this configured number of days.
    - **ChangeTime:** (24hr format: 00:00-23:59) UTC time of day scheduled password changes take place.
- **RemoteClientType:** The type of remote client to use.
    - **None:** No remote client.
    - **EPM:** Endpoint Privilege Management.
- **ApplicationHostID:** Managed system ID of the target application host. Must be an ID of a managed system whose IsApplicationHost = true.
- **IsApplicationHost:** True if the managed system can be used as an application host, otherwise false. Can be set when the Platform.ApplicationHostFlag = true, and cannot be set when ApplicationHostID has a value.
- **AccessURL:** The URL used for cloud access (applies to cloud systems only).

Response Codes

200 - Request successful. Managed system in response body.

For more information, please see "Common Response Codes" on page 17.

GET Assets/{assetId}/ManagedSystems

Purpose

Returns a managed system for the asset referenced by ID.

Required Permissions

Password Safe System Management (Read).

URL Parameters

assetId: ID of the asset.

Request Body

None.

Response Body

Content-Type: application/json

```
[
    {
        WorkgroupID : int

        HostName : string

        IPAddress : string
        DNSName : string
        InstanceName : string
        IsDefaultInstance : bool // can be null
        Template : string
        ForestName : string
        UseSSL : bool // can be null

        ManagedSystemID : int,
        EntityTypeID : int,
        AssetID : int, // can be null
        DatabaseID : int, // can be null
        DirectoryID : int, // can be null
        CloudID : int, // can be null
        SystemName : string,
        Timeout : short,
        PlatformID: int,
        NetBiosName : string,
        ContactEmail : string,
        Description : string,
```

```
        Port : int, // can be null
        Timeout : short,
        SshKeyEnforcementMode : int, // can be null
        PasswordRuleID : int,
        DSSKeyRuleID : int, // can be null
        LoginAccountID : int, // can be null
        AccountNameFormat : int,
        OracleInternetDirectoryID : guid, // can be null
        OracleInternetDirectoryServiceName : string,
        ReleaseDuration : int,
        MaxReleaseDuration : int,
        ISAReleaseDuration : int,

        AutoManagementFlag : bool,
        FunctionalAccountID : int, // can be null
        ElevationCommand : string, // can be null
        CheckPasswordFlag : bool,
        ChangePasswordAfterAnyReleaseFlag : bool,
        ResetPasswordOnMismatchFlag : bool,
        ChangeFrequencyType : string,
        ChangeFrequencyDays : int,
        ChangeTime : string,
        RemoteClientType : string,
        ApplicationHostID : int, // can be null
        IsApplicationHost : bool,
        AccessURL : string
    },
    …
]
```

Response Body Details

- **ManagedSystemID:** ID of the managed system.
- **AssetD:** Asset ID; set if the managed system is an asset or a database.
- **DatabaseID:** Database ID; set if the managed system is a database.
- **DirectoryID:** Directory ID; set if the managed system is a directory.
- **CloudID:** Cloud system ID; set if the managed system is a cloud system.
- **SystemName:** Name of the related entity (asset, directory, database, or cloud).
- **PlatformID:** ID of the managed system platform.
- **NetBiosName:** (Managed domains only) Domain NetBIOS name. Setting this value will allow Password Safe to fall back to the NetBIOS name if needed.
- **Port:** The port used to connect to the host. If null and the related **Platform.PortFlag** is true, Password Safe uses **Platform.DefaultPort** for communication.
- **Timeout:** (seconds) Connection timeout. Length of time in seconds before a slow or unresponsive connection to the system fails.
- **SshKeyEnforcementMode:** Enforcement mode for SSH host keys.
    - **0:** None.
    - **1:** Auto. Auto accept initial key.
    - **2:** Strict. Manually accept keys.

- **PasswordRuleID:** ID of the default password rule assigned to managed accounts created under this managed system.
- **DSSKeyRuleID:** ID of the default DSS key rule assigned to managed accounts created under this managed system.
- **LoginAccountID:** ID of the functional account used for SSH session logins.
- **ReleaseDuration:** (minutes: 1-525600) Default release duration.
- **MaxReleaseDuration:** (minutes: 1-525600) Default maximum release duration.
- **ISAReleaseDuration:** (minutes: 1-525600) Default Information Systems Administrator (ISA) release duration.
- **AutoManagementFlag:** True if password auto-management is enabled, otherwise false.
    - **FunctionalAccountID:** ID of the functional account used for local managed account password changes.
    - **ElevationCommand:** Elevation command to use (**sudo**, **pbrun**, **pmrun**).
    - **CheckPasswordFlag:** True to enable password testing, otherwise false.
    - **ChangePasswordAfterAnyReleaseFlag:** True to change passwords on release of a request, otherwise false.
    - **ResetPasswordOnMismatchFlag:** True to queue a password change when scheduled password test fails, otherwise false.
    - **ChangeFrequencyType:** The change frequency for scheduled password changes:
        - **first:** Changes scheduled for the first day of the month.
        - **last:** Changes scheduled for the last day of the month.
        - **xdays:** Changes scheduled every x days (see **ChangeFrequencyDays**).
    - **ChangeFrequencyDays:** (days: 1-90) When **ChangeFrequencyType** is **xdays**, password changes take place this configured number of days.
    - **ChangeTime:** (24hr format: 00:00-23:59) UTC time of day scheduled password changes take place.
- **RemoteClientType:** The type of remote client to use.
    - **None:** No remote client.
    - **EPM:** Endpoint Privilege Management.
- **ApplicationHostID:** Managed system ID of the target application host. Must be an ID of a managed system whose IsApplicationHost = true.
- **IsApplicationHost:** True if the managed system can be used as an application host, otherwise false. Can be set when the Platform.ApplicationHostFlag = true, and cannot be set when ApplicationHostID has a value.
- **AccessURL:** The URL used for cloud access (applies to cloud systems only).

Response Codes

200 - Request successful. Managed System in response body.

For more information, please see "Common Response Codes" on page 17.

GET Databases/{databaseID}/ManagedSystems

Purpose

Returns a managed system for the database referenced by ID.

Required Permissions

Password Safe System Management (Read).

URL Parameters

databaseID: ID of the database.

Request Body

None.

Response Body

Content-Type: application/json

```
[
    {
        WorkgroupID : int

        HostName : string

        IPAddress : string
        DNSName : string
        InstanceName : string
        IsDefaultInstance : bool // can be null
        Template : string
        ForestName : string
        UseSSL : bool // can be null

        ManagedSystemID : int,
        EntityTypeID : int,
        AssetID : int, // can be null
        DatabaseID : int, // can be null
        DirectoryID : int, // can be null
        CloudID : int, // can be null
        SystemName : string,
        Timeout : short,
        PlatformID: int,
        NetBiosName : string,
        ContactEmail : string,
        Description : string,
```

```
        Port : int, // can be null
        Timeout : short,
        SshKeyEnforcementMode : int, // can be null
        PasswordRuleID : int,
        DSSKeyRuleID : int, // can be null
        LoginAccountID : int, // can be null
        AccountNameFormat : int,
        OracleInternetDirectoryID : guid, // can be null
        OracleInternetDirectoryServiceName : string,
        ReleaseDuration : int,
        MaxReleaseDuration : int,
        ISAReleaseDuration : int,

        AutoManagementFlag : bool,
        FunctionalAccountID : int, // can be null
        ElevationCommand : string, // can be null
        CheckPasswordFlag : bool,
        ChangePasswordAfterAnyReleaseFlag : bool,
        ResetPasswordOnMismatchFlag : bool,
        ChangeFrequencyType : string,
        ChangeFrequencyDays : int,
        ChangeTime : string,
        RemoteClientType : string,
        AccessURL : string
    },
    …
]
```

Response Body Details

- **ManagedSystemID:** ID of the managed system.
- **AssetD:** Asset ID; set if the managed system is an asset or a database.
- **DatabaseID:** Database ID; set if the managed system is a database.
- **DirectoryID:** Directory ID; set if the managed system is a directory.
- **CloudID:** Cloud system ID; set if the managed system is a cloud system.
- **SystemName:** Name of the related entity (asset, directory, database, or cloud).
- **PlatformID:** ID of the managed system platform.
- **NetBiosName:** (Managed domains only) Domain NetBIOS name. Setting this value will allow Password Safe to fall back to the NetBIOS name if needed.
- **Port:** The port used to connect to the host. If null and the related **Platform.PortFlag** is true, Password Safe uses **Platform.DefaultPort** for communication.
- **Timeout:** (seconds) Connection timeout. Length of time in seconds before a slow or unresponsive connection to the system fails.
- **SshKeyEnforcementMode:** Enforcement mode for SSH host keys.
    - **0:** None.
    - **1:** Auto. Auto accept initial key.
    - **2:** Strict. Manually accept keys.
- **PasswordRuleID:** ID of the default password rule assigned to managed accounts created under this managed system.
- **DSSKeyRuleID:** ID of the default DSS key rule assigned to managed accounts created under this managed system.

- **LoginAccountID:** ID of the functional account used for SSH session logins.
- **ReleaseDuration:** (minutes: 1-525600) Default release duration.
- **MaxReleaseDuration:** (minutes: 1-525600) Default maximum release duration.
- **ISAReleaseDuration:** (minutes: 1-525600) Default Information Systems Administrator (ISA) release duration.
- **AutoManagementFlag:** True if password auto-management is enabled, otherwise false.
    - **FunctionalAccountID:** ID of the functional account used for local managed account password changes.
    - **ElevationCommand:** Elevation command to use (**sudo**, **pbrun**, **pmrun**).
    - **CheckPasswordFlag:** True to enable password testing, otherwise false.
    - **ChangePasswordAfterAnyReleaseFlag:** True to change passwords on release of a request, otherwise false.
    - **ResetPasswordOnMismatchFlag:** True to queue a password change when scheduled password test fails, otherwise false.
    - **ChangeFrequencyType:** The change frequency for scheduled password changes:
        - **first:** Changes scheduled for the first day of the month.
        - **last:** Changes scheduled for the last day of the month.
        - **xdays:** Changes scheduled every x days (see **ChangeFrequencyDays**).
    - **ChangeFrequencyDays:** (days: 1-90) When **ChangeFrequencyType** is **xdays**, password changes take place this configured number of days.
    - **ChangeTime:** (24hr format: 00:00-23:59) UTC time of day scheduled password changes take place.
- **RemoteClientType:** The type of remote client to use.
    - **None:** No remote client.
    - **EPM:** Endpoint Privilege Management.
- **AccessURL:** The URL used for cloud access (applies to cloud systems only).

Response Codes

200 - Request successful. Managed System in response body.

For more information, please see "Common Response Codes" on page 17.

GET FunctionalAccounts/{id}/ManagedSystems

Purpose

Returns a list of managed systems auto-managed by the functional account referenced by ID.

Required Permissions

Password Safe System Management (Read).

Password Safe Account Management (Read).

URL Parameters

id: ID of the functional account.

Query Parameters (Optional)

- **type:** The entity type of the managed system.
- **name:** The name of the managed system.
- **limit:** (default: 100000) Number of records to return.
- **offset:** (default: 0) Number of records to skip before returning records (can only be used in conjunction with limit).

Request Body

None.

Response Body (when limit is not given)

Content-Type: application/json

```
[
    {
        WorkgroupID : int

        HostName : string

        IPAddress : string
        DNSName : string
        InstanceName : string
        IsDefaultInstance : bool // can be null
        Template : string
        ForestName : string
        UseSSL : bool // can be null

        ManagedSystemID : int,
```

```
        EntityTypeID : int,
        AssetID : int, // can be null
        DatabaseID : int, // can be null
        DirectoryID : int, // can be null
        CloudID : int, // can be null
        SystemName : string,
        Timeout : short,
        PlatformID: int,
        NetBiosName : string,
        ContactEmail : string,
        Description : string,
        Port : int, // can be null
        Timeout : short,
        SshKeyEnforcementMode : int, // can be null
        PasswordRuleID : int,
        DSSKeyRuleID : int, // can be null
        LoginAccountID : int, // can be null
        AccountNameFormat : int,
        OracleInternetDirectoryID : guid, // can be null
        OracleInternetDirectoryServiceName : string,
        ReleaseDuration : int,
        MaxReleaseDuration : int,
        ISAReleaseDuration : int,

        AutoManagementFlag : bool,
        FunctionalAccountID : int, // can be null
        ElevationCommand : string, // can be null
        CheckPasswordFlag : bool,
        ChangePasswordAfterAnyReleaseFlag : bool,
        ResetPasswordOnMismatchFlag : bool,
        ChangeFrequencyType : string,
        ChangeFrequencyDays : int,
        ChangeTime : string,
        RemoteClientType : string,
        ApplicationHostID : int, // can be null
        IsApplicationHost : bool,
        AccessURL : string
    },
    …
]
```

Response Body (when limit is given)

Content-Type: application/json

```
[
    {
        TotalCount : int,
        Data : [{
        WorkgroupID : int

        HostName : string
```

```
        IPAddress : string
        DNSName : string
        InstanceName : string
        IsDefaultInstance : bool // can be null
        Template : string
        ForestName : string
        UseSSL : bool // can be null

        ManagedSystemID : int,
        EntityTypeID : int,
        AssetID : int, // can be null
        DatabaseID : int, // can be null
        DirectoryID : int, // can be null
        CloudID : int, // can be null
        SystemName : string,
        Timeout : short,
        PlatformID: int,
        NetBiosName : string,
        ContactEmail : string,
        Description : string,
        Port : int, // can be null
        Timeout : short,
        SshKeyEnforcementMode : int, // can be null
        PasswordRuleID : int,
        DSSKeyRuleID : int, // can be null
        LoginAccountID : int, // can be null
        AccountNameFormat : int,
        OracleInternetDirectoryID : guid, // can be null
        OracleInternetDirectoryServiceName : string,
        ReleaseDuration : int,
        MaxReleaseDuration : int,
        ISAReleaseDuration : int,

        AutoManagementFlag : bool,
        FunctionalAccountID : int, // can be null
        ElevationCommand : string, // can be null
        CheckPasswordFlag : bool,
        ChangePasswordAfterAnyReleaseFlag : bool,
        ResetPasswordOnMismatchFlag : bool,
        ChangeFrequencyType : string,
        ChangeFrequencyDays : int,
        ChangeTime : string,
        RemoteClientType : string,
        ApplicationHostID : int, // can be null
        IsApplicationHost : bool,
        AccessURL : string
    },
    …
]
```

Response Body Details

- **ManagedSystemID:** ID of the managed system.
- **AssetD:** Asset ID; set if the managed system is an asset or a database.

- **DatabaseID:** Database ID; set if the managed system is a database.
- **DirectoryID:** Directory ID; set if the managed system is a directory.
- **CloudID:** Cloud system ID; set if the managed system is a cloud system.
- **SystemName:** Name of the related entity (asset, directory, database, or cloud).
- **PlatformID:** ID of the managed system platform.
- **NetBiosName:** (Managed domains only) Domain NetBIOS name. Setting this value will allow Password Safe to fall back to the NetBIOS name if needed.
- **Port:** The port used to connect to the host. If null and the related **Platform.PortFlag** is true, Password Safe uses **Platform.DefaultPort** for communication.
- **Timeout:** (seconds) Connection timeout. Length of time in seconds before a slow or unresponsive connection to the system fails.
- **SshKeyEnforcementMode:** Enforcement mode for SSH host keys.
    - **0:** None.
    - **1:** Auto. Auto accept initial key.
    - **2:** Strict. Manually accept keys.
- **PasswordRuleID:** ID of the default password rule assigned to managed accounts created under this managed system.
- **DSSKeyRuleID:** ID of the default DSS key rule assigned to managed accounts created under this managed system.
- **LoginAccountID:** ID of the functional account used for SSH session logins.
- **ReleaseDuration:** (minutes: 1-525600) Default release duration.
- **MaxReleaseDuration:** (minutes: 1-525600) Default maximum release duration.
- **ISAReleaseDuration:** (minutes: 1-525600) Default Information Systems Administrator (ISA) release duration.
- **AutoManagementFlag:** True if password auto-management is enabled, otherwise false.
    - **FunctionalAccountID:** ID of the functional account used for local managed account password changes.
    - **ElevationCommand:** Elevation command to use (**sudo**, **pbrun**, **pmrun**).
    - **CheckPasswordFlag:** True to enable password testing, otherwise false.
    - **ChangePasswordAfterAnyReleaseFlag:** True to change passwords on release of a request, otherwise false.
    - **ResetPasswordOnMismatchFlag:** True to queue a password change when scheduled password test fails, otherwise false.
    - **ChangeFrequencyType:** The change frequency for scheduled password changes:
        - **first:** Changes scheduled for the first day of the month.
        - **last:** Changes scheduled for the last day of the month.
        - **xdays:** Changes scheduled every x days (see **ChangeFrequencyDays**).
    - **ChangeFrequencyDays:** (days: 1-90) When **ChangeFrequencyType** is **xdays**, password changes take place this configured number of days.
    - **ChangeTime:** (24hr format: 00:00-23:59) UTC time of day scheduled password changes take place.
- **RemoteClientType:** The type of remote client to use.
    - **None:** No remote client.
    - **EPM:** Endpoint Privilege Management.
- **ApplicationHostID:** Managed system ID of the target application host. Must be an ID of a managed system whose IsApplicationHost = true.
- **IsApplicationHost:** True if the managed system can be used as an application host, otherwise false. Can be set when the Platform.ApplicationHostFlag = true, and cannot be set when ApplicationHostID has a value.

- **AccessURL:** The URL used for cloud access (applies to cloud systems only).

Response Codes

200 - Request successful. Managed System in response body.

For more information, please see "Common Response Codes" on page 17.

GET Workgroups/{id}/ManagedSystems

Purpose

Returns a list of managed systems by Workgroup ID.

Required Permissions

Password Safe System Management (Read).

URL Parameters

id: ID of the Workgroup.

Query Parameters (Optional)

- **limit:** (default: 100000) Number of records to return.
- **offset:** (default: 0) Number of records to skip before returning <limit> records (can be used only in conjunction with limit).

Request Body

None.

Response Body (when limit is not given)

Content-Type: application/json

```
[
    {
        WorkgroupID : int,
        ManagedSystemID : int,
        EntityTypeID : int,
        AssetID : int, // can be null
        DatabaseID : int, // can be null
        DirectoryID : int, // can be null
        CloudID : int, // can be null

        HostName : string,
        IPAddress : string,
        DnsName : string,
        InstanceName : string,
        IsDefaultInstance : bool, // can be null
        Template : string,
        ForestName : string,
        UseSSL : bool, // can be null
        AccountNameFormat : int,
```

```
        OracleInternetDirectoryID : guid, // can be null
        OracleInternetDirectoryServiceName : string,

        SystemName : string,
        PlatformID : int,
        NetBiosName : string,
        ContactEmail : string,
        Description : string,
        Port : int, // can be null
        Timeout : short,
        SshKeyEnforcementMode : int, // can be null
        PasswordRuleID : int,
        DSSKeyRuleID : int, // can be null
        LoginAccountID : int, // can be null
        ReleaseDuration : int,
        MaxReleaseDuration : int,
        ISAReleaseDuration : int,
        AutoManagementFlag : bool,
        FunctionalAccountID : int, // can be null
        ElevationCommand : string, // can be null
        CheckPasswordFlag : bool,
        ChangePasswordAfterAnyReleaseFlag : bool,
        ResetPasswordOnMismatchFlag : bool,
        ChangeFrequencyType : string,
        ChangeFrequencyDays : int,
        ChangeTime : string,
        RemoteClientType : string,
        ApplicationHostID : int, // can be null
        IsApplicationHost : bool
        AccessURL : string
    },
…]
```

Response Body (when limit is given)

Content-Type: application/json

```
{
    TotalCount : int,
    Data :
    [{
        WorkgroupID : int,
        ManagedSystemID : int,
        EntityTypeID: int,
        AssetID : int, // can be null
        DatabaseID : int, // can be null
        DirectoryID : int, // can be null
        CloudID : int, // can be null

        HostName : string,
        IPAddress : string,
        DnsName : string,
        InstanceName : string,
```

```
        IsDefaultInstance : bool, // can be null
        Template : string,
        ForestName : string,
        UseSSL : bool, // can be null
        AccountNameFormat : int,
        OracleInternetDirectoryID : guid, // can be null
        OracleInternetDirectoryServiceName : string,

        SystemName : string,
        PlatformID : int,
        NetBiosName : string,
        ContactEmail : string,
        Description : string,
        Port : int, // can be null
        Timeout : short,
        PasswordRuleID : int,
        DSSKeyRuleID : int, // can be null
        LoginAccountID : int, // can be null
        ReleaseDuration : int,
        MaxReleaseDuration : int,
        ISAReleaseDuration : int,
        AutoManagementFlag : bool,
        FunctionalAccountID : int, // can be null
        ElevationCommand : string, // can be null
        CheckPasswordFlag : bool,
        ChangePasswordAfterAnyReleaseFlag : bool,
        ResetPasswordOnMismatchFlag : bool,
        ChangeFrequencyType : string,
        ChangeFrequencyDays : int,
        ChangeTime : string,
        RemoteClientType : string,
        ApplicationHostID : int, // can be null
        IsApplicationHost : bool,
        AccessURL : string
    },
    …]
}
```

Response Body Details

- **ManagedSystemID:** ID of the managed system.
- **AssetD:** Asset ID; set if the managed system is an asset or a database.
- **DatabaseID:** Database ID; set if the managed system is a database.
- **DirectoryID:** Directory ID; set if the managed system is a directory.
- **CloudID:** Cloud system ID; set if the managed system is a cloud system.
- **SystemName:** Name of the related entity (asset, directory, database, or cloud).
- **PlatformID:** ID of the managed system platform.
- **NetBiosName:** (Managed domains only) Domain NetBIOS name. Setting this value will allow Password Safe to fall back to the NetBIOS name if needed.
- **Port:** The port used to connect to the host. If null and the related **Platform.PortFlag** is true, Password Safe uses **Platform.DefaultPort** for communication.

- **Timeout:** (seconds) Connection timeout. Length of time in seconds before a slow or unresponsive connection to the system fails.
- **SshKeyEnforcementMode:** Enforcement mode for SSH host keys.
    - **0:** None.
    - **1:** Auto. Auto accept initial key.
    - **2:** Strict. Manually accept keys.
- **PasswordRuleID:** ID of the default password rule assigned to managed accounts created under this managed system.
- **DSSKeyRuleID:** ID of the default DSS key rule assigned to managed accounts created under this managed system.
- **LoginAccountID:** ID of the functional account used for SSH session logins.
- **ReleaseDuration:** (minutes: 1-525600) Default release duration.
- **MaxReleaseDuration:** (minutes: 1-525600) Default maximum release duration.
- **ISAReleaseDuration:** (minutes: 1-525600) Default Information Systems Administrator (ISA) release duration.
- **AutoManagementFlag:** True if password auto-management is enabled, otherwise false.
    - **FunctionalAccountID:** ID of the functional account used for local managed account password changes.
    - **ElevationCommand:** Elevation command to use (**sudo**, **pbrun**, **pmrun**).
    - **CheckPasswordFlag:** True to enable password testing, otherwise false.
    - **ChangePasswordAfterAnyReleaseFlag:** True to change passwords on release of a request, otherwise false.
    - **ResetPasswordOnMismatchFlag:** True to queue a password change when scheduled password test fails, otherwise false.
    - **ChangeFrequencyType:** The change frequency for scheduled password changes:
        - **first:** Changes scheduled for the first day of the month.
        - **last:** Changes scheduled for the last day of the month.
        - **xdays:** Changes scheduled every x days (see **ChangeFrequencyDays**).
    - **ChangeFrequencyDays:** (days: 1-90) When **ChangeFrequencyType** is **xdays**, password changes take place this configured number of days.
    - **ChangeTime:** (24hr format: 00:00-23:59) UTC time of day scheduled password changes take place.
- **RemoteClientType:** The type of remote client to use.
    - **None:** No remote client.
    - **EPM:** Endpoint Privilege Management.
- **ApplicationHostID:** Managed system ID of the target application host. Must be an ID of a managed system whose IsApplicationHost = true.
- **IsApplicationHost:** True if the managed system can be used as an application host, otherwise false. Can be set when the Platform.ApplicationHostFlag = true, and cannot be set when ApplicationHostID has a value.
- **AccessURL:** The URL used for cloud access (applies to cloud systems only).

Response Codes

200 - Request successful. Managed System in response body.

For more information, please see "Common Response Codes" on page 17.

PUT ManagedSystems/{id}

Purpose

Updates an existing managed system by ID.

> ***Note: PUT ManagedSystems/{id}*** *supports all managed system types: dynamic asset, static asset, dynamic database, static database, directory, and cloud.*

Required Permissions

Password Safe System Management (Read/Write).

URL Parameters

id: ID of the managed system.

Query Parameters

Version: (optional, default: 3.0) Request body model version (3.0, 3.1, 3.2, 3.3)

Request Body (version 3.0)

Content-Type: application/json

```
{
    WorkgroupID : int,

    HostName : string,

    IPAddress : string,
    DnsName : string,
    InstanceName : string,
    IsDefaultInstance : bool, // can be null
    Template : string,
    ForestName : string,
    UseSSL : bool, // can be null

    PlatformID : int,
    NetBiosName : string,
    ContactEmail : string,
    Description : string,
    Port : int, // can be null
    Timeout : short,
    SshKeyEnforcementMode : int, // can be null
    PasswordRuleID : int,
    DSSKeyRuleID : int, // can be null
```

```
    LoginAccountID : int, // can be null
    ReleaseDuration : int,
    MaxReleaseDuration : int,
    ISAReleaseDuration : int,
    AutoManagementFlag : bool,
    FunctionalAccountID : int, // can be null
    ElevationCommand : string, // can be null
    CheckPasswordFlag : bool,
    ChangePasswordAfterAnyReleaseFlag : bool,
    ResetPasswordOnMismatchFlag : bool,
    ChangeFrequencyType : string,
    ChangeFrequencyDays : int,
    ChangeTime : string,
    AccessURL : string
}
```

Request Body (version 3.1)

Content-Type: application/json

```
{
    WorkgroupID : int,

    HostName : string,

    IPAddress : string,
    DnsName : string,
    InstanceName : string,
    IsDefaultInstance : bool, // can be null
    Template : string,
    ForestName : string,
    UseSSL : bool, // can be null

    PlatformID : int,
    NetBiosName : string,
    ContactEmail : string,
    Description : string,
    Port : int, // can be null
    Timeout : short,
    SshKeyEnforcementMode : int, // can be null
    PasswordRuleID : int,
    DSSKeyRuleID : int, // can be null
    LoginAccountID : int, // can be null
    ReleaseDuration : int,
    MaxReleaseDuration : int,
    ISAReleaseDuration : int,
    AutoManagementFlag : bool,
    FunctionalAccountID : int, // can be null
    ElevationCommand : string, // can be null
    CheckPasswordFlag : bool,
    ChangePasswordAfterAnyReleaseFlag : bool,
    ResetPasswordOnMismatchFlag : bool,
    ChangeFrequencyType : string,
```

```
    ChangeFrequencyDays : int,
    ChangeTime : string,
    RemoteClientType : string,
    AccessURL : string
}
```

Request Body (version 3.2)

Content-Type: application/json

```
{
    WorkgroupID : int,
    HostName : string,
    IPAddress : string,
    DnsName : string,
    InstanceName : string,
    IsDefaultInstance : bool, // can be null
    Template : string,
    ForestName : string,
    UseSSL : bool, // can be null
    PlatformID : int,
    NetBiosName : string,
    ContactEmail : string,
    Description : string,
    Port : int, // can be null
    Timeout : short,
    SshKeyEnforcementMode : int, // can be null
    PasswordRuleID : int,
    DSSKeyRuleID : int, // can be null
    LoginAccountID : int, // can be null
    ReleaseDuration : int,
    MaxReleaseDuration : int,
    ISAReleaseDuration : int,
    AutoManagementFlag : bool,
    FunctionalAccountID : int, // can be null
    ElevationCommand : string, // can be null
    CheckPasswordFlag : bool,
    ChangePasswordAfterAnyReleaseFlag : bool,
    ResetPasswordOnMismatchFlag : bool,
    ChangeFrequencyType : string,
    ChangeFrequencyDays : int,
    ChangeTime : string,
    RemoteClientType : string,
    ApplicationHostID : int, // can be null
    IsApplicationHost : bool,
    AccessURL : string
}
```

Request Body (version 3.3)

Content-Type: application/json

```
{
    WorkgroupID : int,
    HostName : string,
    IPAddress : string,
    DnsName : string,
    InstanceName : string,
    IsDefaultInstance : bool, // can be null
    Template : string,
    ForestName : string,
    UseSSL : bool, // can be null
    PlatformID : int,
    NetBiosName : string,
    ContactEmail : string,
    Description : string,
    Port : int, // can be null
    Timeout : short,
    SshKeyEnforcementMode : int, // can be null
    PasswordRuleID : int,
    DSSKeyRuleID : int, // can be null
    LoginAccountID : int, // can be null
    ReleaseDuration : int,
    MaxReleaseDuration : int,
    ISAReleaseDuration : int,
    AutoManagementFlag : bool,
    FunctionalAccountID : int, // can be null
    ElevationCommand : string, // can be null
    CheckPasswordFlag : bool,
    ChangePasswordAfterAnyReleaseFlag : bool,
    ResetPasswordOnMismatchFlag : bool,
    ChangeFrequencyType : string,
    ChangeFrequencyDays : int,
    ChangeTime : string,
    RemoteClientType : string,
    ApplicationHostID : int, // can be null
    IsApplicationHost : bool,
    AccessURL : string
}
```

Request Body Details

- **WorkgroupID:** ID of the Workgroup.
- **HostName:** (required) Name of the host (applies to Static Asset, Static Database, Directory, Cloud). Max string length is 128 characters.
    - **Static Asset:** Asset Name.
    - **Static Database:** Database Host Name.
    - **Directory:** Directory/Domain Name.
    - **Cloud:** Cloud System Name.
- **IPAddress:** IPv4 address of the host (applies to Static Asset, Static Database).
- **DnsName:** DNS name of the host (applies to Static Asset, Static Database).
- **InstanceName:** Name of the database instance. Required when **IsDefaultInstance** is false (applies to Static Database only).

- **IsDefaultInstance:** True if the database instance is the default instance, otherwise false. Only Platforms MS SQL Server and MySQL support setting this value to true (applies to Static Database only).
- **Template:** The database connection template (applies to Static Database only).
- **ForestName:** Name of the Directory Forest (applies to Directory only).
- **UseSSL** (default: false) True to use an SSL connection, otherwise false (applies to Directory only).
- **PlatformID:** (required) ID of the Managed System Platform.
- **NetBiosName:** The NetBIOS name of the host. Can be set if **Platform.NetBiosNameFlag** is true.
- **Port:** (optional) The port used to connect to the host. If null and the related **Platform.PortFlag** is true, Password Safe uses **Platform.DefaultPort** for communication.
- **Timeout:** (seconds, default: 30) Connection timeout. Length of time in seconds before a slow or unresponsive connection to the system fails.
- **SshKeyEnforcementMode:** (default: 0/None) Enforcement mode for SSH host keys.
    - **0:** None.
    - **1:** Auto - Auto Accept Initial Key.
    - **2:** Strict - Manually Accept Keys.
- **PasswordRuleID:** (default: 0) ID of the default Password Rule assigned to Managed Accounts created under this Managed System.
- **DSSKeyRuleID:** (default: 0) ID of the default DSS Key Rule assigned to Managed Accounts created under this Managed System. Can be set when **Platform.DSSFlag** is true.
- **LoginAccountID:** (optional) ID of the Functional Account used for SSH Session logins. Can be set if the **Platform.LoginAccountFlag** is true.
- **ReleaseDuration:** (minutes: 1-525600, default: 120) Default release duration.
- **MaxReleaseDuration:** (minutes: 1-525600, default: 525600) Default maximum release duration.
- **ISAReleaseDuration:** (minutes: 1-525600, default: 120) Default Information Systems Administrator (ISA) release duration.
- **AutoManagementFlag:** (default: false) True if password auto-management is enabled, otherwise false. Can be set if **Platform.AutoManagementFlag** is true.
    - **FunctionalAccountID:** (required if **AutoManagementFlag** is true) ID of the Functional Account used for local Managed Account password changes. **FunctionalAccount.PlatformID** must either match the **ManagedSystem.PlatformID** or be a Directory Platform (AD, LDAP).
    - **ElevationCommand:** (optional) Elevation Command to use. Can be set if **Platform.SupportsElevationFlag** is true.
        - **sudo**
            - **pbrun**
            - **pmrun**
- **CheckPasswordFlag:** True to enable password testing, otherwise false.
- **ChangePasswordAfterAnyReleaseFlag:** True to change passwords on release of a request, otherwise false.
- **ResetPasswordOnMismatchFlag:** True to queue a password change when scheduled password test fails, otherwise false.
- **RemoteClientType:** (default: none) The type of remote client to use.
    - **None:** No remote client.
    - **EPM:** Endpoint Privilege Management.
- **ApplicationHostID:** (default: null, required when Platform.RequiresApplicationHost = true) Managed system ID of the target application host. Must be an ID of a managed system whose IsApplicationHost = true.

- **IsApplicationHost:** (default: false) True if the managed system can be used as an application host, otherwise false. Can be set when the Platform.ApplicationHostFlag = true, and cannot be set when ApplicationHostID has a value.
- **AccessURL:** (default: Default URL for the selected platform) The URL used for cloud access (applies to cloud systems only). Max string length is 2048.

Response Body

Content-Type: application/json

```
{
    WorkgroupID : int,
    ManagedSystemID : int,
    EntityTypeID: int,
    AssetID : int, // can be null
    DatabaseID : int, // can be null
    DirectoryID : int, // can be null
    CloudID : int, // can be null

    HostName : string,
    IPAddress : string,
    DnsName : string,
    InstanceName : string,
    IsDefaultInstance : bool, // can be null
    Template : string,
    ForestName : string,
    UseSSL : bool, // can be null

    SystemName : string,
    PlatformID : int,
    NetBiosName : string,
    ContactEmail : string,
    Description : string,
    Port : int, // can be null
    Timeout : short,
    SshKeyEnforcementMode : int, // can be null
    PasswordRuleID : int,
    DSSKeyRuleID : int, // can be null
    LoginAccountID : int, // can be null
    AccountNameFormat : int,
    OracleInternetDirectoryID : guid, // can be null
    OracleInternetDirectoryServiceName : string,
    ReleaseDuration : int,
    MaxReleaseDuration : int,
    ISAReleaseDuration : int,
    AutoManagementFlag : bool,
    FunctionalAccountID : int, // can be null
    ElevationCommand : string, // can be null
    CheckPasswordFlag : bool,
    ChangePasswordAfterAnyReleaseFlag : bool,
    ResetPasswordOnMismatchFlag : bool,
    ChangeFrequencyType : string,
    ChangeFrequencyDays : int,
    ChangeTime : string,
    RemoteClientType : string,
```

```
    ApplicationHostID : int, // can be null
    IsApplicationHost : bool,
    AccessURL : string
}
```

Response Body Details

- **ManagedSystemID:** ID of the managed system.
- **AssetD:** Asset ID; set if the managed system is an asset or a database.
- **DatabaseID:** Database ID; set if the managed system is a database.
- **DirectoryID:** Directory ID; set if the managed system is a directory.
- **CloudID:** Cloud system ID; set if the managed system is a cloud system.
- **SystemName:** Name of the related entity (asset, directory, database, or cloud).
- **PlatformID:** ID of the managed system platform.
- **NetBiosName:** (Managed domains only) Domain NetBIOS name. Setting this value will allow Password Safe to fall back to the NetBIOS name if needed.
- **Port:** The port used to connect to the host. If null and the related **Platform.PortFlag** is true, Password Safe uses **Platform.DefaultPort** for communication.
- **Timeout:** (seconds) Connection timeout. Length of time in seconds before a slow or unresponsive connection to the system fails.
- **SshKeyEnforcementMode:** Enforcement mode for SSH host keys.
    - **0:** None.
    - **1:** Auto. Auto accept initial key.
    - **2:** Strict. Manually accept keys.
- **PasswordRuleID:** ID of the default password rule assigned to managed accounts created under this managed system.
- **DSSKeyRuleID:** ID of the default DSS key rule assigned to managed accounts created under this managed system.
- **LoginAccountID:** ID of the functional account used for SSH session logins.
- **ReleaseDuration:** (minutes: 1-525600) Default release duration.
- **MaxReleaseDuration:** (minutes: 1-525600) Default maximum release duration.
- **ISAReleaseDuration:** (minutes: 1-525600) Default Information Systems Administrator (ISA) release duration.
- **AutoManagementFlag:** True if password auto-management is enabled, otherwise false.
    - **FunctionalAccountID:** ID of the functional account used for local managed account password changes.
    - **ElevationCommand:** Elevation command to use (**sudo**, **pbrun**, **pmrun**).
    - **CheckPasswordFlag:** True to enable password testing, otherwise false.
    - **ChangePasswordAfterAnyReleaseFlag:** True to change passwords on release of a request, otherwise false.
    - **ResetPasswordOnMismatchFlag:** True to queue a password change when scheduled password test fails, otherwise false.
    - **ChangeFrequencyType:** The change frequency for scheduled password changes:
        - **first:** Changes scheduled for the first day of the month.
        - **last:** Changes scheduled for the last day of the month.
        - **xdays:** Changes scheduled every x days (see **ChangeFrequencyDays**).

  - **ChangeFrequencyDays:** (days: 1-90) When **ChangeFrequencyType** is **xdays**, password changes take place this configured number of days.
  - **ChangeTime:** (24hr format: 00:00-23:59) UTC time of day scheduled password changes take place.
- **RemoteClientType:** The type of remote client to use.
  - **None:** No remote client.
  - **EPM:** Endpoint Privilege Management.
- **ApplicationHostID:** Managed system ID of the target application host. Must be an ID of a managed system whose IsApplicationHost = true.
- **IsApplicationHost:** True if the managed system can be used as an application host, otherwise false. Can be set when the Platform.ApplicationHostFlag = true, and cannot be set when ApplicationHostID has a value.
- **AccessURL:** The URL used for cloud access (applies to cloud systems only).

Response Codes

200 - Request successful. Managed System in response body.

For more information, please see "Common Response Codes" on page 17.

POST Assets/{assetId}/ManagedSystems

Purpose

Creates a managed system for the asset referenced by ID.

Required Permissions

Password Safe System Management (Read/Write).

URL Parameters

assetId: ID of the asset.

Query Parameters

Version: (optional, default: 3.0) Request body model version (3.0, 3.1, 3.2)

Request Body (version 3.0)

Content-Type: application/json

```
{
    PlatformID : int,
    ContactEmail : string,
    Description : string,
    Port : int, // can be null
    Timeout : short,
    SshKeyEnforcementMode : int, // can be null
    PasswordRuleID : int,
    DSSKeyRuleID : int, // can be null
    LoginAccountID : int, // can be null
    ReleaseDuration : int,
    MaxReleaseDuration : int,
    ISAReleaseDuration : int,

    AutoManagementFlag : bool,
    FunctionalAccountID : int, // can be null
    ElevationCommand : string, // can be null
    CheckPasswordFlag : bool,
    ChangePasswordAfterAnyReleaseFlag : bool,
    ResetPasswordOnMismatchFlag : bool,
    ChangeFrequencyType : string,
    ChangeFrequencyDays : int,
    ChangeTime : string,
}
```

Request Body (version 3.1)

Content-Type: application/json

```
{
    PlatformID : int,
    ContactEmail : string,
    Description : string,
    Port : int, // can be null
    Timeout : short,
    SshKeyEnforcementMode : int, // can be null
    PasswordRuleID : int,
    DSSKeyRuleID : int, // can be null
    LoginAccountID : int, // can be null
    ReleaseDuration : int,
    MaxReleaseDuration : int,
    ISAReleaseDuration : int,

    AutoManagementFlag : bool,
    FunctionalAccountID : int, // can be null
    ElevationCommand : string, // can be null
    CheckPasswordFlag : bool,
    ChangePasswordAfterAnyReleaseFlag : bool,
    ResetPasswordOnMismatchFlag : bool,
    ChangeFrequencyType : string,
    ChangeFrequencyDays : int,
    ChangeTime : string,
    RemoteClientType : string
}
```

Request Body (version 3.2)

Content-Type: application/json

```
{
    PlatformID : int,
    ContactEmail : string,
    Description : string,
    Port : int, // can be null
    Timeout : short,
    SshKeyEnforcementMode : int, // can be null
    PasswordRuleID : int,
    DSSKeyRuleID : int, // can be null
    LoginAccountID : int, // can be null
    ReleaseDuration : int,
    MaxReleaseDuration : int,
    ISAReleaseDuration : int,
    AutoManagementFlag : bool,
    FunctionalAccountID : int, // can be null
    ElevationCommand : string, // can be null
    CheckPasswordFlag : bool,
    ChangePasswordAfterAnyReleaseFlag : bool,
```

```
    ResetPasswordOnMismatchFlag : bool,
    ChangeFrequencyType : string,
    ChangeFrequencyDays : int,
    ChangeTime : string,
    RemoteClientType : string
    ApplicationHostID : int, // can be null
    IsApplicationHost : bool
}
```

Request Body Details

- **PlatformID:**(required) ID of the managed system platform.
- **ContactEmail:** Max string length is 1000.
- **Description:** Max string length is 255.
- **Port:** (optional) The port used to connect to the host. If null and the related **Platform.PortFlag** is true, Password Safe uses **Platform.DefaultPort** for communication.
- **Timeout:** (seconds, default: 30) Connection timeout. Length of time in seconds before a slow or unresponsive connection to the system fails.
- **SshKeyEnforcementMode:** (default: 0/None) Enforcement mode for SSH host keys.
    - **0:** None.
    - **1:** Auto. Auto accept initial key.
    - **2:** Strict. Manually accept keys.
- **PasswordRuleID:** (default: 0) ID of the default password rule assigned to managed accounts created under this managed system.
- **DSSKeyRuleID:** (default: 0) ID of the default DSS key rule assigned to managed accounts created under this managed system. Can be set when **Platform.DSSFlag** is true.
- **LoginAccountID:** (optional) ID of the functional account used for SSH Session logins. Can be set if the **Platform.LoginAccountFlag** is true.
- **ReleaseDuration:** (minutes: 1-525600, default: 120) Default release duration.
- **MaxReleaseDuration:** (minutes: 1-525600, default: 525600) Default maximum release duration.
- **ISAReleaseDuration:** (minutes: 1-525600, default: 120) Default Information Systems Administrator (ISA) release duration.
- **AutoManagementFlag:** (default: false) True if password auto-management is enabled, otherwise false. Can be set if **Platform.AutoManagementFlag** is true.
    - **FunctionalAccountID:** (required if **AutoManagementFlag** is true) ID of the functional account used for local managed account password changes. **FunctionalAccount.PlatformID** must either match the **ManagedSystem.PlatformID** or be a domain platform (AD, LDAP).
    - **ElevationCommand:** (optional) Elevation command to use. Can be set if **Platform.SupportsElevationFlag** is true (**sudo**, **pbrun**, **pmrun**).
    - **CheckPasswordFlag:** True to enable password testing, otherwise false.
    - **ChangePasswordAfterAnyReleaseFlag:** True to change passwords on release of a request, otherwise false.
    - **ResetPasswordOnMismatchFlag:** True to queue a password change when scheduled password test fails, otherwise false.

  - **ChangeFrequencyType:** (default: first) The change frequency for scheduled password changes:
    - **first:** Changes scheduled for the first day of the month.
    - **last:** Changes scheduled for the last day of the month.
    - **xdays:** Changes scheduled every x days (ChangeFrequencyDays).
  - **ChangeFrequencyDays:** (days: 1-999, required if **ChangeFrequencyType** is **xdays**) When **ChangeFrequencyType** is **xdays**, password changes take place this configured number of days.
  - **ChangeTime:** (24hr format: 00:00-23:59, default: 23:30) UTC time of day scheduled password changes take place.
- **RemoteClientType:** The type of remote client to use.
  - **None:** No remote client.
  - **EPM:** Endpoint Privilege Management.
- **ApplicationHostID:** (default: null, required when **Platform.RequiresApplicationHost** = true) Managed system ID of the target application host. Must be an ID of a managed system whose **IsApplicationHost** = true.
- **IsApplicationHost:** (default: false) true if the managed system can be used as an application host, otherwise false. Can be set when the **Platform.ApplicationHostFlag** = true, and cannot be set when **ApplicationHostID** has a value.

Response Body

Content-Type: application/json

```
[
    {
        WorkgroupID : int

        HostName : string

        IPAddress : string
        DNSName : string
        InstanceName : string
        IsDefaultInstance : bool // can be null
        Template : string
        ForestName : string
        UseSSL : bool // can be null

        ManagedSystemID : int,
        EntityTypeID : int,
        AssetID : int, // can be null
        DatabaseID : int, // can be null
        DirectoryID : int, // can be null
        CloudID : int, // can be null
        SystemName : string,
        Timeout : short,
        PlatformID: int,
        NetBiosName : string,
        ContactEmail : string,
        Description : string,
        Port : int, // can be null
        Timeout : short,
        SshKeyEnforcementMode : int, // can be null
        PasswordRuleID : int,
```

```
        DSSKeyRuleID : int, // can be null
        LoginAccountID : int, // can be null
        AccountNameFormat : int,
        OracleInternetDirectoryID : guid, // can be null
        OracleInternetDirectoryServiceName : string,
        ReleaseDuration : int,
        MaxReleaseDuration : int,
        ISAReleaseDuration : int,

        AutoManagementFlag : bool,
        FunctionalAccountID : int, // can be null
        ElevationCommand : string, // can be null
        CheckPasswordFlag : bool,
        ChangePasswordAfterAnyReleaseFlag : bool,
        ResetPasswordOnMismatchFlag : bool,
        ChangeFrequencyType : string,
        ChangeFrequencyDays : int,
        ChangeTime : string,
        RemoteClientType : string,
        ApplicationHostID : int, // can be nullIs
        ApplicationHost : bool,
        AccessURL : string
    },
    …
]
```

Response Body Details

- **ManagedSystemID:** ID of the managed system.
- **AssetD:** Asset ID; set if the managed system is an asset or a database.
- **DatabaseID:** Database ID; set if the managed system is a database.
- **DirectoryID:** Directory ID; set if the managed system is a directory.
- **CloudID:** Cloud system ID; set if the managed system is a cloud system.
- **SystemName:** Name of the related entity (asset, directory, database, or cloud).
- **PlatformID:** ID of the managed system platform.
- **NetBiosName:** (Managed domains only) Domain NetBIOS name. Setting this value will allow Password Safe to fall back to the NetBIOS name if needed.
- **Port:** The port used to connect to the host. If null and the related **Platform.PortFlag** is true, Password Safe uses **Platform.DefaultPort** for communication.
- **Timeout:** (seconds) Connection timeout. Length of time in seconds before a slow or unresponsive connection to the system fails.
- **SshKeyEnforcementMode:** Enforcement mode for SSH host keys.
    - **0:** None.
    - **1:** Auto. Auto accept initial key.
    - **2:** Strict. Manually accept keys.
- **PasswordRuleID:** ID of the default password rule assigned to managed accounts created under this managed system.
- **DSSKeyRuleID:** ID of the default DSS key rule assigned to managed accounts created under this managed system.
- **LoginAccountID:** ID of the functional account used for SSH session logins.

- **ReleaseDuration:** (minutes: 1-525600) Default release duration.
- **MaxReleaseDuration:** (minutes: 1-525600) Default maximum release duration.
- **ISAReleaseDuration:** (minutes: 1-525600) Default Information Systems Administrator (ISA) release duration.
- **AutoManagementFlag:** True if password auto-management is enabled, otherwise false.
    - **FunctionalAccountID:** ID of the functional account used for local managed account password changes.
    - **ElevationCommand:** Elevation command to use (**sudo**, **pbrun**, **pmrun**).
    - **CheckPasswordFlag:** True to enable password testing, otherwise false.
    - **ChangePasswordAfterAnyReleaseFlag:** True to change passwords on release of a request, otherwise false.
    - **ResetPasswordOnMismatchFlag:** True to queue a password change when scheduled password test fails, otherwise false.
    - **ChangeFrequencyType:** The change frequency for scheduled password changes:
        - **first:** Changes scheduled for the first day of the month.
        - **last:** Changes scheduled for the last day of the month.
        - **xdays:** Changes scheduled every x days (see **ChangeFrequencyDays**).
    - **ChangeFrequencyDays:** (days: 1-90) When **ChangeFrequencyType** is **xdays**, password changes take place this configured number of days.
    - **ChangeTime:** (24hr format: 00:00-23:59) UTC time of day scheduled password changes take place.
- **RemoteClientType:** The type of remote client to use.
    - **None:** No remote client.
    - **EPM:** Endpoint Privilege Management.
- **ApplicationHostID:** Managed system ID of the target application host. Must be an ID of a managed system whose IsApplicationHost = true.
- **IsApplicationHost:** True if the managed system can be used as an application host, otherwise false. Can be set when the Platform.ApplicationHostFlag = true, and cannot be set when ApplicationHostID has a value.
- **AccessURL:** The URL used for cloud access (applies to cloud systems only).

Response Codes

- 200 - Request successful - Asset was already managed. Managed System in response body.
- 201 - Request successful - Asset is now managed. Managed System in response body.

For more information, please see "Common Response Codes" on page 17.

POST Databases/{databaseID}/ManagedSystems

Purpose

Creates a managed system for the database referenced by ID.

Required Permissions

Password Safe System Management (Read/Write).

URL Parameters

databaseID: ID of the database.

Request Body

Content-Type: application/json

```
{
    ContactEmail : string,
    Description : string,
    Timeout : short,
    PasswordRuleID : int,
    ReleaseDuration : int,
    MaxReleaseDuration : int,
    ISAReleaseDuration : int,

    AutoManagementFlag : bool,
    FunctionalAccountID : int, // can be null
    CheckPasswordFlag : bool,
    ChangePasswordAfterAnyReleaseFlag : bool,
    ResetPasswordOnMismatchFlag : bool,
    ChangeFrequencyType : string,
    ChangeFrequencyDays : int,
    ChangeTime : string,
}
```

Request Body Details

- **ContactEmail:** Max string length is 1000.
- **Description:** Max string length is 255.
- **Timeout:** (seconds, default: 30) Connection timeout. Length of time in seconds before a slow or unresponsive connection to the system fails.
- **PasswordRuleID:** (default: 0) ID of the default password rule assigned to managed accounts created under this managed system.
- **ReleaseDuration:** (minutes: 1-525600, default: 120) Default release duration.

- **MaxReleaseDuration:** (minutes: 1-525600, default: 525600) Default maximum release duration.
- **ISAReleaseDuration:** (minutes: 1-525600, default: 120) Default Information Systems Administrator (ISA) release duration.
- **AutoManagementFlag:** (default: false) True if password auto-management is enabled, otherwise false. Can be set if **Platform.AutoManagementFlag** is true.
    - **FunctionalAccountID:** (required if **AutoManagementFlag** is true) ID of the functional account used for local managed account password changes. **FunctionalAccount.PlatformID** must either match the **ManagedSystem.PlatformID** or be a domain platform (AD, LDAP).
    - **CheckPasswordFlag:** True to enable password testing, otherwise false.
    - **ChangePasswordAfterAnyReleaseFlag:** True to change passwords on release of a request, otherwise false.
    - **ResetPasswordOnMismatchFlag:** True to queue a password change when scheduled password test fails, otherwise false.
    - **ChangeFrequencyType:** (default: first) The change frequency for scheduled password changes:
        - **first:** Changes scheduled for the first day of the month.
        - **last:** Changes scheduled for the last day of the month.
        - **xdays:** Changes scheduled every x days (see **ChangeFrequencyDays**).
    - **ChangeFrequencyDays:** (days: 1-999, required if **ChangeFrequencyType** is **xdays**) When **ChangeFrequencyType** is **xdays**, password changes take place this configured number of days.
    - **ChangeTime:** (24hr format: 00:00-23:59, default: 23:30) UTC time of day scheduled password changes take place.

Response Body

Content-Type: application/json

```
[
    {
        WorkgroupID : int

        HostName : string

        IPAddress : string
        DNSName : string
        InstanceName : string
        IsDefaultInstance : bool // can be null
        Template : string
        ForestName : string
        UseSSL : bool // can be null

        ManagedSystemID : int,
        EntityTypeID: int,
        AssetID : int, // can be null
        DatabaseID : int, // can be null
        DirectoryID : int, // can be null
        CloudID : int, // can be null
        SystemName : string,
        Timeout : short,
        PlatformID: int,
        NetBiosName : string,
        ContactEmail : string,
```

```
        Description : string,
        Port : int, // can be null
        Timeout : short,
        SshKeyEnforcementMode : int, // can be null
        PasswordRuleID : int,
        DSSKeyRuleID : int, // can be null
        LoginAccountID : int, // can be null
        AccountNameFormat : int,
        OracleInternetDirectoryID : guid, // can be null
        OracleInternetDirectoryServiceName : string,
        ReleaseDuration : int,
        MaxReleaseDuration : int,
        ISAReleaseDuration : int,

        AutoManagementFlag : bool,
        FunctionalAccountID : int, // can be null
        ElevationCommand : string, // can be null
        CheckPasswordFlag : bool,
        ChangePasswordAfterAnyReleaseFlag : bool,
        ResetPasswordOnMismatchFlag : bool,
        ChangeFrequencyType : string,
        ChangeFrequencyDays : int,
        ChangeTime : string,
        RemoteClientType : string,
        ApplicationHostID : int, // can be nullIs
        ApplicationHost : bool,
        AccessURL : string
    },
    …
]
```

Response Body Details

- **ManagedSystemID:** ID of the managed system.
- **AssetD:** Asset ID; set if the managed system is an asset or a database.
- **DatabaseID:** Database ID; set if the managed system is a database.
- **DirectoryID:** Directory ID; set if the managed system is a directory.
- **CloudID:** Cloud system ID; set if the managed system is a cloud system.
- **SystemName:** Name of the related entity (asset, directory, database, or cloud).
- **PlatformID:** ID of the managed system platform.
- **NetBiosName:** (Managed domains only) Domain NetBIOS name. Setting this value will allow Password Safe to fall back to the NetBIOS name if needed.
- **Port:** The port used to connect to the host. If null and the related **Platform.PortFlag** is true, Password Safe uses **Platform.DefaultPort** for communication.
- **Timeout:** (seconds) Connection timeout. Length of time in seconds before a slow or unresponsive connection to the system fails.
- **SshKeyEnforcementMode:** Enforcement mode for SSH host keys.
    - **0:** None.
    - **1:** Auto. Auto accept initial key.
    - **2:** Strict. Manually accept keys.

- **PasswordRuleID:** ID of the default password rule assigned to managed accounts created under this managed system.
- **DSSKeyRuleID:** ID of the default DSS key rule assigned to managed accounts created under this managed system.
- **LoginAccountID:** ID of the functional account used for SSH session logins.
- **ReleaseDuration:** (minutes: 1-525600) Default release duration.
- **MaxReleaseDuration:** (minutes: 1-525600) Default maximum release duration.
- **ISAReleaseDuration:** (minutes: 1-525600) Default Information Systems Administrator (ISA) release duration.
- **AutoManagementFlag:** True if password auto-management is enabled, otherwise false.
    - **FunctionalAccountID:** ID of the functional account used for local managed account password changes.
    - **ElevationCommand:** Elevation command to use (**sudo**, **pbrun**, **pmrun**).
    - **CheckPasswordFlag:** True to enable password testing, otherwise false.
    - **ChangePasswordAfterAnyReleaseFlag:** True to change passwords on release of a request, otherwise false.
    - **ResetPasswordOnMismatchFlag:** True to queue a password change when scheduled password test fails, otherwise false.
    - **ChangeFrequencyType:** The change frequency for scheduled password changes:
        - **first:** Changes scheduled for the first day of the month.
        - **last:** Changes scheduled for the last day of the month.
        - **xdays:** Changes scheduled every x days (see **ChangeFrequencyDays**).
    - **ChangeFrequencyDays:** (days: 1-90) When **ChangeFrequencyType** is **xdays**, password changes take place this configured number of days.
    - **ChangeTime:** (24hr format: 00:00-23:59) UTC time of day scheduled password changes take place.
- **RemoteClientType:** The type of remote client to use.
    - **None:** No remote client.
    - **EPM:** Endpoint Privilege Management.
- **ApplicationHostID:** Managed system ID of the target application host. Must be an ID of a managed system whose IsApplicationHost = true.
- **IsApplicationHost:** True if the managed system can be used as an application host, otherwise false. Can be set when the Platform.ApplicationHostFlag = true, and cannot be set when ApplicationHostID has a value.
- **AccessURL:** The URL used for cloud access (applies to cloud systems only).

Response Codes

- 200 - Request successful - Asset was already managed. Managed System in response body.
- 201 - Request successful - Asset is now managed. Managed System in response body.

For more information, please see "Common Response Codes" on page 17.

POST Workgroups/{id}/ManagedSystems

Purpose

Creates a managed system in the Workgroup referenced by ID.

Required Permissions

Password Safe System Management (Read/Write).

URL Parameters

id: ID of the Workgroup.

version: (optional, default: 3.0) Request body model version (3.0, 3.1, 3.2, 3.3).

Request Body (version 3.0)

Content-Type: application/json

```
{
    EntityTypeID : int,

    HostName : string,
    IPAddress : string,
    DnsName : string,
    InstanceName : string,
    IsDefaultInstance : bool, // can be null
    Template : string,
    ForestName : string,
    UseSSL : bool, // can be null

    PlatformID : int,
    NetBiosName : string,
    ContactEmail : string,
    Description : string,
    Port : int, // can be null
    Timeout : short,
    SshKeyEnforcementMode : int, // can be null
    PasswordRuleID : int,
    DSSKeyRuleID : int, // can be null
    LoginAccountID : int, // can be null
    AccountNameFormat : int,
    OracleInternetDirectoryID : guid, // can be null
    OracleInternetDirectoryServiceName : string,
    ReleaseDuration : int,
    MaxReleaseDuration : int,
    ISAReleaseDuration : int,
    AutoManagementFlag : bool,
    FunctionalAccountID : int, // can be null
```

```
    ElevationCommand : string, // can be null
    CheckPasswordFlag : bool,
    ChangePasswordAfterAnyReleaseFlag : bool,
    ResetPasswordOnMismatchFlag : bool,
    ChangeFrequencyType : string,
    ChangeFrequencyDays : int,
    ChangeTime : string,
    AccessURL : string
}
```

Request Body (version 3.1)

Content-Type: application/json

```
{
    EntityTypeID : int,

    HostName : string,
    IPAddress : string,
    DnsName : string,
    InstanceName : string,
    IsDefaultInstance : bool, // can be null
    Template : string,
    ForestName : string,
    UseSSL : bool, // can be null

    PlatformID : int,
    NetBiosName : string,
    ContactEmail : string,
    Description : string,
    Port : int, // can be null
    Timeout : short,
    SshKeyEnforcementMode : int, // can be null
    PasswordRuleID : int,
    DSSKeyRuleID : int, // can be null
    LoginAccountID : int, // can be null
    AccountNameFormat : int,
    OracleInternetDirectoryID : guid, // can be null
    OracleInternetDirectoryServiceName : string,
    ReleaseDuration : int,
    MaxReleaseDuration : int,
    ISAReleaseDuration : int,
    AutoManagementFlag : bool,
    FunctionalAccountID : int, // can be null
    ElevationCommand : string, // can be null
    CheckPasswordFlag : bool,
    ChangePasswordAfterAnyReleaseFlag : bool,
    ResetPasswordOnMismatchFlag : bool,
    ChangeFrequencyType : string,
    ChangeFrequencyDays : int,
    ChangeTime : string,
    RemoteClientType : string,
```

```
    AccessURL : string
}
```

Request Body (version 3.2)

Content-Type: application/json

```
{
    EntityTypeID : int,
    HostName : string,
    IPAddress : string,
    DnsName : string,
    InstanceName : string,
    IsDefaultInstance : bool, // can be null
    Template : string,
    ForestName : string,
    UseSSL : bool, // can be null
    PlatformID : int,
    NetBiosName : string,
    ContactEmail : string,
    Description : string,
    Port : int, // can be null
    Timeout : short,
    SshKeyEnforcementMode : int, // can be null
    PasswordRuleID : int,
    DSSKeyRuleID : int, // can be null
    LoginAccountID : int, // can be null
    AccountNameFormat : int,
    OracleInternetDirectoryID : guid, // can be null
    OracleInternetDirectoryServiceName : string,
    ReleaseDuration : int,
    MaxReleaseDuration : int,
    ISAReleaseDuration : int,
    AutoManagementFlag : bool,
    FunctionalAccountID : int, // can be null
    ElevationCommand : string, // can be null
    CheckPasswordFlag : bool,
    ChangePasswordAfterAnyReleaseFlag : bool,
    ResetPasswordOnMismatchFlag : bool,
    ChangeFrequencyType : string,
    ChangeFrequencyDays : int,
    ChangeTime : string,
    ApplicationHostID : int, // can be null
    IsApplicationHost : bool,
    RemoteClientType : string,
    AccessURL : string
}
```

Request Body (version 3.3)

Content-Type: application/json

```
{
    EntityTypeID : int,
    HostName : string,
    IPAddress : string,
    DnsName : string,
    InstanceName : string,
    IsDefaultInstance : bool, // can be null
    Template : string,
    ForestName : string,
    UseSSL : bool, // can be null
    PlatformID : int,
    NetBiosName : string,
    ContactEmail : string,
    Description : string,
    Port : int, // can be null
    Timeout : short,
    SshKeyEnforcementMode : int, // can be null
    PasswordRuleID : int,
    DSSKeyRuleID : int, // can be null
    LoginAccountID : int, // can be null
    AccountNameFormat : int,
    OracleInternetDirectoryID : guid, // can be null
    OracleInternetDirectoryServiceName : string,
    ReleaseDuration : int,
    MaxReleaseDuration : int,
    ISAReleaseDuration : int,
    AutoManagementFlag : bool,
    FunctionalAccountID : int, // can be null
    ElevationCommand : string, // can be null
    CheckPasswordFlag : bool,
    ChangePasswordAfterAnyReleaseFlag : bool,
    ResetPasswordOnMismatchFlag : bool,
    ChangeFrequencyType : string,
    ChangeFrequencyDays : int,
    ChangeTime : string,
    RemoteClientType : string,
    ApplicationHostID : int, // can be null
    IsApplicationHost : bool,
    AccessURL : string
}
```

Request Body Details

- **EntityTypeID:** (required) Type of entity being created.
- **HostName:** (required) Name of the host (applies to static asset, static database, directory, cloud). Max string length is 128 characters.
    - **Static Asset:** Asset name.
    - **Static Database:** Database host name.
    - **Directory:** Directory/domain name.
    - **Cloud:** Cloud system name.
- **IPAddress:** IPv4 address of the host (applies to static asset, static database). Max string length is 45.

- **DnsName:** DNS name of the host (applies to static asset, static database). Max string length is 255.
- **InstanceName:** Name of the database instance. Required when **IsDefaultInstance** is false (applies to static database only). Max string length is 100.
- **IsDefaultInstance:** True if the database instance is the default instance, otherwise false. Only platforms MS SQL Server and MySQL support setting this value to true (applies to static database only).
- **Template:** The database connection template (applies to static database only).
- **ForestName:** Name of the directory forest (required for Active Directory; optional for Entra ID). Max string length is 64.
- **UseSSL** (default: false) True to use an SSL connection, otherwise false (applies to directory only).
- **PlatformID:** (required) ID of the managed system platform.
- **NetBiosName:** The NetBIOS name of the host. Can be set if **Platform.NetBiosNameFlag** is true. Max string length is 15.
- **ContactEmail:** Max string length is 1000.
- **Description:** Max string length is 255.
- **Port:** (optional) The port used to connect to the host. If null and the related **Platform.PortFlag** is true, Password Safe uses **Platform.DefaultPort** for communication.
- **Timeout:** (seconds, default: 30) Connection timeout. Length of time in seconds before a slow or unresponsive connection to the system fails.
- **SshKeyEnforcementMode:** (default: 0/None) Enforcement mode for SSH host keys.
    - **0:** None
    - **1:** Auto. Auto accept initial key.
    - **2:** Strict. Manually accept keys.
- **PasswordRuleID:** (default: 0) ID of the default password rule assigned to managed accounts created under this managed system.
- **DSSKeyRuleID:** (default: 0) ID of the default DSS key rule assigned to managed accounts created under this managed system. Can be set when **Platform.DSSFlag** is true.
- **LoginAccountID:** (optional) ID of the functional account used for SSH session logins. Can be set if the **Platform.LoginAccountFlag** is true.
- **AccountNameFormat:** (Active Directory only, default: 0) Account name format to use:
    - **0:** Domain and account. Use **ManagedAccount.DomainName\ManagedAccount.AccountName**.
    - **1:** UPN. Use the managed account UPN.
    - **2:** SAM. Use the managed account SAM account name.
- **OracleInternetDirectoryID:** The Oracle Internet Directory ID (applies to database entity types and Oracle platform only).
- **OracleInternetDirectoryServiceName:** (required when **OracleInternetDirectoryID** is set) The database service name related to the given **OracleInternetDirectoryID** (applies to database entity types and Oracle platform only). Max string length is 200.
- **ReleaseDuration:** (minutes: 1-525600, default: 120) Default release duration.
- **MaxReleaseDuration:** (minutes: 1-525600, default: 525600) Default maximum release duration.
- **ISAReleaseDuration:** (minutes: 1-525600, default: 120) Default Information Systems Administrator (ISA) release duration.
- **AutoManagementFlag:** (default: false) True if password auto-management is enabled, otherwise false. Can be set if **Platform.AutoManagementFlag** is true.
    - **FunctionalAccountID:** (required if **AutoManagementFlag** is true) ID of the functional account used for local managed account password changes. **FunctionalAccount.PlatformID** must either match the **ManagedSystem.PlatformID** or be a directory platform (AD, LDAP).

    - **ElevationCommand:** (optional) Elevation command to use. Can be set if **Platform.SupportsElevationFlag** is true.
        - **sudo**
        - **pbrun**
        - **pmrun**

- **CheckPasswordFlag:** True to enable password testing, otherwise false.
- **ChangePasswordAfterAnyReleaseFlag:** True to change passwords on release of a request, otherwise false.
- **ResetPasswordOnMismatchFlag:** True to queue a password change when scheduled password test fails, otherwise false.
- **ApplicationHostID:** (default: null, required when **Platform.RequiresApplicationHost** = true) Managed system ID of the target application host. Must be an ID of a managed system where **IsApplicationHost** = true.
- **IsApplicationHost:** (default: false) true if the managed system can be used as an application host, otherwise false. Can be set when the **Platform.ApplicationHostFlag** = true, and cannot be set when **ApplicationHostID** has a value.
- **RemoteClientType:** (default: None) The type of remote client to use.
    - **None:** No remote client.
    - **EPM:** Endpoint Privilege Management.
- **AccessURL:** (default: default URL for the selected platform) The URL used for cloud access (applies to cloud systems only). Max string length is 2048.

Response Body (when limit is not given)

Content-Type: application/json

```
{
    WorkgroupID : int,
    ManagedSystemID : int,
    EntityTypeID : int,
    AssetID : int, // can be null
    DatabaseID : int, // can be null
    DirectoryID : int, // can be null
    CloudID : int, // can be null

    HostName : string,
    IPAddress : string,
    DnsName : string,
    InstanceName : string,
    IsDefaultInstance : bool, // can be null
    Template : string,
    ForestName : string,
    UseSSL : bool, // can be null
    AccountNameFormat : int,

    SystemName : string,
    PlatformID : int,
    NetBiosName : string,
    ContactEmail : string,
    Description : string,
    Port : int, // can be null
    Timeout : short,
    SshKeyEnforcementMode : int, // can be null
```

```
    PasswordRuleID : int,
    DSSKeyRuleID : int, // can be null
    LoginAccountID : int, // can be null
    AccountNameFormat : int,
    OracleInternetDirectoryID : guid, // can be null
    OracleInternetDirectoryServiceName : string,
    ReleaseDuration : int,
    MaxReleaseDuration : int,
    ISAReleaseDuration : int,
    AutoManagementFlag : bool,
    FunctionalAccountID : int, // can be null
    ElevationCommand : string, // can be null
    CheckPasswordFlag : bool,
    ChangePasswordAfterAnyReleaseFlag : bool,
    ResetPasswordOnMismatchFlag : bool,
    ChangeFrequencyType : string,
    ChangeFrequencyDays : int,
    ChangeTime : string,
    RemoteClientType : string,
    ApplicationHostID : int, // can be null
    IsApplicationHost : bool,
    AccessURL : string
}
```

Response Body Details

- **ManagedSystemID:** ID of the managed system.
- **AssetD:** Asset ID; set if the managed system is an asset or a database.
- **DatabaseID:** Database ID; set if the managed system is a database.
- **DirectoryID:** Directory ID; set if the managed system is a directory.
- **CloudID:** Cloud system ID; set if the managed system is a cloud system.
- **SystemName:** Name of the related entity (asset, directory, database, or cloud).
- **PlatformID:** ID of the managed system platform.
- **NetBiosName:** (Managed domains only) Domain NetBIOS name. Setting this value will allow Password Safe to fall back to the NetBIOS name if needed.
- **Port:** The port used to connect to the host. If null and the related **Platform.PortFlag** is true, Password Safe uses **Platform.DefaultPort** for communication.
- **Timeout:** (seconds) Connection timeout. Length of time in seconds before a slow or unresponsive connection to the system fails.
- **SshKeyEnforcementMode:** Enforcement mode for SSH host keys.
    - **0:** None.
    - **1:** Auto. Auto accept initial key.
    - **2:** Strict. Manually accept keys.
- **PasswordRuleID:** ID of the default password rule assigned to managed accounts created under this managed system.
- **DSSKeyRuleID:** ID of the default DSS key rule assigned to managed accounts created under this managed system.
- **LoginAccountID:** ID of the functional account used for SSH session logins.
- **ReleaseDuration:** (minutes: 1-525600) Default release duration.
- **MaxReleaseDuration:** (minutes: 1-525600) Default maximum release duration.

- **ISAReleaseDuration:** (minutes: 1-525600) Default Information Systems Administrator (ISA) release duration.
- **AutoManagementFlag:** True if password auto-management is enabled, otherwise false.
    - **FunctionalAccountID:** ID of the functional account used for local managed account password changes.
    - **ElevationCommand:** Elevation command to use (**sudo**, **pbrun**, **pmrun**).
    - **CheckPasswordFlag:** True to enable password testing, otherwise false.
    - **ChangePasswordAfterAnyReleaseFlag:** True to change passwords on release of a request, otherwise false.
    - **ResetPasswordOnMismatchFlag:** True to queue a password change when scheduled password test fails, otherwise false.
    - **ChangeFrequencyType:** The change frequency for scheduled password changes:
        - **first:** Changes scheduled for the first day of the month.
        - **last:** Changes scheduled for the last day of the month.
        - **xdays:** Changes scheduled every x days (see **ChangeFrequencyDays**).
    - **ChangeFrequencyDays:** (days: 1-90) When **ChangeFrequencyType** is **xdays**, password changes take place this configured number of days.
    - **ChangeTime:** (24hr format: 00:00-23:59) UTC time of day scheduled password changes take place.
- **RemoteClientType:** The type of remote client to use.
    - **None:** No remote client.
    - **EPM:** Endpoint Privilege Management.
- **ApplicationHostID:** Managed system ID of the target application host. Must be an ID of a managed system whose IsApplicationHost = true.
- **IsApplicationHost:** True if the managed system can be used as an application host, otherwise false. Can be set when the Platform.ApplicationHostFlag = true, and cannot be set when ApplicationHostID has a value.
- **AccessURL:** The URL used for cloud access (applies to cloud systems only).

Response Codes

200 - Request successful. Managed System in response body.

For more information, please see "Common Response Codes" on page 17.

DELETE ManagedSystems/{id}

Purpose

Deletes a managed system by ID.

> ***Note: DELETE ManagedSystems/{id}*** *supports all managed system types: dynamic asset, static asset, dynamic database, static database, directory, and cloud.*

Required Permissions

Password Safe System Management (Read/Write).

URL Parameters

id: ID of the managed system.

Request Body

None.

Response Body

None.

Response Codes

200 - Request successful.

> *For more information, please see "Common Response Codes" on page 17.*

Quick Rule Managed Systems

Quick Navigation

GET QuickRules/{quickRuleID}/ManagedSystems

Purpose

Returns a list of managed systems by Quick Rule ID.

Required Permissions

Read access to the Quick Rule.

URL Parameters

quickRuleID: ID of the Quick Rule.

Request Body

None.

Response Body

Content-Type: application/json

```
[
    {
        WorkgroupID : int
        HostName : string
        IPAddress : string
        DNSName : string
        InstanceName : string
        IsDefaultInstance : bool // can be null
        Template : string
        ForestName : string
        UseSSL : bool // can be null
        ManagedSystemID : int,
        EntityTypeID : int,
```

```
        AssetID : int, // can be null
        DatabaseID : int, // can be null
        DirectoryID : int, // can be null
        CloudID : int, // can be null
        SystemName : string,
        Timeout : short,
        PlatformID: int,
        NetBiosName : string,
        ContactEmail : string,
        Description : string,
        Port : int, // can be null
        Timeout : short,
        SshKeyEnforcementMode : int, // can be null
        PasswordRuleID : int,
        DSSKeyRuleID : int, // can be null
        LoginAccountID : int, // can be null
        AccountNameFormat : int,
        OracleInternetDirectoryID : guid, // can be null
        OracleInternetDirectoryServiceName : string,
        ReleaseDuration : int,
        MaxReleaseDuration : int,
        ISAReleaseDuration : int,
        AutoManagementFlag : bool,
        FunctionalAccountID : int, // can be null
        ElevationCommand : string, // can be null
        CheckPasswordFlag : bool,
        ChangePasswordAfterAnyReleaseFlag : bool,
        ResetPasswordOnMismatchFlag : bool,
        ChangeFrequencyType : string,
        ChangeFrequencyDays : int,
        ChangeTime : string,
        RemoteClientType : string,
        ApplicationHostID : int, // can be null
        IsApplicationHost : bool,
        AccessURL : string
    },
    …
]
```

Response Codes

200 – Request successful. Managed Systems in the response body.

For more information, please see "Common Response Codes" on page 17.

PUT QuickRules/{quickRuleID}/ManagedSystems

Purpose

Updates the entire list of Managed Systems in a Quick Rule by removing all **Managed System - Quick Rule** filters and adding a new one with the Managed Systems referenced by ID.

Required Permissions

Password Safe System Management (Read).

Read/Write access to the Quick Rule.

URL Parameters

quickRuleID: ID of the Quick Rule.

Request Body

Content-Type: application/json

```
{
    IDs: [ int, …]
}
```

Response Body

Content-Type: application/json

```
[
    {
        WorkgroupID : int
        HostName : string
        IPAddress : string
        DNSName : string
        InstanceName : string
        IsDefaultInstance : bool // can be null
        Template : string
        ForestName : string
        UseSSL : bool // can be null
        ManagedSystemID : int,
        EntityTypeID : int,
        AssetID : int, // can be null
        DatabaseID : int, // can be null
        DirectoryID : int, // can be null
        CloudID : int, // can be null
        SystemName : string,
        Timeout : short,
```

```
        PlatformID: int,
        NetBiosName : string,
        ContactEmail : string,
        Description : string,
        Port : int, // can be null
        Timeout : short,
        SshKeyEnforcementMode : int, // can be null
        PasswordRuleID : int,
        DSSKeyRuleID : int, // can be null
        LoginAccountID : int, // can be null
        AccountNameFormat : int,
        OracleInternetDirectoryID : guid, // can be null
        OracleInternetDirectoryServiceName : string,
        ReleaseDuration : int,
        MaxReleaseDuration : int,
        ISAReleaseDuration : int,
        AutoManagementFlag : bool,
        FunctionalAccountID : int, // can be null
        ElevationCommand : string, // can be null
        CheckPasswordFlag : bool,
        ChangePasswordAfterAnyReleaseFlag : bool,
        ResetPasswordOnMismatchFlag : bool,
        ChangeFrequencyType : string,
        ChangeFrequencyDays : int,
        ChangeTime : string,
        RemoteClientType : string,
        ApplicationHostID : int, // can be null
        IsApplicationHost : bool,
        AccessURL : string
    },
    …
]
```

Respon seCodes

200 – Request successful. Managed Systems in the response body.

For more information, please see "Common Response Codes" on page 17.

POST QuickRules/{quickRuleID}/ManagedSystems/{systemID}

Purpose

Adds the Managed System referenced by ID to the Quick Rule by adding it to the first **Managed System - Quick Rule** filter found.

Required Permissions

Password Safe System Management (Read).

Read/Write access to the Quick Rule.

URL Parameters

quickRuleID: ID of the Quick Rule.

systemID: ID of the Managed System.

Request Body

None.

Response Body

Content-Type: application/json

```
[
    {
        WorkgroupID : int
        HostName : string
        IPAddress : string
        DNSName : string
        InstanceName : string
        IsDefaultInstance : bool // can be null
        Template : string
        ForestName : string
        UseSSL : bool // can be null
        ManagedSystemID : int,
        EntityTypeID : int,
        AssetID : int, // can be null
        DatabaseID : int, // can be null
        DirectoryID : int, // can be null
        CloudID : int, // can be null
        SystemName : string,
        Timeout : short,
        PlatformID: int,
        NetBiosName : string,
        ContactEmail : string,
        Description : string,
        Port : int, // can be null
        Timeout : short,
        SshKeyEnforcementMode : int, // can be null
        PasswordRuleID : int,
        DSSKeyRuleID : int, // can be null
        LoginAccountID : int, // can be null
        AccountNameFormat : int,
        OracleInternetDirectoryID : guid, // can be null
        OracleInternetDirectoryServiceName : string,
        ReleaseDuration : int,
        MaxReleaseDuration : int,
        ISAReleaseDuration : int,
        AutoManagementFlag : bool,
        FunctionalAccountID : int, // can be null
        ElevationCommand : string, // can be null
```

```
        CheckPasswordFlag : bool,
        ChangePasswordAfterAnyReleaseFlag : bool,
        ResetPasswordOnMismatchFlag : bool,
        ChangeFrequencyType : string,
        ChangeFrequencyDays : int,
        ChangeTime : string,
        RemoteClientType : string,
        ApplicationHostID : int, // can be null
        IsApplicationHost : bool,
        AccessURL : string
    },
    …
]
```

Response Codes

200 – Request successful. Managed Systems in the response body.

For more information, please see "Common Response Codes" on page 17.

DELETE QuickRules/{quickRuleID}/ManagedSystems/{systemID}

Purpose

Removes the Managed System referenced by ID from the Quick Rule by removing it from all **Managed System - Quick Rule** filters found.

IMPORTANT!

A rule cannot be left in an invalid state. If removing the system would result in an empty filter, the filter itself will be removed. If there are no filters left in the rule, a "400 Bad Request" is returned.

- *If you intend to replace all systems in the rule, see "PUT QuickRules/{quickRuleID}/ManagedSystems" on page 337.*
- *If you intend to delete the rule, see "DELETE QuickRules/{id}" on page 369.*

Required Permissions

Read/Write access to the Quick Rule.

URL Parameters

quickRuleID: ID of the Quick Rule.

systemID: ID of the Managed System.

Request Body

None.

Response Codes

200 – Request successful.

For more information, please see "Common Response Codes" on page 17.

Smart Rule Managed Systems

GET SmartRules/{id}/ManagedSystems

Purpose

Returns a list of managed systems by Smart Rule ID.

Required Permissions

- Read access to the Smart Rule referenced by ID.

URL Parameters

id: ID of the Smart Rule.

Query Parameters (Optional)

- **limit:** (default: 100000) Number of records to return.
- **offset:** (default: 0) Number of records to skip before returning <limit> records (can be used only in conjunction with limit).

Request Body

None.

Response Body (when limit is not given)

Content-Type: application/json

```
[
    {
        ManagedSystemID : int,
        AssetID : int, // can be null
        DatabaseID : int, // can be null
        DirectoryID : int, // can be null
        CloudID : int, // can be null
        SystemName : string,
        PlatformID : int,
        NetBiosName : string,
        ContactEmail : string,
        Description : string,
        Port : int, // can be null
        Timeout : short,
        SshKeyEnforcementMode : int, // can be null
```

```
        PasswordRuleID : int,
        DSSKeyRuleID : int, // can be null
        LoginAccountID : int, // can be null
        ReleaseDuration : int,
        MaxReleaseDuration : int,
        ISAReleaseDuration : int,
        AutoManagementFlag : bool,
        FunctionalAccountID : int, // can be null
        ElevationCommand : string, // can be null
        CheckPasswordFlag : bool,
        ChangePasswordAfterAnyReleaseFlag : bool,
        ResetPasswordOnMismatchFlag : bool,
        ChangeFrequencyType : string,
        ChangeFrequencyDays : int,
        ChangeTime : string,
        RemoteClientType : string,
        ApplicationHostID : int, // can be null
        IsApplicationHost : bool,
        AccessURL : string
    },
    …
]
```

Response Body (when limit is given)

Content-Type: application/json

```
{
    TotalCount : int,
    Data :
    [
        {
            ManagedSystemID : int,
            AssetID : int, // can be null
            DatabaseID : int, // can be null
            DirectoryID : int, // can be null
            CloudID : int, // can be null
            SystemName : string,
            PlatformID : int,
            NetBiosName : string,
            ContactEmail : string,
            Description : string,
            Port : int, // can be null
            Timeout : short,
            PasswordRuleID : int,
            DSSKeyRuleID : int, // can be null
            LoginAccountID : int, // can be null
            ReleaseDuration : int,
            MaxReleaseDuration : int,
            ISAReleaseDuration : int,
            AutoManagementFlag : bool,
            FunctionalAccountID : int, // can be null
            ElevationCommand : string, // can be null
```

```
            CheckPasswordFlag : bool,
            ChangePasswordAfterAnyReleaseFlag : bool,
            ResetPasswordOnMismatchFlag : bool,
            ChangeFrequencyType : string,
            ChangeFrequencyDays : int,
            ChangeTime : string,
            RemoteClientType : string,
            ApplicationHostID : int, // can be null
            IsApplicationHost : bool,
            AccessURL : string
        },
    …]
}
```

Response Codes

200 - Request successful. Managed Systems in response body.

For more information, please see "Common Response Codes" on page 17.

Nodes

Nodes represent the session monitoring agent nodes that can be used for establishing sessions.

For more information on related topics, please see "Sessions" on page 397.

GET Nodes

Purpose

Returns a list of session monitoring agent nodes.

Query Parameters

includeInactive: (optional, default: false) **True** to return all nodes including nodes that are inactive, otherwise **False**.

Request Body

None.

Response Body

Content-Type: application/json

```
[
    {
        NodeID: string,
        HostName: string,
        DisplayName: string,
        LastHeartbeat: DateTime, // can be null
        IsActive: bool,
    },
    …
]
```

Response Body Details

- **NodeID:** Node unique ID.
- **HostName:** Node host name.
- **DisplayName:** Node display name.
- **LastHeartbeat:** The date and time of the last session monitoring agent heartbeat from this node.
- **IsActive:** True if the session monitoring agent is considered active and running, otherwise false.

Response Codes

200 - Request successful. Nodes in the response body.

For more information, please see "Common Response Codes" on page 17.

Password Policies

> ***Note:*** *Password policies are formerly known as password rules but the API remains* ***PasswordRules*** *to be compatible with earlier versions.*

Quick Navigation

- "GET PasswordRules" on page 347
- "GET PasswordRules?enabledproducts={productName}" on page 348
- "GET PasswordRules/{id}" on page 350

GET PasswordRules

Purpose

Returns a list of password rules.

Required Permissions

Password Safe System Management (Read).

Request Body

None.

Response Body

Content-Type: application/json

```
[
    {
        PasswordRuleID : int,
        Name : string,
        Description : string,
        MinimumLength : int,
        MaximumLength : int,
        FirstCharacterRequirement : char,
        LowercaseRequirement : char,
        UppercaseRequirement : char,
        NumericRequirement : char,
        SymbolRequirement : char,
        ValidLowercaseCharacters : char[],
        ValidUppercaseCharacters : char[],
        ValidSymbols : char[],
```

```
            EnabledProducts : int
        },
        …
]
```

Response Body Details

- **FirstCharacterRequirement:** The first character of the password must be:
    - **C:** Characters (alpha) only.
    - **N:** Numeric permitted, in addition to alpha characters.
    - **A:** Any character permitted.
- **LowercaseRequirement:** Lowercase character requirements:
- **UppercaseRequirement:** Uppercase character requirements:
- **NumericRequirement:** Numeric requirements:
- **SymbolRequirement:** Symbol requirements:
    - **N:** Not permitted.
    - **P:** Permitted, not required.
    - **R:** Required.
- **EnabledProducts:** The type of products to return:
    - **1:** Password Safe.
    - **2:** Secrets Safe.

Response Codes

200 - Request successful. Password Rules in the response body.

400 - Enabled product not valid.

For more information, please see "Common Response Codes" on page 17.

GET PasswordRules?enabledproducts={productName}

Purpose

Returns a list of password rules, with an optional parameter to return polices enabled for Password Safe or Secrets Safe.

Required Permissions

Password Safe System Management (Read).

Query Parameters

{string} The product name to select polices enabled for Password Safe or Secrets Safe:

- **1:** PasswordSafe
- **2:** SecretsSafe

Request Body

None.

Response Body

Content-Type: application/json

```
[
         {
            PasswordRuleID : int,
            Name : string,
            Description : string,
            MinimumLength : int,
            MaximumLength : int,
            FirstCharacterRequirement : char,
            LowercaseRequirement : char,
            UppercaseRequirement : char,
            NumericRequirement : char,
            SymbolRequirement : char,
            ValidLowercaseCharacters : char[],
            ValidUppercaseCharacters : char[],
            ValidSymbols : char[],
            EnabledProducts : int
         },
         …
]
```

Response Body Details

- **FirstCharacterRequirement:** The first character of the password must be:
  - **C:** Characters (alpha) only.
  - **N:** Numeric permitted, in addition to alpha characters.
  - **A:** Any character permitted.
- **LowercaseRequirement:** Lowercase character requirements:
- **UppercaseRequirement:** Uppercase character requirements:
- **NumericRequirement:** Numeric requirements:

- **SymbolRequirement:** Symbol requirements:
  - **N:** Not permitted.
  - **P:** Permitted, not required.
  - **R:** Required.
- **EnabledProducts:** The type of products to return:
  - **1:** Password Safe.
  - **2:** Secrets Safe.

Response Codes

200 - Request successful. Password Rules in the response body.

400 - Enabled product not valid.

For more information, please see "Common Response Codes" on page 17.

GET PasswordRules/{id}

Purpose

Returns a password rule by ID.

Required Permissions

Password Safe System Management (Read).

URL Parameters

id: ID of the password rule.

Request Body

None.

Response Body

Content-Type: application/json

```
{
    PasswordRuleID: int,
    Name: string,
    Description: string,
```

```
    MinimumLength: int,
    MaximumLength: int,
    FirstCharacterRequirement: char,
    LowercaseRequirement: char,
    UppercaseRequirement: char,
    NumericRequirement: char,
    SymbolRequirement: char,
    ValidLowercaseCharacters: char[],
    ValidUppercaseCharacters: char[],
    ValidSymbols: char[],
    EnabledProducts : int
}
```

Response Body Details

- **FirstCharacterRequirement:** The first character of the password must be:
  - **C:** Characters (alpha) only.
  - **N:** Numeric permitted, in addition to alpha characters.
  - **A:** Any character permitted.
- **LowercaseRequirement:** Lowercase character requirements:
- **UppercaseRequirement:** Uppercase character requirements:
- **NumericRequirement:** Numeric requirements:
- **SymbolRequirement:** Symbol requirements:
  - **N:** Not permitted.
  - **P:** Permitted, not required.
  - **R:** Required.
- **EnabledProducts:** The type of products to return:
  - **1:** Password Safe.
  - **2:** Secrets Safe.

Response Codes

200 - Request successful. Password rules in the response body.

400 - Enabled product not valid.

For more information, please see "Common Response Codes" on page 17.

Platforms

Quick Navigation

For more information on related topics, please see "Entity Types" on page 203

GET Platforms

Purpose

Returns a list of platforms for managed systems.

Required Permissions

None.

Request Body

None.

Response Body

Content-Type: application/json

```
[
    {
        PlatformID : int,
        Name : string,
        ShortName : string,
        PortFlag : bool,
        DefaultPort : int, // can be null
        SupportsElevationFlag : bool,
        DomainNameFlag : bool,
        AutoManagementFlag : bool,
        DSSAutoManagementFlag : bool,
        ManageableFlag : bool,
        DSSFlag : bool,
        LoginAccountFlag : bool,
        DefaultSessionType : string // can be null,
        ApplicationHostFlag : bool,
```

```
        RequiresApplicationHost : bool,
        RequiresTenantID : bool,
        RequiresObjectID : bool,
        RequiresSecret : bool
    }
    …
]
```

Response Body Details

- **PlatformID:** Platform ID.
- **Name:** Platform name.
- **ShortName:** Platform short name.
- **PortFlag:** True if the platform supports setting a port, otherwise false.
- **DefaultPort:** The default port used when no port is given for managed systems of this platform.
- **DomainNameFlag:** True if the platform supports setting a domain name on a functional account of this platform, otherwise false.
- **SupportsElevationFlag:** True if the platform supports elevation, otherwise false.
- **AutoManagementFlag:** True if the platform supports password auto-management, otherwise false.
- **DSSAutoManagementFlag:** True if the platform supports DSS key auto-management, otherwise false.
- **ManageableFlag:** True if functional accounts can be created for the platform, otherwise false.
- **DSSFlag:** True if the platform supports DSS keys, otherwise false.
- **LoginAccountFlag:** True if the platform supports SSH login accounts, otherwise false.
- **DefaultSessionType:** The default type of session for the platform (RDP, SSH, or null).
- **ApplicationHostFlag:** true if the platform supports being used as a managed system application host, otherwise false.
- **RequiresApplicationHost:** true if the platform requires a target application host, otherwise false.
- **RequiresTenantID:** true if the platform requires a TenantID.
- **RequiresObjectID:** true if the platform requires an ObjectID.
- **RequiresSecret:** true if the platform requires a secret.

Response Codes

200 – Request successful. Platforms in response body.

For more information, please see "Common Response Codes" on page 17.

GET Platforms/{id}

Purpose

Returns a platform by ID for managed systems.

Required Permissions

None.

URL Parameters

id: ID of the platform.

Request Body

None.

Response Body

Content-Type: application/json

```
{
    PlatformID : int,
    Name : string,
    ShortName : string,
    PortFlag : bool,
    DefaultPort: int, // can be null
    SupportsElevationFlag : bool,
    DomainNameFlag: bool,
    AutoManagementFlag: bool,
    DSSAutoManagementFlag: bool,
    ManageableFlag: bool,
    DSSFlag: bool,
    LoginAccountFlag : bool,
    DefaultSessionType: string // can be null,
    ApplicationHostFlag : bool,
    RequiresApplicationHost : bool,
    RequiresTenantID : bool,
    RequiresObjectID : bool,
    RequiresSecret : bool
}
```

Response Body Details

- **PlatformID:** Platform ID.
- **Name:** Platform name.
- **ShortName:** Platform short name.
- **PortFlag:** True if the platform supports setting a port, otherwise false.
- **DefaultPort:** The default port used when no port is given for managed systems of this platform.
- **DomainNameFlag:** True if the platform supports setting a domain name on a functional account of this platform, otherwise false.
- **SupportsElevationFlag:** True if the platform supports elevation, otherwise false.
- **AutoManagementFlag:** True if the platform supports password auto-management, otherwise false.

- **DSSAutoManagementFlag:** True if the platform supports DSS key auto-management, otherwise false.
- **ManageableFlag:** True if functional accounts can be created for the platform, otherwise false.
- **DSSFlag:** True if the platform supports DSS keys, otherwise false.
- **LoginAccountFlag:** True if the platform supports SSH login accounts, otherwise false.
- **DefaultSessionType:** The default type of session for the platform (RDP, SSH, or null).
- **ApplicationHostFlag:** true if the platform supports being used as a managed system application host, otherwise false.
- **RequiresApplicationHost:** true if the platform requires a target application host, otherwise false.
- **RequiresTenantID:** true if the platform requires a TenantID.
- **RequiresObjectID:** true if the platform requires an ObjectID.
- **RequiresSecret:** true if the platform requires a secret.

Response Codes

200 – Request successful. Platform in response body.

For more information, please see "Common Response Codes" on page 17.

GET EntityTypes/{id}/Platforms

Purpose

Returns a list of Platforms by entity type ID.

Required Permissions

None.

URL Parameters

id: ID of the entity type.

Request Body

None.

Response Body

Content-Type: application/json

```
{
    PlatformID : int,
```

```
    Name : string,
    ShortName : string,
    PortFlag : bool,
    DefaultPort: int, // can be null
    SupportsElevationFlag : bool,
    DomainNameFlag: bool,
    AutoManagementFlag: bool,
    DSSAutoManagementFlag: bool,
    ManageableFlag: bool,
    DSSFlag: bool,
    LoginAccountFlag : bool,
    DefaultSessionType: string // can be null,
    ApplicationHostFlag : bool,
    RequiresApplicationHost : bool
    RequiresTenantID : bool,
    RequiresObjectID : bool,
    RequiresSecret : bool
}
```

Response Body Details

- **PlatformID:** Platform ID.
- **Name:** Platform name.
- **ShortName:** Platform short name.
- **PortFlag:** True if the platform supports setting a port, otherwise false.
- **DefaultPort:** The default port used when no port is given for managed systems of this platform.
- **DomainNameFlag:** True if the platform supports setting a domain name on a functional account of this platform, otherwise false.
- **SupportsElevationFlag:** True if the platform supports elevation, otherwise false.
- **AutoManagementFlag:** True if the platform supports password auto-management, otherwise false.
- **DSSAutoManagementFlag:** True if the platform supports DSS key auto-management, otherwise false.
- **ManageableFlag:** True if functional accounts can be created for the platform, otherwise false.
- **DSSFlag:** True if the platform supports DSS keys, otherwise false.
- **LoginAccountFlag:** True if the platform supports SSH login accounts, otherwise false.
- **DefaultSessionType:** The default type of session for the platform (RDP, SSH, or null).
- **ApplicationHostFlag:** true if the platform supports being used as a managed system application host, otherwise false.
- **RequiresApplicationHost:** true if the platform requires a target application host, otherwise false.
- **RequiresTenantID:** true if the platform requires a TenantID.
- **RequiresObjectID:** true if the platform requires an ObjectID.
- **RequiresSecret:** true if the platform requires a secret.

Response Codes

200 – Request successful. Platform in response body.

For more information, please see "Common Response Codes" on page 17.

Propagation Action Types

GET PropagationActionTypes

Purpose

Returns a list of propagation action types.

Required Permissions

Password Safe Account Management (Read).

Request Body

None.

Response Body

Content-Type: application/json

```
[
    {
    PropagationActionTypeID : int,
    Name : string,
    }, ...
]
```

Response Codes

200 – Request successful. Propagation action types in the response body.

For more information, please see "Common Response Codes" on page 17.

Propagation Actions

Quick Navigation

GET PropagationActions

Purpose

Returns a list of propagation actions.

Required Permissions

Password Safe Account Management (Read).

Request Body

None.

Response Body

Content-Type: application/json

```
[
    {
    PropagationActionID : int,
    PropagationActionTypeID : int,
    Name : string,
    Description : string,
    }, ...
]
```

Response Codes

200 – Request successful. Propagation actions in the response body.

For more information, please see "Common Response Codes" on page 17.

GET PropagationActions/{id}

Purpose

Returns a propagation action by ID.

Required Permissions

Password Safe Account Management (Read).

Request Body

None.

Response Body

Content-Type: application/json

```
{
    PropagationActionID : int,
    PropagationActionTypeID : int,
    Name : string,
    Description : string,
    }
```

Response Codes

200 – Request successful. Propagation action in the response body.

For more information, please see "Common Response Codes" on page 17.

Managed Account Propagation Actions

Quick Navigation

GET ManagedAccounts/{id}/PropagationActions/

Purpose

Returns a list of assigned propagation actions by managed account ID.

Required Permissions

Password Safe Account Management (Read).

Request Body

None.

Response Body

Content-Type: application/json

```
[
    {
    PropagationActionID : int,
    PropagationActionTypeID : int,
    Name : string,
    Description : string,
    SmartRuleID : int? // can be null
    }, ...
]
```

Response Codes

200 - Request successful. Propagation Actions in the response body.

For more information, please see "Common Response Codes" on page 17.

POST ManagedAccounts/{id}/PropagationActions/{propagationActionID}

Purpose

Assigns a propagation action to the managed account referenced by ID.

Required Permissions

Password Safe Account Management (Read/Write).

Request Body (optional)

Content-Type: application/json

```
{
    SmartRuleID : int? // can be null
    }
```

Request Body Details

SmartRuleID : (optional) ID of the managed system-based Smart Rule to use for the propagation action assignment. If null or not given, uses scan data to determine propagation targets.

Response Body

Content-Type: application/json

```
{
    PropagationActionID : int,
    PropagationActionTypeID : int,
    Name : string,
    Description : string,
    SmartRuleID : int? // can be null
    }
```

Response Codes

200 - Propagation action was already assigned. Propagation action in the response body.

201 - Propagation action was assigned successfully. Propagation action in the response body.

For more information, please see "Common Response Codes" on page 17.

DELETE ManagedAccounts/{id}/PropagationActions/

Purpose

Unassigns all propagation actions from the managed account by ID.

Required Permissions

Password Safe Account Management (Read/Write).

Request Body

None.

Response Body

None.

Response Codes

200 - Request successful.

For more information, please see "Common Response Codes" on page 17.

DELETE ManagedAccounts/{id}/PropagationActions/{propagationActionID}

Purpose

Unassigns a propagation action from the managed account by ID.

Required Permissions

Password Safe Account Management (Read/Write).

Request Body

None.

Response Body

None.

Response Codes

200 - Request successful.

> *For more information, please see "Common Response Codes" on page 17.*

Quick Rules

Quick Rules are a specialized Smart Rule for building a list of known managed accounts by ID. Smart Rules are considered Quick Rules when they contain at least one **Managed Account Fields - Quick Group ID** filter. Quick Rules can also be accessed via the SmartRules API endpoint.

Quick Navigation

For more information on related topics, please see:

- *"GET QuickRules/{quickRuleID}/ManagedAccounts" on page 267*
- *"PUT QuickRules/{quickRuleID}/ManagedAccounts" on page 270*
- *"POST QuickRules/{quickRuleID}/ManagedAccounts/{accountID}" on page 273*
- *"DELETE QuickRules/{quickRuleID}/ManagedAccounts/{accountID}" on page 275*

POST QuickRules

Purpose

Creates a new Quick Rule with the managed accounts or systems referenced by ID and Rule Type.

Required Permissions

When RuleType=ManagedAccount:

- Password Safe Account Management (Read).
- Smart Rule Management - Managed Account (Read/Write).

When RuleType=ManagedSystem:

- Password Safe System Management (Read).
- Smart Rule Management - Managed System (Read/Write).

Request Body

Content-Type: application/json

> ***Note:*** *AccountIDs are deprecated. Use IDs instead.*

```
{
    IDs : [ int, …],
    Title : string,
    Category : string,
    Description : string,
    RuleType : string
}
```

Request Body Details

- **AccountIDs:** (deprecated) A list of managed account IDs to add to the Quick Rule.
- **IDs:** (required) A list of IDs to add to the Quick Rule.
- **Title:** (required) The title/name of the new Quick Rule. Must be unique across all Quick Rules and all Smart Rules. Max string length is 75.
- **Category:** (optional, default: Quick Rules) The category in which to place the Quick Rule. Max string length is 50.
- **Description:** (optional, default: <value of Title>) The Quick Rule description.
- **RuleType:** (ManagedAccount, ManagedSystem, default: ManagedAccount)

Response Body

Content-Type: application/json

```
{
    SmartRuleID : int,
    OrganizationID : string, // can be null
    Title : string,
    Description : string,
    Category : string,
    Status : int,
    LastProcessedDate : datetime,
    IsReadOnly : bool,
    RuleType : string
}
```

Response Codes

201 – Request successful. Quick Rule in the response body.

> *For more information, please see "Common Response Codes" on page 17.*

GET QuickRules

Purpose

Returns a list of Quick Rules to which the current user has at least Read access.

Request Body

None.

Response Body

Content-Type: application/json

```
[
    {
        SmartRuleID : int,
        OrganizationID : string, // can be null
        Title : string,
        Description : string,
        Category : string,
        Status : int,
        LastProcessedDate : datetime,
        IsReadOnly : bool,
        RuleType : string
    },
    …
]
```

Response Codes

200 – Request successful. Quick Rules in the response body.

For more information, please see "Common Response Codes" on page 17.

GET QuickRules/{id}

Purpose

Returns a Quick Rule by ID.

Required permissions

Read access to the Quick Rule referenced by ID.

URL Parameters

id: ID of the Quick Rule.

Request Body

None.

Response Body

Content-Type: application/json

```
{
    SmartRuleID : int,
    OrganizationID : string, // can be null
    Title : string,
    Description : string,
    Category : string,
    Status : int,
    LastProcessedDate : datetime,
    IsReadOnly : bool,
    RuleType : string
}
```

Response Codes

200 – Request successful. Quick Rule in the response body.

For more information, please see "Common Response Codes" on page 17.

GET QuickRules?title={title}

Purpose

Returns a Quick Rule by title.

In a multi-tenant environment, assumes global organization.

Required permissions

Read access to the Quick Rule referenced by title.

Query Parameters

title: Title of the Quick Rule.

Request Body

None.

Response Body

Content-Type: application/json

```
{
    SmartRuleID : int,
    OrganizationID : string, // can be null
    Title : string,
    Description : string,
    Category : string,
    Status : int,
    LastProcessedDate : datetime,
    IsReadOnly : bool,
    RuleType : string
}
```

Response Codes

200 – Request successful. Quick Rule in the response body.

For more information, please see "Common Response Codes" on page 17.

GET Organizations/{orgID}/QuickRules?title={title}

Purpose

Returns a Quick Rule by organization ID and title.

Only valid in a mult-tenant environment.

Required permissions

Read access to the Quick Rule referenced by organization and title.

URL Parameters

orgID: ID of the organization.

Query Parameters

title: Title of the Quick Rule.

Request Body

None.

Response Body

Content-Type: application/json

```
{
    SmartRuleID : int,
    OrganizationID : string, // can be null
    Title : string,
    Description : string,
    Category : string,
    Status : int,
    LastProcessedDate : datetime,
    IsReadOnly : bool,
    RuleType : string
}
```

Response Codes

200 – Request successful. Quick Rule in the response body.

For more information, please see "Common Response Codes" on page 17.

DELETE QuickRules/{id}

Purpose

Deletes a Quick Rule by ID.

Required Permissions

Read/Write access to the Quick Rule referenced by ID.

URL Parameters

ID: ID of the Quick Rule.

Request Body

None.

Response Body

None.

Response Codes

200 – Request successful.

For more information, please see "Common Response Codes" on page 17.

DELETE QuickRules?title={title}

Purpose

Deletes a Quick Rule by title.

In a mult-tenant environment, assumes global organization.

Required Permissions

Read/Write access to the Quick Rule referenced by title.

Query Parameters

title: Title of the Quick Rule.

Request Body

None.

Response Body

None.

Response Codes

200 – Request successful.

For more information, please see "Common Response Codes" on page 17.

DELETE Organizations/{orgID}/QuickRules?title={title}

Purpose

Deletes a Quick Rule by organization ID and title. Only valid in a multi-tenant environment.

Required permissions

Read/Write access to the Quick Rule referenced by organization and title.

URL Parameters

orgID: ID of the organization.

Query Parameters

title: Title of the Quick Rule.

Request Body

None.

Response Body

None.

Response Codes

200 – Request successful.

For more information, please see "Common Response Codes" on page 17.

Replay

Quick Navigation

POST pbsm/replay

Purpose

Creates a new replay session for a specified session token. The session token can be discovered using the sessions endpoints.

Query Parameters

None.

Request Body

Content-Type: application/json

```
{
    id: string, // Session Token from query to <base>/Sessions endpoint
    record_key: string, // RecordKey from query to <base>/Sessions endpoint
    protocol: string, // When session Type is 0 this should be RDP or for type 1 SSH
    headless: boolean // Must be set to true
}
```

Response Body

Content-Type: application/json

```
{
    id: string, // ReplayID for this replay session
    token: string, // ReplayID for this replay session
    ticket: string, // Ticket value used internally
}
```

Response Codes

- 200 – Request successful.
- 403 – Access forbidden. Response body contains a message or status code indicating the reason for this forbidden access:
- 404 – Not found. The requested replay session was not found on the server.

For more information, please see "Common Response Codes" on page 17.

GET pbsm/replay/{replayId}

Purpose

Displays the replay session details.

URL Parameters

ReplayID: ID of the replay session returned from **POST pbsm/replay**.

Query Parameters

- **jpeg=(scale):** Requests a JPEG image of the current RDP replay session scaled in size by the given scale.
- **png=(scale):** Requests a PNG image of the current RDP replay session scaled in size by the given scale.
- **screen=1:** Requests a text representation of the current SSH session.

Request Body

None.

Response Body

Content-Type: application/json

```
{
    tstamp: int, // Start time of the session in seconds
    end: int, // End time of the session in seconds
    offset: int, // Current offset of replay session in ms
    next: int, // Offset of next activity of replay session in ms
    speed: int, // Speed of replay session as a %
    eof: boolean, // Set to true when the end of the replay has been reached
    duration: int // Duration in ms of the replay session
}
```

Response Codes

- 200 – Request successful.
- 403 – Access forbidden. Response body contains a message or status code indicating the reason for this forbidden access.
- 404 – Not found. The requested replay session was not found on the server.

For more information, please see "Common Response Codes" on page 17.

PUT pbsm/replay/{replayId}

Purpose

Controls the replay session status.

URL Parameters

ReplayID: ID of the replay session returned from **POST pbsm/replay**.

Query Parameters

None.

Request Body

```
{
    speed: int, // Sets the replay speed of this session as a %
    offset: int, // Sets the offset of the replay cursor for this session in ms
    next: int // Requests the next changed frame based on the given % change
}
```

Response Body

Content-Type: application/json

```
{
    tstamp: int, // Start time of the session in seconds
    end: int, // End time of the session in seconds
    offset: int, // Current offset of replay session in ms
    next: int, // Offset of next activity of replay session in ms
    speed: int, // Speed of replay session as a %
    eof: boolean, // Set to true when the end of the replay has been reached
    duration: int // Duration in ms of the replay session
}
```

Response Codes

- 200 – Request successful.
- 403 – Access forbidden. Response body contains a message or status code indicating the reason for this forbidden access:
- 404 – Not found. The requested replay session was not found on the server.

For more information, please see "Common Response Codes" on page 17.

DELETE pbsm/replay/{replayId}

Purpose

Terminates the replay session.

URL Parameters

ReplayID: ID of the replay session returned from **POST pbsm/replay**.

Query Parameters

None.

Request Body

None.

Response Codes

- 200 – Request successful.
- 403 – Access forbidden. Response body contains a message or status code indicating the reason for this forbidden access:
- 404 – Not found. The requested replay session was not found on the server.

For more information, please see "Common Response Codes" on page 17.

Requests

Quick Navigation

For more information on related topics, please see "Credentials" on page 179.

GET Requests

Purpose

Lists requests for the current user.

Query Parameters

- **status:** (optional, default: all) Status of requests to return.
  - **all:** Both active and pending requests.
  - **active:** Requests that have been approved (including auto-approved).
  - **pending:** Requests that have not yet been approved.
- **queue:** (optional, default: req): Type of request queue to return.
  - **req:** Requestor queue, returns requests available to the user as a requestor.
  - **app:** Approver queue, returns requests for an approver or requestor/approver that have either been approved by the user (active) or have not yet been approved (pending).

Request Body

None.

Response Body

Content-Type: application/json

```
[
    {
        RequestID: int,
        SystemID: int,
        SystemName: string,
        AccountID: int,
        AccountName: string,
        DomainName: string,
        AliasID: int,
        ApplicationID: int,
        RequestReleaseDate: date-formatted string,
        ApprovedDate: date-formatted string,
        ExpiresDate: date-formatted string,
        Status: string,
        AccessType: string,
        Reason: string
    },
    …
]
```

Response Codes

- 200 – Request successful. Requests in the response body.
- 403 – Access forbidden. Response body contains a message or status code indicating the reason for this forbidden access:
    - 4033 – Approver Only API or account. Only Approvers can access this API or account.

For more information, please see "Common Response Codes" on page 17.

POST Requests

Purpose

Creates a new release request.

Required Roles

- Requestor or requestor/approver role to managed account referenced by ID

For information on ISA role access, please see "ISA Requests" on page 210.

Request Body

Content-Type: application/json

```
{
    AccessType: string,
    SystemID: int,
    AccountID: int,
    ApplicationID: int, // can be null
    DurationMinutes : int,
    Reason : string,
    AccessPolicyScheduleID : int, // can be null
    ConflictOption : string,
    TicketSystemID : int,
    TicketNumber : string,
    RotateOnCheckin: bool
}
```

Request Body Details

- **AccessType:** (optional, default: View) The type of access requested (View, RDP, SSH, App).
  - **View: View Password** access.
  - **RDP:** RDP access (corresponds to **POST Sessions SessionType RDP** or **rdpfile**).
  - **SSH:** SSH access (corresponds to **POST Sessions SessionType SSH**).
  - **App:** Application access (corresponds to **POST Sessions SessionType App** or **appfile**).
- **SystemID:** (required) ID of the managed system to request.
- **AccountID:** (required) ID of the managed account to request.
- **ApplicationID:** (required when **AccessType=App**): ID of the application for an application-based request.
- **DurationMinutes:** (required: 1-525600) The request duration (in minutes).
- **Reason:** (optional) The reason for the request.
- **AccessPolicyScheduleID:** (optional) The schedule ID of an access policy to use for the request. If omitted, automatically selects the best schedule.
- **ConflictOption:** (optional) The conflict resolution option to use if an existing request is found for the same user, system, and account (reuse, renew). If omitted and a conflicting request is found, returns a 409 code (see below).
  - **reuse:** Returns an existing, approved request ID for the same user/system/account/access type (if one exists). If the request does not already exist, creates a new request using the request body details.
  - **renew:** Cancels any existing approved requests for the same user/system/account and creates a new request using the request body details.
- **TicketSystemID:** ID of the ticket system. If omitted, then default ticket system will be used.
- **TicketNumber:** Number of associated ticket. Can be required if ticket system is marked as required in the access policy used. Max string length is 20.
- **RotateOnCheckin:** (optional, default: true) True to rotate the credentials on check-in/expiry, otherwise false. This property can only be used if the access policy (either auto-selected or given in **AccessPolicyScheduleID**) supports it.

> ***Note:*** *In reference to* ***RotateOnCheckin****, If the Managed Account given in* ***AccountID*** *does not rotate the credentials after check-in/expiry, this setting is ignored.*

> *For more information, please see the **Allow API Rotation Override** access policy setting under **View** access.*

Response Body

```
{
    RequestID: int
}
```

Response Codes

- 200 – Existing request is being reused. Existing request ID in the response body.
- 201 – Request successful. Request ID in the response body.
- 403 – User does not have permissions to request the indicated account or the account does not have API access enabled. Response body contains a status code indicating the reason for this forbidden access:
    - 4031 – User does not have permission to request the account or the account is not valid for the system.
    - 4033 – Approver Only API or account. Only Approvers can access this API or account.
    - 4035 - Not enough Approvers configured to approve a request.
- 409 – Conflicting request exists. This user or another user has already requested a password for the specified account within the next <durationMinutes> window.

> *For more information, please see "Common Response Codes" on page 17.*

POST Aliases/{aliasId}/Requests

Purpose

Creates a new release request using an alias.

Required Roles

Requestor or requestor/approver role to managed account referenced by the alias.

URL Parameters

aliasId: ID of the managed account alias.

Request Body

Content-Type: application/json

```
{
    AccessType: string,
    DurationMinutes : int,
    Reason : string,
    AccessPolicyScheduleID : int, // can be null
    ConflictOption : string,
    TicketSystemID : int,
    TicketNumber : string,
    RotateOnCheckin: bool
}
```

Request Body Details

- **AccessType:** (optional, default: View) The type of access requested (View, RDP, SSH, App).
  - **View:** View password access.
  - **RDP:** RDP access (corresponds to **POST Sessions SessionType RDP** or **rdpfile**).
  - **SSH:** SSH access (corresponds to **POST Sessions SessionType SSH**).
- **DurationMinutes:** (required: 1-525600): The request duration (in minutes).
- **Reason:** (optional) The reason for the request.
- **AccessPolicyScheduleID:** (optional) The schedule ID of an access policy to use for the request. If omitted, automatically selects the best schedule.
- **ConflictOption:** (optional) The conflict resolution option to use if an existing request is found for the same user, system, and account (reuse, renew). If omitted and a conflicting request is found, returns a 409 (see below).
  - **reuse:** Return an existing, approved request ID for the same user/system/account/access type (if one exists). If the request does not already exist, creates a new request using the request body details.
  - **renew:** Cancel any existing approved requests for the same user/system/account and create a new request using the request body details.
- **TicketSystemID:** ID of the ticket system. If omitted then default ticket system is used.
- **TicketNumber:** Number of associated ticket. Can be required if ticket system is marked as required in the access policy used. Max string length is 20.
- **RotateOnCheckin:** (optional, default: true) True to rotate the credentials on check-in/expiry, otherwise false. This property can only be used if the access policy (either auto-selected or given in **AccessPolicyScheduleID**) supports it. If the managed account given in **AccountID** does not rotate the credentials after check-in/expiry, this setting is ignored.

> *For more information, please see the **Allow API Rotation Override** access policy setting under **View** access.*

Response Body

```
{
    RequestID: int
}
```

Response Codes

- 200 – Existing request is being reused. Existing request ID in the response body.
- 201 – Request successful. Request ID in the response body.
- 403 – User does not have permissions to request the indicated alias or the account referenced by the alias does not have API access enabled. Response body contains a status code indicating the reason for this forbidden access:
    - 4031 – User does not have permission to request the account or the account is not valid for the system.
    - 4033 – Approver Only API or account. Only Approvers can access this API or account.
    - 4035 - Not enough approvers configured to approve a request.
- 409 – Conflicting request exists. This user or another user has already requested a password for the specified account within the next <durationMinutes> window.

For more information, please see "Common Response Codes" on page 17.

PUT Requests/{id}/Checkin

Alternate URI (deprecated)

```
PUT Requests/Release/{id}
```

Purpose

Checks-in/releases a request before it has expired.

Required Roles

Requestor role to managed account referenced by the request.

URL Parameters

id: ID of the request to check-in/release.

Request Body

Content-Type: application/json

```
{
    Reason : string
}
```

Request Body Details

Reason: (optional) A reason or comment why the request is being released. Max string length is 1000.

Response Body

None.

Response Codes

- 204 – Request successful. No content in body.
- 403 – User does not have permissions to release the indicated request or the associated account does not have API access enabled. Message or status code in response body:
  - 4031 – User does not have permission to release a password.
  - 4034 – Request is not yet approved.

For more information, please see "Common Response Codes" on page 17.

PUT Requests/{id}/Approve

Purpose

Approves a pending request.

Required Roles

Approver or requestor/approver role to managed account referenced by the request.

URL Parameters

id: ID of the request to approve.

Request Body

Content-Type: application/json

```
{
    Reason : string
}
```

Request Body Details

Reason: (optional) A reason or comment why the request is being approved. Max string length is 1000.

Response Body

None.

Response Codes

- 204 – Request successful. No content in body.
- 403 – User does not have permissions to approve the indicated request or the associated account does not have API access enabled. Message or status code in response body:
    - 4033 – Approver only - User cannot approve his or her own request.
    - 4036 – Request has been approved already.

For more information, please see "Common Response Codes" on page 17.

PUT Requests/{id}/Deny

Purpose

Denies/cancels an active or pending request.

Required Roles

Approver or requestor/approver role to managed account referenced by the request.

URL Parameters

id: ID of the request to deny/cancel.

Request Body

Content-Type: application/json

```
{
    Reason : string
}
```

Request Body Details

Reason: (optional) A reason or comment why the request is being denied/cancelled. Max string length is 1000.

Response Body

None.

Response Codes

- 204 – Request successful. No content in body.
- 403 – User does not have permissions to deny the indicated request or the associated account does not have API access enabled. Message or status code in response body:
- 4033 – Approver only - User cannot deny his or her own request.

For more information, please see "Common Response Codes" on page 17.

PUT Requests/{id}/RotateOnCheckin

Purpose

Updates a request to rotate the credentials on check-in/expiry.

***Note:** If **POST Requests RotateOnCheckin=false**, this updates the request to **true**. If **POST Requests RotateOnCheckin=true**, the request is not modified.*

Requirements

- Current user must be the owner of the request.
- Request must not be cancelled or expired.

URL Parameters

id: ID of the request to update.

Request Body

None.

Response Body

None.

Response Codes

204 – Request successful. No content in body.

For more information, please see "Common Response Codes" on page 17.

Request Termination

Quick Navigation

POST ManagedAccounts/{managedAccountID}/Requests/Terminate

Purpose

Terminates all active requests by managed account ID.

Required Permissions

Password Safe API Global Quarantine (Read/Write).

URL Parameters

managedAccountID: ID of the managed account.

Request Body

Content-Type: application/json

```
{
    Reason : string
}
```

Request Body Details

Reason: (optional) A reason or comment why the requests are being terminated. Max string length is 1000.

Response Body

None.

Response Codes

204 – Termination successful. No content in body.

For more information, please see "Common Response Codes" on page 17.

POST ManagedSystems/{managedSystemID}/Requests/Terminate

Purpose

Terminates all active requests by managed system ID.

Required Permissions

Password Safe API Global Quarantine (Read/Write).

URL Parameters

managedSystemID: ID of the managed system.

Request Body

Content-Type: application/json

```
{
    Reason : string
}
```

Request Body Details

Reason: (optional) A reason or comment why the requests are being terminated. Max string length is 1000.

Response Body

None.

Response Codes

204 – Termination successful. No content in body.

For more information, please see "Common Response Codes" on page 17.

POST Users/{userID}/Requests/Terminate

Purpose

Terminates all active requests by requestor user ID.

Required Permissions

Password Safe API Global Quarantine (Read/Write).

URL Parameters

userID: ID of the requestor user.

Request Body

Content-Type: application/json

```
{
    Reason : string
}
```

Request Body Details

Reason: (optional) A reason or comment why the requests are being terminated. Max string length is 1000.

Response Body

None.

Response Codes

204 – Termination successful. No content in body.

For more information, please see "Common Response Codes" on page 17.

Request Sets

Request sets are a grouping of requests to the same system and account with different access types (i.e. View and RDP). Requests in a request set are also accessible individually via GET requests.

Quick Navigation

GET RequestSets

Purpose

Lists request sets for the current user.

Query Parameters

status: (optional, default: all) Status of request sets to return (all, active, pending).

Request Body

None.

Response Body

Content-Type: application/json

```
[
    {
        RequestSetID: string,
        Requests:
        [
            {
                RequestID: int,
                RequestorName: string,
                SystemID: int,
                SystemName: string,
                AccountID: int,
                AccountName: string,
                DomainName: string,
                ApplicationID: int, // can be null,
                AliasID: int, // can be null
                RequestReleaseDate: date-formatted string,
                ApprovedDate: date-formatted string,
                CanceledDate: date-formatted string,
```

```
                ExpiresDate: date-formatted string,
                Status: string,
                AccessType: string,
                ApplicationID: int,
                Reason: string
            },
            …
        ]
    },
    …
]
```

Response Codes

- 200 – Request successful. Requests in the response body.
- 403 – Access forbidden. Response body contains a message or status code indicating the reason for this forbidden access:
    - 4033 – Approver Only API or account. Only Approvers can access this API or account.

For more information, please see "Common Response Codes" on page 17.

POST RequestSets

Purpose

Creates a new release request set.

Required Roles

- Requestor or Requestor/Approver role to managed account referenced by ID.
- Information Systems Administrator (ISA) role access.

For more information, please see:
- *"ISA Requests" on page 210*
- *"ISA Sessions" on page 212*

Request Body

Content-Type: application/json

```
{
    AccessTypes: [ string, … ],
```

```
    SystemID: int,
    AccountID: int,
    ApplicationID: int, // can be null,
    DurationMinutes : int,
    Reason : string,
    TicketSystemID : int,
    TicketNumber : string
}
```

Request Body Details

- **AccessTypes:** (at least two are required) A list of the types of access requested (View, RDP, SSH, App).
- **SystemID:** (required) ID of the managed system to request.
- **AccountID:** (required) ID of the managed account to request.
- **ApplicationID:** (required when an **AccessType** is App) ID of the application to request.
- **DurationMinutes:** (required) The request duration (in minutes).
- **Reason:** (optional) The reason for the request.
- **TicketSystemID:** ID of the ticket system. If omitted then default ticket system is used.
- **TicketNumber:** Number of associated ticket. Can be required if ticket system is marked as required in the access policy used. Max string length is 20.

Response Body

Content-Type: application/json

```
{
    RequestSetID: string,
    Requests:
    [
        {
            RequestID: int,
            SystemID: int,
            SystemName: string,
            AccountID: int,
            AccountName: string,
            DomainName: string,
            ApplicationID: int, // can be null
            AliasID: int,
            RequestReleaseDate: date-formatted string,
            ApprovedDate: date-formatted string,
            ExpiresDate: date-formatted string,
            Status: string,
            AccessType: string
        },
        …
    ]
}
```

Response Codes

- 201 – Request successful. Request set in the response body.
- 403 – User does not have permissions to perform a request for the indicated account or the account does not have API access enabled. Response body contains a status code indicating the reason for this forbidden access:
    - 4031 – User does not have permission to request the account or the account is not valid for the system.
    - 4033 – Approver Only API or account. Only Approvers can access this API or account.
    - 4035 - Not enough approvers configured to approve a request.
- 409 – Conflicting request exists. Another user has already requested a password for the specified account within the next <durationMinutes> window.

For more information, please see "Common Response Codes" on page 17.

Roles

(i.e. requestor, approver, credentials manager, etc.)

GET Roles

Purpose

Returns a list of Password Safe roles.

Required Permissions

Password Safe Role Management (Read).

Request Body

None.

Response Body

Content-Type: application/json

```
[
    {
        RoleID : int,
        Name : string
    },
    …
]
```

Response Codes

200 – Request successful. Roles in the response body.

For more information, please see "Common Response Codes" on page 17.

User Group Roles

Quick Navigation

GET UserGroups/{userGroupId}/SmartRules/{smartRuleId}/Roles

Purpose

Returns a list of roles for the user group and Smart Rule referenced by ID.

Required Permissions

- User Accounts Management (Read)
- Password Safe Role Management (Read).

URL Parameters

- **userGroupId:** ID of the user group.
- **smartRuleId:** ID of the Smart Rule.

Request Body

None.

Response Body

Content-Type: application/json

```
[
    {
        RoleID : int,
        Name : string
    },
    …
]
```

Response Codes

200 – Request successful. Roles in the response body.

For more information, please see "Common Response Codes" on page 17.

POST UserGroups/{userGroupId}/SmartRules/{smartRuleId}/Roles

Purpose

Sets Password Safe roles for the user group and Smart Rule referenced by ID.

Required Permissions

- User Accounts Management (Read/Write).
- Password Safe Role Management (Read/Write).

URL Parameters

- **userGroupId:** ID of the user group.
- **smartRuleId:** ID of the Smart Rule.

Request Body

Content-Type: application/json

```
{
    Roles :
    [
        {
            RoleID : int
        },
        …
    ],
    AccessPolicyID : int
}
```

Request Body Details

- **Roles:** (required) Zero or more roles to set on the UserGroup-SmartRule.
- **AccessPolicyID:** The access policy ID to set on the UserGroup-SmartRule. Required when the Requestor or Requestor/Approver role is set.

Response Body

None.

Response Codes

204 – Request successful. No content in body.

For more information, please see "Common Response Codes" on page 17.

DELETE UserGroups/{userGroupId}/SmartRules/{smartRuleId}/Roles

Purpose

Deletes all Password Safe roles for the user group and Smart Rule referenced by ID.

Required Permissions

- User Accounts Management (Read/Write).
- Password SafeRole Management (Read/Write).

URL Parameters

- **userGroupId:** ID of the user group.
- **smartRuleId:** ID of the Smart Rule.

Request Body

None.

Response Body

None.

Response Codes

200 – Request successful.

For more information, please see "Common Response Codes" on page 17.

Sessions

Quick Navigation

GET Sessions

Purpose

Returns a list of sessions.

> ***Note:*** *The maximum number of sessions returned is 100,000.*

Required Permissions

A member of the Administrators group, or ISA or auditor role to at least one asset Smart Rule.

Query Parameters (Optional)

- **status:** Session status - A single value or comma-delimited list of values:
  - **0:** Not Started
  - **1:** In Progress
  - **2:** Completed
  - **5:** Locked
  - **7:** Terminated (deprecated)
  - **8:** Logged Off
  - **9:** Disconnected (RDP only)
- **userID:** ID of the user that requested the session

Request Body

None.

Response Body

Content-Type: application/json

```
[
    {
        SessionID : int,
        UserID : int,
        NodeID : string,
        Status : int,
        ArchiveStatus : int,
        Protocol : int,
        StartTime : date,
        EndTime : date,
        Duration : int,
        AssetName : string,
        ManagedSystemID : int, // can be null
        ManagedAccountID : int,
        ManagedAccountName : string,
        RecordKey : string,
        Token : string
    },
    …
]
```

Response Codes

200 – Request successful. Sessions in the response body.

For more information, please see "Common Response Codes" on page 17.

GET Sessions/{id}

Purpose

Returns a session by ID.

Required Permissions

A member of the Administrators group, or ISA or auditor role to at least one asset Smart Rule.

URL Parameters

id: ID of the session.

Request Body

None.

Response Body

Content-Type: application/json

```
{
    SessionID : int,
    UserID : int,
    NodeID : string,
    Status : int,
    ArchiveStatus : int,
    Protocol : int,
    StartTime : date,
    EndTime : date,
    Duration : int,
    AssetName : string,
    ManagedSystemID : int,
    ManagedAccountID : int,
    ManagedAccountName : string,
    RecordKey : string,
    Token : string
}
```

Response Codes

200 – Request successful. Sessions in the response body.

For more information, please see "Common Response Codes" on page 17.

POST Requests/{requestID}/Sessions

Purpose

Create a new session for the given release.

Requirements

Must be the owner of the request ID.

URL Parameters

requestID: ID of the request for which to create a session.

Request Body

Content- Type: application/json

```
{
    SessionType : string,
    NodeID : string
}
```

Request Body Details

- **SessionType:** (required) The type of session to create (SSH or sshticket, RDP or rdpticket, rdpfile, app, or appfile).
- **NodeID:** (optional) ID of the node that should be used to establish the session. If **NodeID** is not given or if the Remote Session Proxy feature is disabled, uses the local node.

Response Body (SSH or sshticket)

Content-Type: application/json

```
{
    ID : string,
    Ticket : string,
    Host : string,
    Port : string,
    TicketAtHost : string,
    Link : string,
    Command : string,
    SessionID : int,
    NodeID : string
}
```

Response Body (RDP or rdpticket)

Content-Type: application/json

```
{
    ID : string,
    Ticket : string,
    Host : string,
    Port : string,
    SessionID : int,
    NodeID : string
}
```

Response Body (rdpfile)

RDP File as an attachment.

Response Body (app – when the target system is Unix- or ssh-based)

Content-Type: application/json

```
{
    ID : string,
    Ticket : string,
    Host : string,
    Port : string,
    TicketAtHost : string,
    Link : string,
    Command : string,
    SessionID : int,
    NodeID : string
}
```

Response Body (app – when the target system is Windows- or rdp-based)

Content-Type: application/json

```
{
    ID : string,
    Ticket : string,
    Host : string,
    Port : string,
    SessionID : int,
    NodeID : string
}
```

Response Body (appfile)

RDP File as an attachment.

Response Codes

- 201– Request successful. Session details or RDP file in the response body.
- 403 – Access forbidden. Response body contains a message or status code indicating the reason for this forbidden access:
- 4034 – Request is not yet approved.

For more information, please see "Common Response Codes" on page 17.

POST Sessions/Admin

Purpose

Create a new admin session.

Required Roles

Password Safe Admin Session (Read/Write).

Request Body

Content-Type: application/json

```
{
    SessionType : string,
    HostName : string,
    Port : int, // can be null
    DomainName : string,
    UserName : string,
    Password : string,
    Reason : string,
    Resolution : string,
    RDPAdminSwitch : bool,
    SmartSizing : bool,
    NodeID : string,
    Record : bool
}
```

Request Body Details

- **SessionType:** (required) The type of session to create (**SSH** or **sshticket**, **RDP** or **rdpticket**, or **rdpfile**)
- **HostName:** (required) Name or IP of the target host. Max string length is 128.
- **Port:** (optional, default: <configured default port>) Port to use for the connection.
- **DomainName:** (optional) The domain name of the user. Max string length is 50.
- **UserName:** (required) The username. Max string length is 200.
- **Password:** (required) The password.
- **Reason:** (optional) The reason for the session.
- **Resolution (RDP-only):** (optional, default: <configured default resolution>) The default resolution (i.e **1024x768** or **Maximized**). Max string length is 50.
- **RDPAdminSwitch (RDP-only):** (optional, default: false) True to use the RDP **/admin** switch, otherwise false.
- **SmartSizing (RDP-only):** (optional, default: false) True to use RDP **Smart Sizing**, otherwise false. Applies only when **SessionType=rdpfile**.
- **NodeID:** (optional) ID of the node that should be used to establish the Session. If **NodeID** is not given or if the Remote Session Proxy feature is disabled, uses the local node.

Response Body (SSH or sshticket)

Content-Type: application/json

```
{
    ID : string,
    Ticket : string,
    Host : string,
    Port : string,
    TicketAtHost : string,
    Link : string,
    Command : string,
    SessionID : int,
    NodeID : string
}
```

Response Body (RDP or rdpticket)

Content-Type: application/json

```
{
    ID : string,
    Ticket : string,
    Host : string,
    Port : string,
    SessionID : int,
    NodeID : string
}
```

Response Body (rdpfile)

RDP file as an attachment.

Response Codes

201 – Request successful. Session details or RDP file in the response body.

403 – Access forbidden. Response body contains a message or status code indicating the reason for this forbidden access.

For more information, please see "Common Response Codes" on page 17.

Session Locking

Quick Navigation

POST Sessions/{sessionID}/Lock

Purpose

Locks an active session.

Required Permissions

One of:

- Password Safe API Global Quarantine (Read/Write)
- Password Safe Active Session Reviewer Role, ISA Role, or a member of BeyondInsight Administrators group.

URL Parameters

sessionID: ID of the session.

Request Body

None.

Response Body

None.

Response Codes

204 – Lock successful. No content in body.

For more information, please see "Common Response Codes" on page 17.

POST ManagedAccounts/{managedAccountID}/Sessions/Lock

Purpose

Locks all active sessions by managed account ID.

Required Permissions

Password Safe API Global Quarantine (Read/Write).

URL Parameters

managedAccountID: ID of the managed account.

Request Body

None.

Response Body

None.

Response Codes

204 – Lock successful. No content in body.

For more information, please see "Common Response Codes" on page 17.

POST ManagedSystems/{managedSystemID}/Sessions/Lock

Purpose

Locks all active Sessions by managed system ID.

Required Permissions

Password Safe API Global Quarantine (Read/Write).

URL Parameters

managedSystemID: ID of the managed system.

Request Body

None.

Response Body

None.

Response Codes

204 – Lock successful. No content in body.

For more information, please see "Common Response Codes" on page 17.

Session Termination

Quick Navigation

POST Sessions/{sessionID}/Terminate

Purpose

Terminates an active session.

Required Permissions

One of:

- Password Safe API Global Quarantine (Read/Write)
- Password Safe Active Session Reviewer Role, ISA Role, or a member of BeyondInsight Administrators group.

URL Parameters

sessionID: ID of the session to terminate.

Request Body

None.

Response Body

None.

Response Codes

204 – Termination successful. No content in body.

For more information, please see "Common Response Codes" on page 17.

POST ManagedAccounts/{managedAccountID}/Sessions/Terminate

Purpose

Terminates all active sessions by managed account ID.

Required Permissions

Password Safe API Global Quarantine (Read/Write).

URL Parameters

managedAccountID: ID of the managed account.

Request Body

None.

Response Body

None.

Response Codes

204 – Termination successful. No content in body.

For more information, please see "Common Response Codes" on page 17.

POST ManagedSystems/{managedSystemID}/Sessions/Terminate

Purpose

Terminates all active sessions by managed system ID.

Required Permissions

Password Safe API Global Quarantine (Read/Write).

URL Parameters

managedSystemID: ID of the managed system.

Request Body

None.

Response Body

None.

Response Codes

- 204 – Termination successful. No content in body.

For more information, please see "Common Response Codes" on page 17.

Synced Accounts

Synced accounts are managed accounts subscribed/synced to another managed account.

Quick Navigation

GET ManagedAccounts/{id}/SyncedAccounts

Purpose

Returns a list of subscribed/synced managed accounts by managed account ID.

Required Permissions

Password Safe Account Management (Read).

URL Parameters

id: ID of the parent managed account.

Request Body

None.

Response Body

Content-Type: application/json

```
[
    {
        ManagedAccountID : int,
        ManagedSystemID : int,
        DomainName : string,
        AccountName : string,
        DistinguishedName : string,
        PasswordFallbackFlag : bool,
        LoginAccountFlag : bool,
        Description : string,
        PasswordRuleID : int,
```

```
        ApiEnabled : bool,
        ReleaseNotificationEmail : string,
        ChangeServicesFlag : bool,
        RestartServicesFlag : bool,
        ReleaseDuration : int,
        MaxReleaseDuration : int,
        ISAReleaseDuration : int,
        MaxConcurrentRequests : int,

        AutoManagementFlag : bool,
        DSSAutoManagementFlag : bool,
        CheckPasswordFlag : bool,
        ResetPasswordOnMismatchFlag : bool,
        ChangePasswordAfterAnyReleaseFlag : bool,
        ChangeFrequencyType : string,
        ChangeFrequencyDays : int,
        ChangeTime : string,

        ParentAccountID : int, // can be null
        IsSubscribedAccount : bool,
        LastChangeDate : datetime, // can be null
        NextChangeDate : datetime, // can be null
        IsChanging : bool,
        ChangeState : int,
        UseOwnCredentials : bool,
        ChangeIISAppPoolFlag : bool,
        RestartIISAppPoolFlag : bool,
        WorkgroupID : int, // can be null

        ChangeWindowsAutoLogonFlag : bool,
        ChangeComPlusFlag : bool,
        ChangeDComFlag : bool,
        ChangeSComFlag : bool,
    },
    …
]
```

Response Body Details

- **DomainName:** The domain name for a domain-type account.
- **AccountName:** The name of the account.
- **DistinguishedName:** The distinguished name of an LDAP managed account.
- **PasswordFallbackFlag:** True if failed DSS authentication can fall back to password authentication, otherwise false.
- **LoginAccountFlag:** True if the account should use the managed system login account for SSH sessions, otherwise false.
- **Description:** A description of the account.
- **PasswordRuleID:** ID of the password rule assigned to this managed account.
- **ApiEnabled:** True if the account can be requested through the API, otherwise false.
- **ReleaseNotificationEmail:** Email address used for notification emails related to this managed account.
- **ChangeServicesFlag:** True if services run as this user should be updated with the new password after a password change, otherwise false.

- **RestartServicesFlag:** True if services should be restarted after the run as password is changed (**ChangeServicesFlag**), otherwise false.
- **ReleaseDuration:** (minutes: 1-525600) Default release duration.
- **MaxReleaseDuration:** (minutes: 1-525600) Default maximum release duration.
- **ISAReleaseDuration:** (minutes: 1-525600) Default Information Systems Administrator (ISA) release duration.
- **MaxConcurrentRequests:** (0-999, 0 is unlimited) Maximum number of concurrent password requests for this account.
- **AutoManagementFlag:** True if password auto-management is enabled, otherwise false.
    - **DSSAutoManagementFlag:** True if DSS key auto-management is enabled, otherwise false.
    - **CheckPasswordFlag:** True to enable password testing, otherwise false.
    - **ChangePasswordAfterAnyReleaseFlag:** True to change passwords on release of a request, otherwise false.
    - **ResetPasswordOnMismatchFlag:** True to queue a password change when scheduled password test fails, otherwise false.
    - **ChangeFrequencyType:** The change frequency for scheduled password changes:
        - **first:** Changes scheduled for the first day of the month.
        - **last:** Changes scheduled for the last day of the month.
        - **xdays:** Changes scheduled every x days (**ChangeFrequencyDays**).
    - **ChangeFrequencyDays:** (days: 1-999) When **ChangeFrequencyType** is **xdays**, password changes take place this configured number of days.
    - **ChangeTime:** (24hr format: 00:00-23:59) UTC time of day scheduled password changes take place.
- **ParentAccountID:** If this is a subscribed account (**IsSubscribedAccount**), this is the ID of the parent managed account.
- **IsSubscribedAccount:** True if the account is a synced or subscribed account, otherwise false.
- **LastChangeDate:** The date and time of the last password change.
- **NextChangeDate:** The date and time of the next scheduled password change.
- **IsChanging:** True if the account credentials are in the process of changing, otherwise false.
- **ChangeState:** The change state of the account credentials:
    - **0:** Idle / no change taking place or scheduled within 5 minutes.
    - **1:** Changing / managed account credential currently changing.
    - **2:** Queued / managed account credential is queued to change or scheduled to change within 5 minutes.

For more information, please see Configure Subscriber Accounts at https://www.beyondtrust.com/docs/beyondinsight-password-safe/ps/admin/managed-accounts.htm#ConfigureAccounts.

Response Codes

200 – Request successful. Linked Managed Account in the response body.

For more information, please see "Common Response Codes" on page 17.

POST ManagedAccounts/{id}/SyncedAccounts/{syncedAccountID}

Purpose

Subscribes/syncs a managed account to the managed account referenced by ID.

Required Permissions

Password Safe Account Management (Read/Write).

URL Parameters

- **id:** ID of the parent managed account.
- **syncedAccountID:** ID of the synced managed account.

Request Body

None.

Response Body

Content-type: application/json

```
{
    ManagedAccountID : int,
    ManagedSystemID : int,
    DomainName : string,
    AccountName : string,
    DistinguishedName : string,
    PasswordFallbackFlag : bool,
    LoginAccountFlag : bool,
    Description : string,
    PasswordRuleID : int,
    ApiEnabled : bool,
    ReleaseNotificationEmail : string,
    ChangeServicesFlag : bool,
    RestartServicesFlag : bool,
    ReleaseDuration : int,
    MaxReleaseDuration : int,
    ISAReleaseDuration : int,
    MaxConcurrentRequests : int,

    AutoManagementFlag : bool,
    DSSAutoManagementFlag : bool,
    CheckPasswordFlag : bool,
    ResetPasswordOnMismatchFlag : bool,
    ChangePasswordAfterAnyReleaseFlag : bool,
    ChangeFrequencyType : string,
```

```
    ChangeFrequencyDays : int,
    ChangeTime : string,

    ParentAccountID : int, // can be null
    IsSubscribedAccount : bool,
    LastChangeDate : datetime, // can be null
    NextChangeDate : datetime, // can be null
    IsChanging : bool,
    ChangeState : int,
    UseOwnCredentials : bool,
    ChangeIISAppPoolFlag : bool,
    RestartIISAppPoolFlag : bool,
    WorkgroupID : int, // can be null

    ChangeWindowsAutoLogonFlag : bool,
    ChangeComPlusFlag : bool,
    ChangeDComFlag : bool,
    ChangeSComFlag : bool,
}
```

Response Body Details

- **AccountName:** The name of the account.
- **PasswordFallbackFlag:** True if failed DSS authentication can fall back to password authentication, otherwise false.
- **LoginAccountFlag:** True if the account should use the managed system login account for SSH sessions, otherwise false.
- **Description:** A description of the account.
- **PasswordRuleID:** ID of the password rule assigned to this managed account.
- **ApiEnabled:**True if the account can be requested through the API, otherwise false.
- **ReleaseNotificationEmail:** Email address used for notification emails related to this managed account.
- **ChangeServicesFlag:** True if services run as this user should be updated with the new password after a password change, otherwise false.
- **RestartServicesFlag:** True if services should be restarted after the run as password is changed (**ChangeServicesFlag**), otherwise false.
- **ReleaseDuration:** (minutes: 1-525600) Default release duration.
- **MaxReleaseDuration:** (minutes: 1-525600) Default maximum release duration.
- **ISAReleaseDuration:** (minutes: 1-525600) Default Information Systems Administrator (ISA) release duration.
- **MaxConcurrentRequests:** (0-999, 0 means unlimited) Maximum number of concurrent password requests for this account.
- **AutoManagementFlag:** True if password auto-management is enabled, otherwise false.
    - **DSSAutoManagementFlag:** True if DSS key auto-management is enabled, otherwise false.
    - **CheckPasswordFlag:** True to enable password testing, otherwise false.
    - **ChangePasswordAfterAnyReleaseFlag:** True to change passwords on release of a request, otherwise false.
    - **ResetPasswordOnMismatchFlag:** True to queue a password change when scheduled password test fails, otherwise false.

  - **ChangeFrequencyType:** The change frequency for scheduled password changes:
    - **first:** Changes scheduled for the first day of the month.
    - **last:** Changes scheduled for the last day of the month.
    - **xdays:** Changes scheduled every x days (**ChangeFrequencyDays**).
  - **ChangeFrequencyDays:** (days: 1-999) When **ChangeFrequencyType** is **xdays**, password changes take place this configured number of days.
  - **ChangeTime:** (24hr format: 00:00-23:59) UTC time of day scheduled password changes take place.
- **ParentAccountID:** If this is a subscribed account (**IsSubscribedAccount**), this is the ID of the parent managed account.
- **IsSubscribedAccount:** True if the account is a synced or subscribed account, otherwise false.
- **LastChangeDate:** The date and time of the last password change.
- **NextChangeDate:** The date and time of the next scheduled password change.
- **IsChanging:** True if the account credentials are in the process of changing, otherwise false.
- **ChangeState:** The change state of the account credentials:
  - **0:** Idle / no change taking place or scheduled within 5 minutes.
  - **1:** Changing / managed account credential currently changing.
  - **2:** Queued / managed account credential is queued to change or scheduled to change within 5 minutes.

For more information, please see Configure Subscriber Accounts at https://www.beyondtrust.com/docs/beyondinsight-password-safe/ps/admin/managed-accounts.htm#ConfigureAccounts.

Response Codes

- 200 – Account was already synced. Managed Account in the response body.
- 201 – Account was synced successfully. Managed Account in the response body.

For more information, please see "Common Response Codes" on page 17.

DELETE ManagedAccounts/{id}/SyncedAccounts

Purpose

Unsubscribes/unsyncs all managed accounts from the parent managed account by ID.

Required Permissions

Password Safe Account Management (Read/Write).

URL Parameters

id: ID of the parent managed account.

Request Body

None.

Response Body

None.

Response Codes

200 – Request successful.

For more information, please see "Common Response Codes" on page 17.

DELETE ManagedAccounts/{id}/SyncedAccounts/{syncedAccountID}

Purpose

Unsubscribes/unsyncs a managed account from the managed account by ID.

Required Permissions

Password Safe Account Management (Read/Write).

URL Parameters

- **id:** ID of the parent managed account.
- **syncedAccountID:** ID of the synced managed account.

Request Body

None.

Response Body

None.

Response Codes

200 – Request successful.

For more information, please see "Common Response Codes" on page 17.

Deprecated

The content in this section of the guide has been deprecated and is compatible with earlier versions only.

Quick Navigation

Aliases

[deprecated] GET Aliases/{name}

> ***Note:*** *This API has been deprecated and is available for backwards compatibility only. Use* ***GET Aliases?name={name}*** *instead.*

Purpose

Returns a requestable managed account alias by name.

Required Roles

Requestor or Requestor/Approver role for the preferred managed account referenced by the alias.

URL Parameters

name: Name of the managed account alias.

Request Body

None.

Response Body

Content-Type: application/json

```
{
    AliasId: int,
    AliasName: string,
```

```
    SystemId: int,
    SystemName: string,
    AccountId: int,
    AccountName: string,
    DomainName: string,
    InstanceName: string,
    DefaultReleaseDuration: int,
    MaximumReleaseDuration: int,
    LastChangeDate: datetime,
    NextChangeDate: datetime,
    IsChanging: bool,
    ChangeState: int,

    MappedAccounts :
    [
        {
            AliasID: int,
            ManagedSystemID: int,
            ManagedAccountID: int,
            Status: string
        },
        …
    ]
}
```

Response Codes

200 - Request successful. Alias in response body.

For more information, please see "Common Response Codes" on page 17.

Keystrokes

[deprecated] GET Keystrokes/search/{condition}

***Note:** This API has been deprecated and is available for backwards compatibility only. Use **POST Keystrokes/Search** instead.*

Purpose

Search for keystrokes by condition/keyword.

Required Roles

Password Safe Auditor Role, ISA Role, or a member of BeyondInsight Administrators group.

URL Parameters

condition: Keyword to search for.

Response Body

Content-Type: application/json

```
[
    {
        KeystrokeID: long,
        SessionID: int,
        TimeMarker: long,
        Type: byte,
        Data: string
    },
    …
]
```

Response Codes

200 - Request successful. Keystrokes are in response body.

For more information, please see "Common Response Codes" on page 17.

[deprecated] GET Keystrokes/search/{condition}/{type:int}

Note: *This API has been deprecated and is available for backwards compatibility only. Use POST Keystrokes/Search instead.*

Purpose

Search for keystrokes by condition/keyword and type.

Required Roles

Password Safe Auditor Role, ISA Role, or a member of BeyondInsight Administrators group.

URL Parameters

- **condition:** Keyword to search for.
- **type:** Type of keystrokes:
    - **0:** All
    - **1:** StdIn
    - **2:** StdOut

- **4:** Window Event
- **5:** User Event

Response Body

Content-Type: application/json

```
[
    {
        KeystrokeID: long,
        SessionID: int,
        TimeMarker: long,
        Type: byte,
        Data: string
    },
    …
]
```

Response Codes

200 - Request successful. Keystrokes are in response body.

For more information, please see "Common Response Codes" on page 17.

Managed Account Credentials

PUT Workgroups/{workgroupName}/Assets/{assetName}/ManagedSystems/ManagedAccounts/{accountName}/Credentials

***Note:** This API has been deprecated and is available for backwards compatibility only. Use **PUT Credentials?workgroupName={workgroupName}&assetName={assetName}&accountName={accountName}** instead.*

Purpose

Updates the credentials for a managed account by Workgroup name, asset name, and managed account name, optionally applying the change to the managed system.

Required Permissions

One of the following is required:

- Password Safe Account Management (Read/Write)
- ISA Role or Credentials Manager Role on a Smart Rule referencing the account

URL Parameters

- **workgroupName:** Name of the Workgroup.
- **assetName:** Name of the asset.
- **accountName:** Name of the managed account for which to set the credentials.

Request Body

Content-Type: application/json

```
{
    Password: string,
    PublicKey: string,
    PrivateKey: string,
    Passphrase: string,
    UpdateSystem: bool
}
```

Request Body Details

- **Password:** (optional) The new password to set. If not given, generates a new random password.
- **PublicKey:** (required if PrivateKey is given and updateSystem=true) The new public key to set on the host.
- **PrivateKey:** The private key to set (provide passphrase if encrypted).
- **Passphrase:** (optional) The passphrase to use for an encrypted private key.
- **UpdateSystem:** (default: true) Whether to update the credentials on the referenced system.

Response Body

None.

Response Codes

204 - Request Successful. No Response Body.

For more information, please see "Common Response Codes" on page 17.

Ticket Systems

GET TicketSystems

Purpose

List registered ticket systems.

Required Permissions

Ticket System (Read).

Request Body

None.

Response Body

Content-Type: application/json

```
[
    {
        TicketSystemID : int,
        IsActive : bool,
        TicketSystemName : string,
        Description : string,
        IsDefaultSystem : bool
    },
    …
]
```

Response Codes

200 – Request successful. Ticket systems in the response body

For more information, please see "Common Response Codes" on page 17.

Secrets Safe APIs

Note: *TeamPasswords API endpoints are deprecated in v22.4 of this guide, and replaced with SecretsSafe v22.4. TeamPasswords API endpoints remain usable, but will be removed in time.*

Folders

Quick Navigation

POST Secrets-Safe/Folders/

Purpose

Creates a new Secrets Safe folder for the given user group.

Required Permissions

Secrets-Safe (Read/Write).

Request Body

Content-Type: application/json

```
{
    Name: string,
    Description: string,
    ParentId: Guid,
    UserGroupId: int,
}
```

Request Body Details

Max string length for description is 256.

Response Body

Content-Type: application/json

```
{
    Id: Guid,
```

```
    Name: string,
    Description: string,
    ParentId: Guid,
    UserGroupId: int,
}
```

Response Codes

- 201 - Request successful. Secrets Safe Folder in the response body.
- 409 - Conflict.

For more information, please see "Common Response Codes" on page 17.

POST Secrets-Safe/Folders/{id}

Purpose

Imports a CSV secrets file into the specified folder.

Required Permissions

- Workforce Passwords Read/Write, when destination folder is a Personal Folder.
- Workforce Passwords Read/Write and Secrets Safe ReadWrite, when destination folder is a team folder.

Parameters

folderid: the folder ID (GUID).

Request Body

Content-Type: multipart/form-data

Response Body

```
{
    totalNumber: int,
    errors: [ {
      lineNumber: int,
      error: string
     }
    ],
```

```
  successfulImport: int
}
```

- **TotalNumber**: Number of credentials processed. Includes failures.
- **Errors**: List of errors. Includes the error message and CSV line number
- **SuccessfulImport**: Number of credentials successfully imported.

Response Codes

201 – Request partially or completely successful. Refer to **errors** and **successfulImport** values in response body.

For more information, please see "Common Response Codes" on page 17.

GET Secrets-Safe/Folders/

Purpose

Returns a list of Secrets Safe folders to which the current user has access.

Required Permissions

Secrets-Safe (Read).

Parameters

To filter the results, use any combination of the following:

- **FolderName**: The partial name of the folder.
- **FolderPath**: Child folders are also included. Separator is /.
- **IncludeSubfolders**: Indicate whether to include the subfolder. Default is **true**.
- **RootOnly**: The results only include those folders at the root level.
- **FolderOwnerId**: Filter results by the folders which are owned by the given **FolderOwnerId**.
- **Limit**: Limits the results by the given integer greater than 0. Default is **1000**.
- **Offset**: Skip the first (offset) number of secrets.

Request Body

None.

Response Body

Content-Type: application/json

```
[{
    Id: Guid,
    Name: string,
    Description: string,
    ParentId: Guid,
    UserGroupId: int,
},
…
]
```

Response Codes

200 - Request successful. Secrets Safe Folders in the response body.

For more information, please see "Common Response Codes" on page 17.

PUT Secrets-Safe/Folders/{id}

Purpose

Updates a Secrets Safe folder by ID.

Required Permissions

Secrets-Safe (Read/Write).

Parameters

id: the folder ID (GUID).

Request Body

Content-Type: application/json

```
{
    Name: string,
    Description: string,
    ParentId: Guid,
    UserGroupId: int,
}
```

Request Body Details

Max string length for description is 256.

Response Body

Content-Type: application/json

```
[{
    Id: Guid,
    Name: string,
    Description: string,
    ParentId: Guid,
    UserGroupId: int,
},
…
]
```

Response Codes

200 - Request successful. Secrets Safe Folders in the response body.

For more information, please see "Common Response Codes" on page 17.

DELETE Secrets-Safe/Folders/{id}

Purpose

Deletes a Secrets Safe folder by ID.

Required Permissions

Secrets-Safe (Read/Write).

***Note:** Folders that contain secrets **cannot** be deleted.*

Parameters

id: the folder ID (GUID).

Request Body

None.

Response Body

None.

Response Codes

200 - Request successful. Secrets Safe folders in the response body.

For more information, please see "Common Response Codes" on page 17.

GET Secrets-Safe/Folders/{id}

Purpose

Returns a Secrets Safe folder by ID.

Required Permissions

Secrets-Safe (Read).

Parameters

id: the folder ID (GUID).

Request Body

None.

Response Body

Content-Type: application/json

```
{
    Id: Guid,
    Name: string,
    Description: string,
    ParentId: Guid,
    UserGroupId: int,
}
```

Response Codes

200 - Request successful. Secrets Safe Folder in the response body.

For more information, please see "Common Response Codes" on page 17.

Secrets

Quick Navigation

POST Secrets-Safe/Folders/{folderId:guid}/secrets

Purpose

Creates a secret in the folder by ID.

Required Permissions

Secrets-Safe (Read/Write).

Parameters

folderid: the folder ID (GUID).

Request Body

Content-Type: application/json

```
{
            Title : string,
            Description : string,
            Username : string,
            Password : string,
```

```
            OwnerId : int,
            OwnerType : string,
            Owners : [{
            OwnerId : int,
            Owner : string,
            Email : string,
            }],
            PasswordRuleID : int,
            Notes : string,
          Urls : [{
          Id : Guid,
          CredentialId : Guid,
          Url : String
          }]
        }
```

Request Body Details

- Max string length for description and password is 256.
- Max string length for notes is 4000.
- Max string length for Url is 2048.
- Required: Title, username, password.
- When OwnerType is set to User, then a list of Owners is required. When OwnerType is set to Group, the OwnerId is required (as the GroupId).
- A password or a PasswordRuleID is required.
    - If a PasswordRuleID is passed in, then a password is generated (based on the Password Policy defined by the PasswordPolicyID).
    - If a password is passed in instead, the same behavior is followed (using that as the password).

Response Body

Content-Type: application/json

```
[
   {
         Id : Guid,
         Title : string,
         Description : string,
         Username : string,
         Password : string,
         OwnerId : int,
         FolderId : Guid,
         CreatedOn : Datetime,
         CreatedBy : string,
         ModifiedOn : Datetime,
         ModifiedBy : string,
         Owner : string,
         Folder : string,
```

```
        FolderPath : string,
        Owners : [{
        OwnerId : int,
        Owner : string,
        Email : string,
        }],
      OwnerType : string,
      Notes : string,
      Urls : [{
      Id : Guid,
      CredentialId : Guid,
      Url : String
      }]
     }
]
```

Response Codes

201 - Created

400 - Bad Request

403 - Forbidden

409 - Conflict

For more information, please see "Common Response Codes" on page 17.

POST Secrets-Safe/Folders/{folderId:guid}/secrets/text

Purpose

Creates a text secret in the given folder ID.

Required Permissions

Secrets-Safe (Read/Write).

Parameters

folderid: the folder ID (GUID).

Request Body

Content-Type: application/json

```
{
                  Title : string,
            Description : string,
            Text : string,
            OwnerId : int,
            OwnerType : string,
            Owners : [{
            OwnerId : int,
            Owner : string,
            Email : string,
            }],
            Notes : string,
            FolderId : Guid,
          Urls : [{
          Id : Guid,
          CredentialId : Guid,
          Url : String
          }]
        }
```

Request Body Details

- Max string length for Title and Description is 256.
- Max string length for text is 4096.
- Max string length for notes is 4000.
- Max string length for Url is 2048.
- Required: Title, FolderId
- When OwnerType is set to User, then a list of Owners is required. When OwnerType is set to Group, the OwnerId is required (as the GroupId).

Response Body

Content-Type: application/json

```
[
   {
         Id : Guid,
         Title : string,
         Description : string,
         OwnerId : int,
         FolderId : Guid,
         CreatedOn : Datetime,
         CreatedBy : string,
         ModifiedOn : Datetime,
         ModifiedBy : string,
         Owner : string,
         Folder : string,
         FolderPath : string,
         Owners : [{
         OwnerId : int,
```

```
        Owner : string,
        Email : string,
        }],
        OwnerType : string,
        Notes : string,
      Urls : [{
      Id : Guid,
      CredentialId : Guid,
      Url : String
      }]
      }
]
```

Response Codes

201 - Created

400 - Bad Request

403 - Forbidden

409 - Conflict.

For more information, please see "Common Response Codes" on page 17.

POST Secrets-Safe/Folders/{folderId:guid}/secrets/file

Purpose

Creates a secret file in the given folder ID.

Required Permissions

Secrets-Safe (Read/Write).

Parameters

folderid: the folder ID (GUID).

Request Body

Content-Type: multipart/form-data

```
{
            Title : string,
            Description : string,
```

```
            OwnerId : int,
            OwnerType : string,
            Owners : [{
            OwnerId : int,
            Owner : string,
            Email : string,
            }],
            Notes : string,
            FileName : string,
          Urls : [{
          Id : Guid,
          CredentialId : Guid,
          Url : String
          }]
        }
```

Request Body Details

- Max string length for Title, Description, and FileName is 256.
- Max string length for notes is 4000.
- Max string length for Url is 2048.
- Max file size is 5 MB. Size must be greater than 0 MB.
- Required: Title, FolderId, Filename
- When OwnerType is set to User, then a list of Owners is required. When OwnerType is set to Group, the OwnerId is required (as the GroupId).
- When adding the file, the form field name must be "*secretmetadata*". If the name of the form is anything else, the following error occurs: *The multipart Request is missing poarts: key:'form-data'=True, key:'secretmetadata'=False.*

Response Body

Content-Type: application/octet-stream

Content Part One - name: form-data, type: binary

Content Part Two - name: secretmetadata, type: string

```
[
   {
        Id : Guid,
        Title : string,
        Description : string,
        OwnerId : int,
        FolderId : Guid,
        CreatedOn : Datetime,
        CreatedBy : string,
        ModifiedOn : Datetime,
        ModifiedBy : string,
        Owner : string,
        Folder : string,
        FolderPath : string,
```

```
        Owners : [{
        OwnerId : int,
        Owner : string,
        Email : string,
        }],
        OwnerType : string,
        Notes : string,
        FileName : string,
        FileHash : string,
      Urls : [{
      Id : Guid,
      CredentialId : Guid,
      Url : String
      }]
    }
]
```

Response Codes

201 - Created

400 - Bad Request

403 - Forbidden

409 - Conflict

For more information, please see "Common Response Codes" on page 17.

PUT Secrets-Safe/Secrets/{secretId:guid}/

Purpose

Updates a secret based on the given ID.

Required Permissions

Secrets-Safe (Read/Write).

Parameters

SecretId: the secret id (GUID)

Request Body

Content-Type: application/json

```
{
            FolderId : Guid,
            Title : string,
            Description : string,
            Username : string,
            Password : string,
            OwnerId : int,
            OwnerType : string,
            Owners : [{
            OwnerId : int,
            Owner : string,
            Email : string,
            }],
            PasswordRuleId : int,
            Notes : string,
          Urls : [{
          Id : Guid,
          CredentialId : Guid,
          Url : String
          }]
        }
```

Request Body Details

- Max string length for description is 256.
- Max string length for notes is 4000.
- Max string length for Url is 2048.
- Required: Title, username, password, FolderID.
- When OwnerType is set to User, then a list of Owners is required. When OwnerType is set to Group, the OwnerId is required (as the GroupId).
- A password or a PasswordRuleID is required.
    - If a PasswordRuleID is passed in, then a password is generated (based on the Password Policy defined by the PasswordPolicyID).
    - If a password is passed in instead, the same behavior is followed (using that as the password).

Response Body

Content-Type: application/json

```
[
   {
        Id : Guid,
        Title : string,
        Description : string,
        OwnerId : int,
        FolderId : Guid,
        CreatedOn : Datetime,
        CreatedBy : string,
```

```
        ModifiedOn : Datetime,
        ModifiedBy : string,
        Owner : string,
        Folder : string,
        FolderPath : string,
        Owners : [{
        OwnerId : int,
        Owner : string,
        Email : string,
        }],
        OwnerType : string,
        Notes : string,
      Urls : [{
      Id : Guid,
      CredentialId : Guid,
      Url : String
      }]
    }
]
```

Response Codes

204 - No Content

403 - Forbidden

400 - Bad Request

For more information, please see "Common Response Codes" on page 17.

PUT Secrets-Safe/Secrets/{secretId:guid}/text

Purpose

Updates a secret text based on the given ID.

Required Permissions

Secrets-Safe (Read/Write).

Parameters

SecretId: the secret ID (GUID)

Request Body

Content-Type: application/json

```
{
            FolderId : Guid,
            Title : string,
            Description : string,
            OwnerId : int,
            OwnerType : string,
            Owners : [{
            OwnerId : int,
            Owner : string,
            Email : string,
            }],
            Notes : string,
          Urls : [{
          Id : Guid,
          CredentialId : Guid,
          Url : String
          }]
        }
```

Request Body Details

- Max string length for description and password is 256.
- Max string length for notes is 4000.
- Max string length for Url is 2048.
- Required: Title.
- When OwnerType is set to User, then a list of Owners is required. When OwnerType is set to Group, the OwnerId is required (as the GroupId).

Response Body

```
[
   {
         Id : Guid,
         Title : string,
         Description : string,
         OwnerId : int,
         FolderId : Guid,
         CreatedOn : Datetime,
         CreatedBy : string,
         ModifiedOn : Datetime,
         ModifiedBy : string,
         Owner : string,
         Folder : string,
         FolderPath : string,
         Owners : [{
         OwnerId : int,
         Owner : string,
         Email : string,
         }],
         OwnerType : string,
```

```
        Notes : string,
      Urls : [{
      Id : Guid,
      CredentialId : Guid,
      Url : String
      }]
       }
]
```

Response Codes

204 - No Content

400 - Bad Request

403 - Forbidden

For more information, please see "Common Response Codes" on page 17.

PUT Secrets-Safe/Secrets/{secretId:guid}/file

Purpose

Updates a file secret based on the folder ID.

Required Permissions

Secrets-Safe (Read/Write).

Parameters

SecretId: the secret ID (GUID).

Request Body

Content-Type: application/json

```
{
            FolderId : Guid,
            Title : string,
            Description : string,
            OwnerId : int,
            OwnerType : string,
            Owners : [{
            OwnerId : int,
            Owner : string,
```

```
            Email : string,
            }],
            Notes : string,
          Urls : [{
          Id : Guid,
          CredentialId : Guid,
          Url : String
          }]
        }
```

Request Body Details

- Max string length for Title, Description, and FileName is 256.
- Max string length for notes is 4000.
- Max string length for Url is 2048.
- Max file size is 5MB. Size must be greater than 0MB.
- Required: Title, FolderId.
- When OwnerType is set to User, then a list of Owners is required. When OwnerType is set to Group, the OwnerId is required (as the GroupId).

Response Body

```
[
   {
        Id : Guid,
        Title : string,
        Description : string,
        OwnerId : int,
        FolderId : Guid,
        CreatedOn : Datetime,
        CreatedBy : string,
        ModifiedOn : Datetime,
        ModifiedBy : string,
        Owner : string,
        Folder : string,
        FolderPath : string,
        Owners : [{
        OwnerId : int,
        Owner : string,
        Email : string,
        }],
        OwnerType : string,
        Notes : string,
        FileName : string,
        FileHash : string,
     Urls : [{
     Id : Guid,
     CredentialId : Guid,
     Url : String
```

```
        }]
    }
]
```

Response Codes

204 - No Content

400 - Bad Request

403 - Forbidden

For more information, please see "Common Response Codes" on page 17.

GET Secrets-Safe/Secrets

Purpose

Returns a list of secrets with the option to filter the list using query parameters.

Required Permissions

Secrets-Safe (Read).

Parameters

All parameters are optional:

- **Path**: the full path to the secret.
- **Separator**: the separator used in the path above. Default is /.
- **Title**: the full title of the secret.
- **AfterDate**: filter by modified or created on, after, or equal to the given date. Must be in the following UTC format: *yyyy-MM-ddTHH:mm:ssZ*.
- **Limit**: limit the results. Default is 1000.
- **Offset**: skip the first (offset) number of secrets.

Request Body

None.

Response Body

> **Note:** *If no secrets match the specified filter parameter(s), a 200 (OK) response with an empty list is expected.*

Content-Type: application/json

```
[
   {
        Id : Guid,
        Title : string,
        Description : string,
        Username : string,
        Password : string,
        OwnerId : int,
        FolderId : Guid,
        CreatedOn : Datetime,
        CreatedBy : string,
        ModifiedOn : Datetime,
        ModifiedBy : string,
        Owner : string,
        Folder : string,
        FolderPath : string,
        Owners : [{
        OwnerId : int,
        Owner : string,
        Email : string,
        }],
        OwnerType : string,
        Notes : string,
     Urls : [{
     Id : Guid,
     CredentialId : Guid,
     Url : String
     }]
    }
 ]
```

Response Codes

200 - OK

403 - Forbidden

> *For more information, please see "Common Response Codes" on page 17.*

GET Secrets-Safe/Secrets/{secretId:guid}

Purpose

Returns a secret by ID.

Required Permissions

Secrets-Safe (Read).

Parameters

SecretId: the secret ID (GUID).

Request Body

None.

Response Body

Content-Type: application/json

```
[
   {
        Id : Guid,
        Title : string,
        Description : string,
        Username : string,
        Password : string,
        OwnerId : int,
        FolderId : Guid,
        CreatedOn : Datetime,
        CreatedBy : string,
        ModifiedOn : Datetime,
        ModifiedBy : string,
        Owner : string,
        Folder : string,
        FolderPath : string,
        Owners : [{
        OwnerId : int,
        Owner : string,
        Email : string,
        }],
        OwnerType : string,
        Notes : string,
     Urls : [{
     Id : Guid,
     CredentialId : Guid,
```

```
      Url : String
      }]
   }
]
```

Response Codes

200 - OK

403 - Forbidden

404 - Not Found

For more information, please see "Common Response Codes" on page 17.

GET Secrets-Safe/Folders/{folderId:guid}/secrets

Purpose

Gets all the secrets based on the folderId.

Required Permissions

Secrets-Safe (Read).

Parameters

folderId: the given folder Id

Request Body

None.

Response Body

Content-Type: application/json

```
[
   {
         Id : Guid,
         Title : string,
         Description : string,
         Username : string,
         OwnerId : int,
         FolderId : Guid,
```

```
        CreatedOn : Datetime,
        CreatedBy : string,
        ModifiedOn : Datetime,
        ModifiedBy : string,
        Owner : string,
        Folder : string,
        FolderPath : string,
        Owners : [{
        OwnerId : int,
        Owner : string,
        Email : string,
        }],
        OwnerType : string,
        Notes : string,
        FileName : string,
        FileHash : string,
      Urls : [{
      Id : Guid,
      CredentialId : Guid,
      Url : String
      }]
    }
]
```

Response Codes

200 - OK

403 - Forbidden

404 - Not Found

For more information, please see "Common Response Codes" on page 17.

GET Secrets-Safe/Secrets/{secretId:guid}/text

Purpose

Get a secret text based on the secretId.

Required Permissions

Secrets-Safe (Read).

Parameters

SecretId: the secret id (GUID)

Request Body

None.

Response Body

Content-Type: application/json

```
[
   {
        Id : Guid,
        Title : string,
        Description : string,
        Text : string,
        OwnerId : int,
        FolderId : Guid,
        CreatedOn : Datetime,
        CreatedBy : string,
        ModifiedOn : Datetime,
        ModifiedBy : string,
        Owner : string,
        Folder : string,
        FolderPath : string,
        Owners : [{
        OwnerId : int,
        Owner : string,
        Email : string,
        }],
        OwnerType : string,
        Notes : string,
     Urls : [{
     Id : Guid,
     CredentialId : Guid,
     Url : String
     }]
   }
]
```

Response Codes

200 - OK

403 - Forbidden

404 - Not Found

For more information, please see "Common Response Codes" on page 17.

GET Secrets-Safe/Secrets/{secretId:guid}/file

Purpose

Gets secret file based on the secretId as file metadata with file properties. This is returned as type application/json.

Required Permissions

Secrets-Safe (Read).

Parameters

SecretId: the secret id (GUID)

Request Body

None.

Response Body

Content-Type: application/json

```
[
   {
        Id : Guid,
        Title : string,
        Description : string,
        OwnerId : int,
        FolderId : Guid,
        CreatedOn : Datetime,
        CreatedBy : string,
        ModifiedOn : Datetime,
        ModifiedBy : string,
        Owner : string,
        Folder : string,
        FolderPath : string,
        Owners : [{
        OwnerId : int,
        Owner : string,
        Email : string,
        }],
        OwnerType : string,
        Notes : string,
        FileName : string,
        FileHash : string,
     Urls : [{
     Id : Guid,
     CredentialId : Guid,
```

```
      Url : String
      }]
    }
]
```

Response Codes

200 - OK

403 - Forbidden

404 - Not Found

For more information, please see "Common Response Codes" on page 17.

GET Secrets-Safe/Secrets/{secretId:guid}/file/download

Purpose

Gets secret file as an attachment based on secretId.

Required Permissions

Secrets-Safe (Read).

Parameters

SecretId: the secret id (GUID)

Request Body

None.

Response Body

Content-Type: application/octet-stream

```
[
   {
     FileContentResult (binary file in the response)
   }
]
```

Response Codes

200 - OK

403 - Forbidden

404 - Not Found

For more information, please see "Common Response Codes" on page 17.

DELETE Secrets-Safe/Secrets/{secretId:guid}/

Purpose

Deletes a secret based on the secretId.

Required Permissions

Secrets-Safe (Read/Write).

Parameters

SecretId: the given secret Id (GUID)

Request Body

None.

Response Body

None.

Response Codes

200 – OK

403 - Forbidden

404 - Not found

For more information, please see "Common Response Codes" on page 17.

Appendix

Migration From v1 or v2

Any script or application written for v1 or v2 of the API needs some minor modifications to work with v3, namely the **Authorization** header and URL endpoints.

Authorization Header

In v1 and v2, the authorization header was used solely for the API application key. Now it is used to communicate the API application key as well as the RunAs username.

Example: *C#*

```
HttpClient client = new HttpClient();

client.DefaultRequestHeaders.Add("Authorization", "PS-Auth key=C9AB26FB-B322- ED97-A34C-215CA4D9630C; runas=doe-main\johndoe;");
```

Example: *Powershell*

```
$headers = @{ Authorization="PS-Auth key=C9AB26FB-B322-ED97-A34C-215CA4D9630C; runas=doe-main\johndoe;"; };
```

Endpoint Comparison

Note the use of https/SSL and removal of **PasswordSafe** segment in v3:

- v1 base endpoint: http://the-server/BeyondTrust/api/public/v1/PasswordSafe
- v2 base endpoint: http://the-server/BeyondTrust/api/public/v2/PasswordSafe
- v3 base endpoint: https://the-server/BeyondTrust/api/public/v3

Endpoint Mapping

Migration from v1

V1		V3	
Method	***Endpoint***	***Method***	***Endpoint***
GET	/v1/PasswordSafe/GetPublicKey	<deprecated>	
GET	/v1/PasswordSafe/SignIn	<deprecated>	
GET	/v1/PasswordSafe/Signout	POST	/v3/Auth/Signout
GET	/v1/PasswordSafe/SignAppIn	POST	/v3/Auth/SignAppin
GET	/v1/PasswordSafe/SecureSignAppIn	<deprecated>	
GET	/v1/PasswordSafe/GetManagedAccountsList	GET	/v3/ManagedAccounts
POST	/v1/PasswordSafe/ImmediatePasswordRequest	POST	/v3/Requests
GET	/v1/PasswordSafe/GetPendingRequests	GET	/v3/Requests?status=pending
GET	/v1/PasswordSafe/GetActiveRequests	GET	/v3/Requests?status=active
POST	/v1/PasswordSafe/RetrievePassword	GET	/v3/Credentials/{requestId}
POST	/v1/PasswordSafe/RetrieveSecurePassword	<deprecated>	
POST	/v1/PasswordSafe/ReleasePassword	PUT	/v3/Requests/{requestId}/Checkin

Migration from v2

v2		v3	
Method	***Endpoint***	***Method***	***Endpoint***
GET	/v2/PasswordSafe/GetPublicKey	<deprecated>	
GET	/v2/PasswordSafe/SignIn	<deprecated>	
POST	/v2/PasswordSafe/Signout	POST	/v3/Auth/Signout
POST	/v2/PasswordSafe/SignAppIn	POST	/v3/Auth/SignAppin
POST	/v2/PasswordSafe/SecureSignAppIn	<deprecated>	
GET	/v2/PasswordSafe/GetManagedAccountsList	GET	/v3/ManagedAccounts
POST	/v2/PasswordSafe/ImmediatePasswordRequest	POST	/v3/Requests
GET	/v2/PasswordSafe/GetPendingRequests	GET	/v3/Requests?status=pending
GET	/v2/PasswordSafe/GetActiveRequests	GET	/v3/Requests?status=active
POST	/v2/PasswordSafe/RetrievePassword	GET	/v3/Credentials/{requestId}
POST	/v2/PasswordSafe/RetrieveSecurePassword	<deprecated>	
POST	/v2/PasswordSafe/ReleasePassword	PUT	/v3/Requests/{requestId}/Checkin
GET	/v2/PasswordSafe/GetWorkgroups	GET	/v3/Workgroups
POST	/v2/PasswordSafe/QueueImport	POST	/v3/Imports