



VISIBILITY. KNOWLEDGE. ACTION.

PowerBroker Auditor Web API

User Guide

Version 5.6 - December 2017

Revision/Update Information: December 2017
Software Version: PowerBroker Auditor API 5.6
Revision Number: 0

CORPORATE HEADQUARTERS

5090 N. 40th Street Phoenix,
AZ 85018
Phone: 1 818-575-4000

COPYRIGHT NOTICE

Copyright © 2017 BeyondTrust Software, Inc. All rights reserved.

The information contained in this document is subject to change without notice.

No part of this document may be photocopied, reproduced or copied or translated in any manner to another language without the prior written consent of BeyondTrust Software.

BeyondTrust Software is not liable for errors contained herein or for any direct, indirect, special, incidental or consequential damages, including lost profit or lost data, whether based on warranty, contract, tort, or any other legal theory in connection with the furnishing, performance, or use of this material.

All brand names and product names used in this document are trademarks, registered trademarks, or trade names of their respective holders. BeyondTrust Software is not associated with any other vendors or products mentioned in this document.

Contents

- PowerBroker Auditor Public Web API..... 1**
- Usage..... 1**
 - Common Response Codes 1
 - Example 1
 - Workflow 1
- Authentication..... 3**
 - POST <base>/pbms/api/auth/login..... 3
 - GET <base>/pbms/api/agents/activeDirectory 4
 - POST <base>/pbms/api/agents/activeDirectory 5
 - PUT <base>/pbms/api/agents/activeDirectory/start 6
 - PUT <base>/pbms/api/agents/activeDirectory/stop 7
 - PUT <base>/pbms/api/agents/activeDirectory/restart 8
 - PUT <base>/pbms/api/agents/activeDirectory/refresh..... 9
 - PUT <base>/pbms/api/agents/activeDirectory/upgrade 10
 - DELETE <base>/pbms/api/agents/activeDirectory 11
- Backups 12**
 - POST <base>/pbms/api/activeDirectory/backups..... 12
 - POST <base>/pbms/api/activeDirectory/backups/details 13
- Installations 14**
 - POST <base>/pbms/api/installs 14
- Recycle Bin..... 15**
 - POST <base>/pbms/api/activeDirectory/recycleBin 15
- Restore 17**
 - POST <base>/pbms/api/activeDirectory/restore 17
- Rollback..... 19**
 - POST <base>/pbms/api/activeDirectory/rollback 19

PowerBroker Auditor Public Web API

This document specifies the Representational State Transfer (REST) compliant Application Programmer Interface (API) over HTTP for PowerBroker Auditor. It is a way to integrate a portion of the PowerBroker Auditor functionality into your own applications or scripts.

This resource is intended for readers with knowledge of HTTP request/response processing, web development, and basic JSON notation experience.

Usage

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 or missing request body. Reason in response body.

401 – Unauthorized – User is not authenticated. The request headers were not set properly, the server could not verify the validity of the request, or the token has expired.

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 BeyondTrust Support.

Example

Powershell

```
$Body = @{
    userName = "jDoe"
    password = "lq2w3e4r"
    domain = "contoso"
}
```

```
$admAuth=Invoke-RestMethod -Uri 'http://localhost/pbms/api/auth/login' -Body (ConvertTo-Json $Body) -ContentType 'application/json' -Method Post
```

Subsequent calls:

```
$HeaderValue = "Bearer " + $admAuth.access_token
```

```
$result = Invoke-RestMethod -Uri 'http://localhost/pbms/api/agents/activeDirectory' -Headers @{Authorization = $HeaderValue} -Method Get
```

```
echo $result
```

Workflow

There are some loose dependencies between the APIs. A typical sequence will be to list Active Directory Objects that have been deleted, use one of their identifiers to request the list of backups, and then perform an action using a

particular backup identifier.

Restore a Deleted Active Directory Object

Case: Authenticate to the Web Service, list the deleted objects from the Recycle Bin, list the available backups for an object, restore the deleted object

1. POST <base>/pbms/api/auth/login
2. POST <base>/pbms/api/activeDirectory/recycleBin
3. POST <base>/pbms/api/activeDirectory/backups
4. POST <base>/pbms/api/activeDirectory/restore

Rollback Active Directory Object Attribute(s)

Case: Authenticate to the Web Service, list the available backups for an object, view the details of a backup, rollback an object to a previous state

1. POST <base>/pbms/api/auth/login
2. POST <base>/pbms/api/activeDirectory/backups
3. POST <base>/pbms/api/activeDirectory/backups/detail
4. POST <base>/pbms/api/activeDirectory/rollback

Authentication

POST <base>/pbms/api/auth/login

Purpose

Authenticates the provided credentials and creates a JSON Web Token (JWT) for use with any API request that requires authentication. The user must also supply the GUID for the PBMS Installation they will be pointing to. If only one installation exists, an empty GUID can be used and it will be automatically selected.

Required Permissions

An Active Directory user must have Administrator access to the web console, granted in either the Web Configuration tool or Web Console user access section.

URL Parameters

None

Request Body Parameters

userName, password, domain – (optional) Active Directory credentials for executing action
install – (optional) Guid of PBMS installation

Request Body

Content-Type: application/json

```
{
  userName : string,
  password : string,
  domain : string,
  install : guid
}
```

Response Body

Content-Type: application/json

```
{
  access_token : string,
  expires_in : int
}
```

Response Codes

See [Common Response Codes](#)

200 – Request successful. JWT is in response body.

400 – See response body for error message.

GET <base>/pbms/api/agents/activeDirectory

Purpose

Returns a list of Active Directory Agents

Required Permissions

Web Console (Administrator)

URL Parameters

None

Request Body

None

Response Body

Content-Type: application/json

```
{
  id : string,
  pld : string,
  mld : int,
  module : string,
  server : string,
  description : string,
  hookVersion : string,
  osVersion : string,
  heartbeat : string,
  monitorStatus : int,
  alertCount : int,
  dqueueCount : int
}
```

Response Codes

See [Common Response Codes](#)

200 – Request successful. Agents in the response body.

400 – See response body for error message.

POST <base>/pbms/api/agents/activeDirectory

Purpose

Deploy an Active Directory Agent. User can either indicate a selectionType of “DomainController” and then select the domain controller(s) you wish to deploy an agent to, or a selectionType of “Domain” and then deploy to all domain controllers in that domain. If the authenticated user does not have the credentials to perform the action, credentials are required.

Required Permissions

Web Console (Administrator)

URL Parameters

None

Request Body Parameters

selectionType – Possible values:

“DomainController” – Deploy to only specific Domain Controller(s)

“Domain” – Deploy Agent to all Domain Controllers

selection – Comma-delimited list of Domain Controllers to deploy an Agent to

userName, password, domain – (optional) Active Directory credentials for executing action

Request Body

Content-Type: application/json

```
{
  selectionType : string,
  selection : string,
  userName : string,
  password : string,
  domain : string
}
```

Response Body

Success message

Response Codes

See [Common Response Codes](#)

200 – Request successful. Success message in response body.

400 – See response body for error message.

PUT <base>/pbms/api/agents/activeDirectory/start

Purpose

Starts an Active Directory Agent. If the authenticated user does not have the credentials to perform the action, credentials are required.

Required Permissions

Web Console (Administrator)

URL Parameters

None

Request Body Parameters

server – Name of Domain Controller

userName, password, domain – (optional) Active Directory credentials for executing action

Request Body

Content-Type: application/json

```
{
  server : string,
  userName : string,
  password : string,
  domain : string
}
```

Response Body

Success message

Response Codes

See [Common Response Codes](#)

200 – Request successful. Success message in response body.

400 – See response body for error message.

PUT <base>/pbms/api/agents/activeDirectory/stop

Purpose

Stops an Active Directory Agent. If the authenticated user does not have the credentials to perform the action, credentials are required.

Required Permissions

Web Console (Administrator)

URL Parameters

None

Request Body Parameters

server – Name of Domain Controller

userName, password, domain – (optional) Active Directory credentials for executing action

Request Body

Content-Type: application/json

```
{
  server : string,
  userName : string,
  password : string,
  domain : string
}
```

Response Body

Success message

Response Codes

See [Common Response Codes](#)

200 – Request successful. Success message in response body.

400 – See response body for error message.

PUT <base>/pbms/api/agents/activeDirectory/restart

Purpose

Stops then restarts an Active Directory Agent. If the authenticated user does not have the credentials to perform the action, credentials are required.

Required Permissions

Web Console (Administrator)

URL Parameters

None

Request Body Parameters

server – Name of Domain Controller

userName, password, domain – (optional) Active Directory credentials for executing action

Request Body

Content-Type: application/json

```
{
  server : string,
  userName : string,
  password : string,
  domain : string
}
```

Response Body

Success message

Response Codes

See [Common Response Codes](#)

200 – Request successful. Success message in response body.

400 – See response body for error message.

PUT <base>/pbms/api/agents/activeDirectory/refresh

Purpose

Refresh the settings of an Active Directory Agent. If the authenticated user does not have the credentials to perform the action, credentials are required.

Required Permissions

Web Console (Administrator)

URL Parameters

None

Request Body Parameters

server – Name of Domain Controller

userName, password, domain – (optional) Active Directory credentials for executing action

Request Body

Content-Type: application/json

```
{
  server : string,
  userName : string,
  password : string,
  domain : string
}
```

Response Body

Success message

Response Codes

See [Common Response Codes](#)

200 – Request successful. Success message in response body.

400 – See response body for error message.

PUT <base>/pbms/api/agents/activeDirectory/upgrade

Purpose

Upgrade an Active Directory Agent. If the authenticated user does not have the credentials to perform the action, credentials are required.

Required Permissions

Web Console (Administrator)

URL Parameters

None

Request Body Parameters

server – Name of Domain Controller

userName, password, domain – (optional) Active Directory credentials for executing action

Request Body

Content-Type: application/json

```
{
  server : string,
  userName : string,
  password : string,
  domain : string
}
```

Response Body

Success message

Response Codes

See [Common Response Codes](#)

200 – Request successful. Success message in response body.

400 – See response body for error message.

DELETE <base>/pbms/api/agents/activeDirectory

Purpose

Remove an Active Directory Agent. If the authenticated user does not have the credentials to perform the action, credentials are required.

Required Permissions

Web Console (Administrator)

URL Parameters

None

Request Body Parameters

server – Name of Domain Controller

userName, password, domain – (optional) Active Directory credentials for executing action

Request Body

Content-Type: application/json

```
{
  server : string,
  userName : string,
  password : string,
  domain : string
}
```

Response Body

Success message

Response Codes

See [Common Response Codes](#)

200 – Request successful. Success message in response body.

400 – See response body for error message.

Backups

POST <base>/pbms/api/activeDirectory/backups

Purpose

Returns all Backups for an Active Directory Object.

Required Permissions

Web Console (Administrator)

URL Parameters

None

Request Body Parameters

objectId – Guid of the object in Active Directory

objectDN – Distinguished Name of the object in Active Directory

Request Body

Content-Type: application/json

```
{
  objectId : guid,
  objectDN : string
}
```

Response Body

Content-Type: application/json

```
{
  BackupTime: string,
  ID : string
}
```

Response Codes

See [Common Response Codes](#)

200 – Request successful. Backups in the response body.

400 – See response body for error message.

POST <base>/pbms/api/activeDirectory/backups/details

Purpose

Returns details for the specified Backup of an Active Directory Object.

Required Permissions

Web Console (Administrator)

URL Parameters

None

Request Body Parameters

backupId – Retrieved from backup list request

objectId – Guid of the object in Active Directory

objectDN – Distinguished Name of the object in Active Directory

Request Body

Content-Type: application/json

```
{
  backupId : string,
  objectId : guid,
  objectDN : string
}
```

Response Body

Content-Type: application/json

```
{
  BackupID : string,
  ObjectID : guid,
  Attribute : [{
    Name : string,
    Value : string
  }]
}
```


Response Codes

See [Common Response Codes](#)

200 – Request successful. Backup details in the response body.

400 – See response body for error message.

Installations

POST <base>/pbms/api/installs

Purpose

Returns all PBMS installations

Required Permissions

None

URL Parameters

None

Request Body Parameters

userName, password, domain – (optional) Active Directory credentials for executing action

install – blank guid

Request Body

Content-Type: application/json

```
{
  userName : string,
  password : string,
  domain : string,
  install : guid
}
```

Response Body

Content-Type: application/json

```
{
  id : guid,
  label : string
}
```

Response Codes

See [Common Response Codes](#)

200 – Request successful. Installations in the response body.

400 – See response body for error message.

Recycle Bin

POST <base>/pbms/api/activeDirectory/recycleBin

Purpose

Returns details of all Active Directory Objects in the Recycle Bin. An optional partition can be set if the Recycle Bin does not reside on the current partition. If the authenticated user does not have the credentials to perform the action, credentials are required.

Required Permissions

Web Console (Administrator)

URL Parameters

None

Request Body Parameters

objectDN – Retrieved from Active Directory

userName, password, domain – (optional) Active Directory credentials for executing action

partition – (optional) Default Naming Context, by default

Request Body

Content-Type: application/json

```
{
  userName : string,
  password : string,
  domain : string,
  partition : string
}
```

Response Body

Content-Type: application/json

```
{
  id : guid,
  name : string,
  distinguishedName : string,
  objectClass : string,
  timeLeft : string,
  timeLeftRaw : string,
  whenChanged : string,
  lastKnownParent : string
}
```

Response Codes

See [Common Response Codes](#)

200 – Request successful. Recycle Bin contents in the response body.

400 – See response body for error message.

Restore

POST <base>/pbms/api/activeDirectory/restore

Purpose

Restore a deleted Active Directory Object from a Backup. If the authenticated user does not have the credentials to perform the action, credentials are required.

Required Permissions

Web Console (Administrator)

URL Parameters

None

Request Body Parameters

backupId – Retrieved from backup request

objectDN – Retrieved from Active Directory

userName, password, domain – (optional) Active Directory credentials for executing action

containerRestoreOption – Possible values:

“0” – Restore entire sub-tree (default)

“1” – Restore immediate children only

“2” – Do not restore any child objects

containerRestoreOption – Possible values:

“0” – Skip the object (default)

“2” – Automatically choose new values

domainControllers – (optional) Server name

partition – (optional) Default Naming Context, by default

Request Body

Content-Type: application/json

```
{
  backupId : string,
  objectDN : string,
  userName : string,
  password : string,
  domain : string,
  containerRestoreOption : string,
  namingConflictOption : string,
  domainController : string,
  partition : string
}
```

Response Body

Success message

Response Codes

See [Common Response Codes](#)

200 – Request successful. Success message in response body.

400 – See response body for error message.

Rollback

POST <base>/pbms/api/activeDirectory/rollback

Purpose

Rollback selected attributes of an Active Directory Object from a Backup. If the authenticated user does not have the credentials to perform the action, credentials are required.

Required Permissions

Web Console (Administrator)

URL Parameters

None

Request Body Parameters

backupId – Retrieved from backup request

objectDN – Guid of the object in Active Directory

userName, password, domain – (optional) Active Directory credentials for executing action

attributes – Comma-delimited list of attributes to rollback

domainControllers – (optional) Server name

Request Body

Content-Type: application/json

```
{
  backupId : string,
  objectDN : string,
  userName : string,
  password : string,
  domain : string,
  attributes : string,
  domainController : string
}
```

Response Body

Success message

Response Codes

See [Common Response Codes](#)

200 – Request successful. Success message in response body.

400 – See response body for error message.