McAfee ePolicy Orchestrator (ePO) Integration Document

Company and Author: Ridge Security

A green rectangular sign with black text

Description automatically generated

Table of Contents

[1 Overview 3](#_Toc148461501)

[2 Included Files 3](#_Toc148461502)

[3 Supported ePO and Product Version 3](#_Toc148461503)

[4 Approved Product ID and Event ID’s 3](#_Toc148461504)

[5 Prerequisites 3](#_Toc148461505)

[6 Partner Product Supported Client Platforms 3](#_Toc148461506)

[7 Installing Partner Software 4](#_Toc148461507)

[8 Adding ePO Integration to a Partner Software 5](#_Toc148461508)

[9 Preparing the ePO Server 5](#_Toc148461509)

[9.1 Setting up an ePO Server 5](#_Toc148461510)

[9.1.1 Steps to install RidgeBot Server extension: 5](#_Toc148461511)

[9.1.2 Steps to Configure RidgeBot Registered Server: 6](#_Toc148461512)

[9.1.3 Steps to Configure RidgeBot Server Task: 7](#_Toc148461513)

[9.1.4 Manage RidgeBot Task: 8](#_Toc148461514)

[9.1.5 Create New RidgeBot Task: 9](#_Toc148461515)

[9.1.6 Delete RidgeBot Task(s): 11](#_Toc148461516)

[9.1.7 Pause RidgeBot Task: 12](#_Toc148461517)

[9.1.8 Start (Resume) RidgeBot Task: 14](#_Toc148461518)

[9.1.9 Stop RidgeBot Task: 16](#_Toc148461519)

[9.1.10 Re-Start RidgeBot Task: 17](#_Toc148461520)

[10 Testing the Integration 18](#_Toc148461521)

[10.1 Deploying Partner Agents to an Endpoint 18](#_Toc148461522)

[10.1.1 Manual Partner Agent Deployment Options 18](#_Toc148461523)

[10.1.2 Event Reporting through Common Event XML 18](#_Toc148461524)

[10.1.3 Policy Enforcement 18](#_Toc148461525)

[10.1.4 Task Enforcement 18](#_Toc148461526)

[10.2 Verifying Agent deployment from ePO 18](#_Toc148461527)

[11 Uninstalling ePO Integration 18](#_Toc148461528)

[12 Reporting 19](#_Toc148461529)

[12.1 Query Targets 19](#_Toc148461530)

[12.2 Canned Queries 19](#_Toc148461531)

[12.3 Custom Tables 20](#_Toc148461532)

[12.4 Dashboards 22](#_Toc148461533)

[13 Appendix A. Logs and Troubleshooting 22](#_Toc148461534)

[13.1 Troubleshooting 22](#_Toc148461535)

[13.2 Useful Logs 22](#_Toc148461536)

[13.3 Known Issues 23](#_Toc148461537)

# Overview

This document guides you to set up and test the RidgeBot server, an automated security testing platform (a product of Ridge Security) integration functionalities from McAfee ePolicy Orchestrator (ePO).

# Included Files

This evaluation version of Ridge Security-ePO integration includes the following files:

|  |  |
| --- | --- |
| **Partner Product Setup** | **ePO Server Setup** |
| RidgeBot server installer can be downloaded here( <https://partners.ridgesecurity.ai/partner-home/software-downloads> ) | RidgeBot ePO Extension: **RidgeBotServiceManager.zip** |
| Ridge Security RidgeBot User Manual |  |
| Please contact [support@ridgesecurity.ai](mailto:support@ridgesecurity.ai) to get an access to partner portal to download the software and apply for a trial license. |  |
|  |  |

# Supported ePO and Product Version

* ePO 5.10.0(Build 4098), Service Pack 1.
* RidgeBot sever 4.2.2

# Approved Product ID and Event ID’s

Approved Produc Id/Software Id: **S\_RIDGBT1000**

# Prerequisites

Refer the “Deploying RidgeBot” section in the “Ridge Security RidgeBot User Manual v4.2.4\_52484.pdf” to get the prerequisites.

# Partner Product Supported Client Platforms

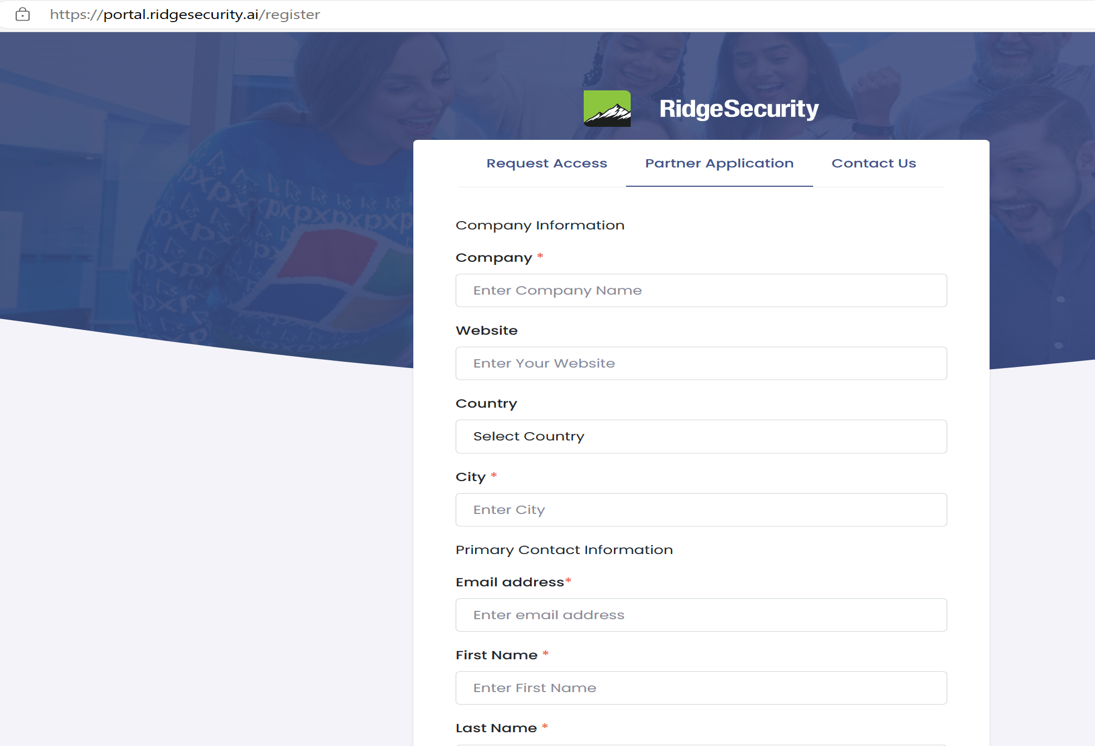
If you have integrations like product deployment, policy management, task management or event reporting, please specify Yes/No in this table.

|  |  |  |
| --- | --- | --- |
| **Partner Supported Client Platforms** | **Client Nodes** | **Supported** |
| Windows Vista x86 | No |
| Windows Vista x64 | No |
| Windows 2008 x86 | No |
| Windows 2008 x64 | No |
| Windows 7 x86 | No |
| Windows 7 x64 | No |
| Windows 8 x86 | No |
| Windows 8 x64 | No |
| Windows 10 x86 | No |
| Windows 10 x64 | No |
| Windows 2K12 R2 | No |
| Linux | No |
| OS X | No |

# Installing Partner Software

Refer the “Deploying RidgeBot” section in the “Ridge Security RidgeBot User Manual v4.2.4\_52484.pdf” to install RidgeBot server.

**Note**: Make sure that you select the right option while creating the account. In this case select “Partner Application” during the signup process.



After the successful installation of RidgeBot server, you have to generate the Identity token to access RidgeBot APIs.

Follow “API Compatibility” section in “Ridge Security RidgeBot User Manual v4.2.4\_52484.pdf” to generate the Identity token and save the same for the future reference (we will use this information while configuring RidgeBot registered server in ePO.)

# Adding ePO Integration to a Partner Software

RidgeBot server can be installed in any windows system, we have provided the product guide (“**Ridge Security RidgeBot User Manual v4.2.4\_52484.pdf**“) to setup RidgeBot server, follow the same instruction to install and configure RidgeBot server.

# Preparing the ePO Server

## Setting up an ePO Server

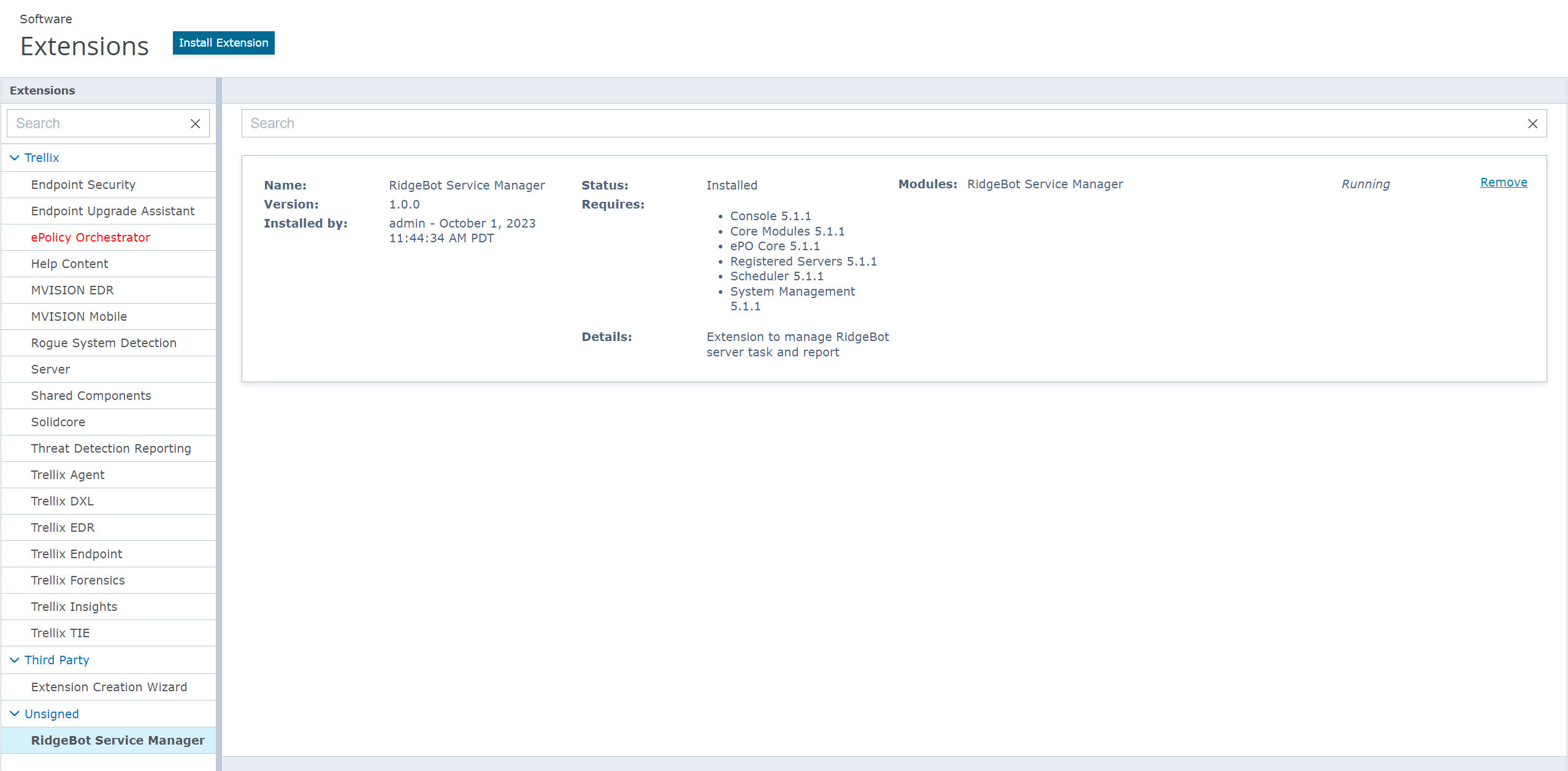
RidgeBot server can be installed in any system and it can be installed in ePO system as well, but it is better to install in different system than ePO server system.

We have provided the **RidgeBotServiceManager.zip** extension that need to be installed in ePO server.

**Note**: We have tested our extension in ePO server 5.10.0(Build 4098), Service Pack 1.

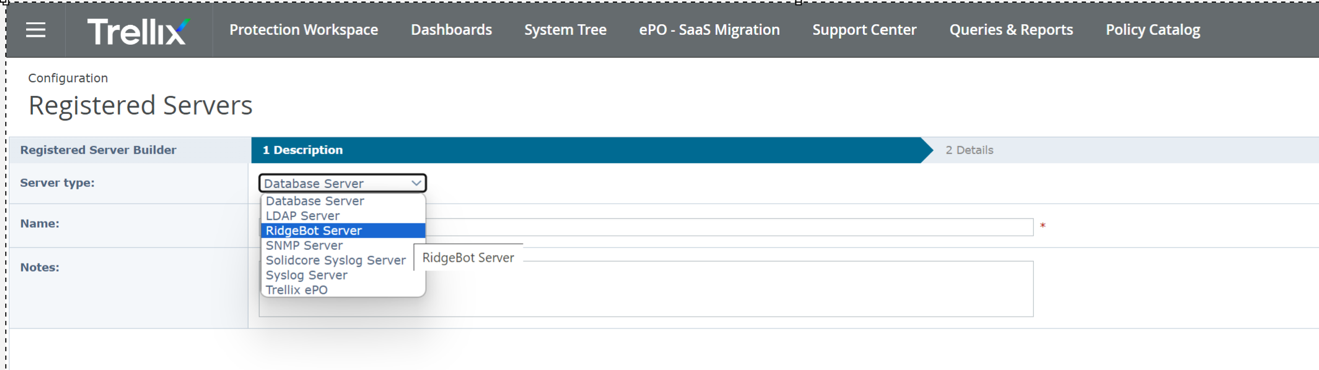
### Steps to install RidgeBot Server extension:

1. Login into ePO server using admin credentials.
2. Go to **Menu | Software | Extensions | Install Extension**
3. Select “**RidgeBotServiceManager.zip”** extension and install**.**
4. This extension will be shown under “**Unsigned**” section. Please refer the below screenshot.

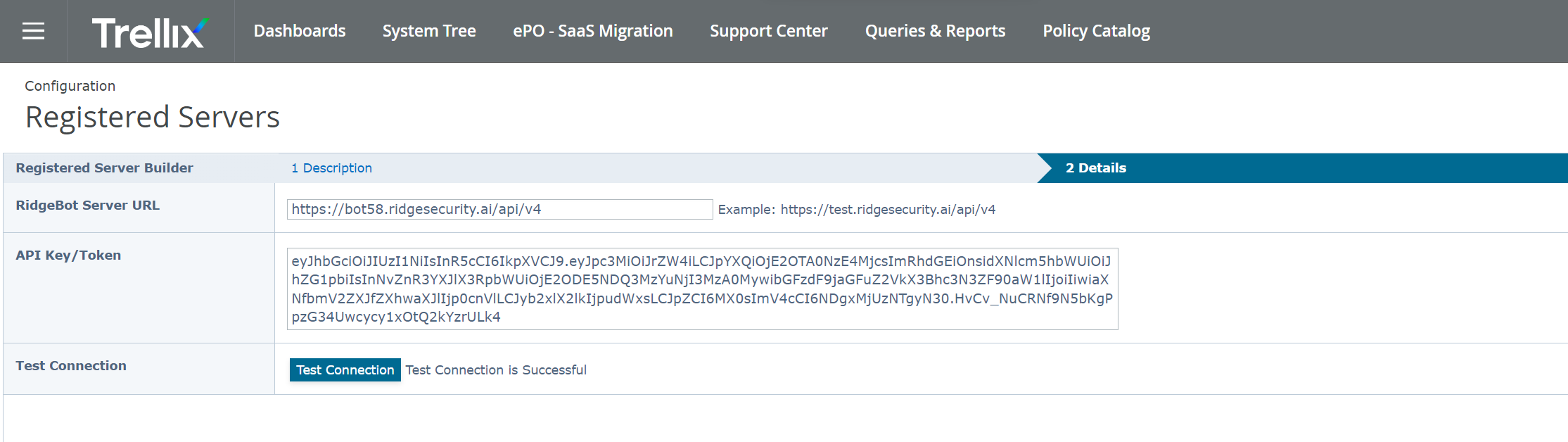


### Steps to Configure RidgeBot Registered Server:

1. Go to **Menu | Configuration | Registered Servers | New Server**
2. Select “**RidgeBot Server**” server type and provide any name (Ex: RidgeBot Test Server.)**.**

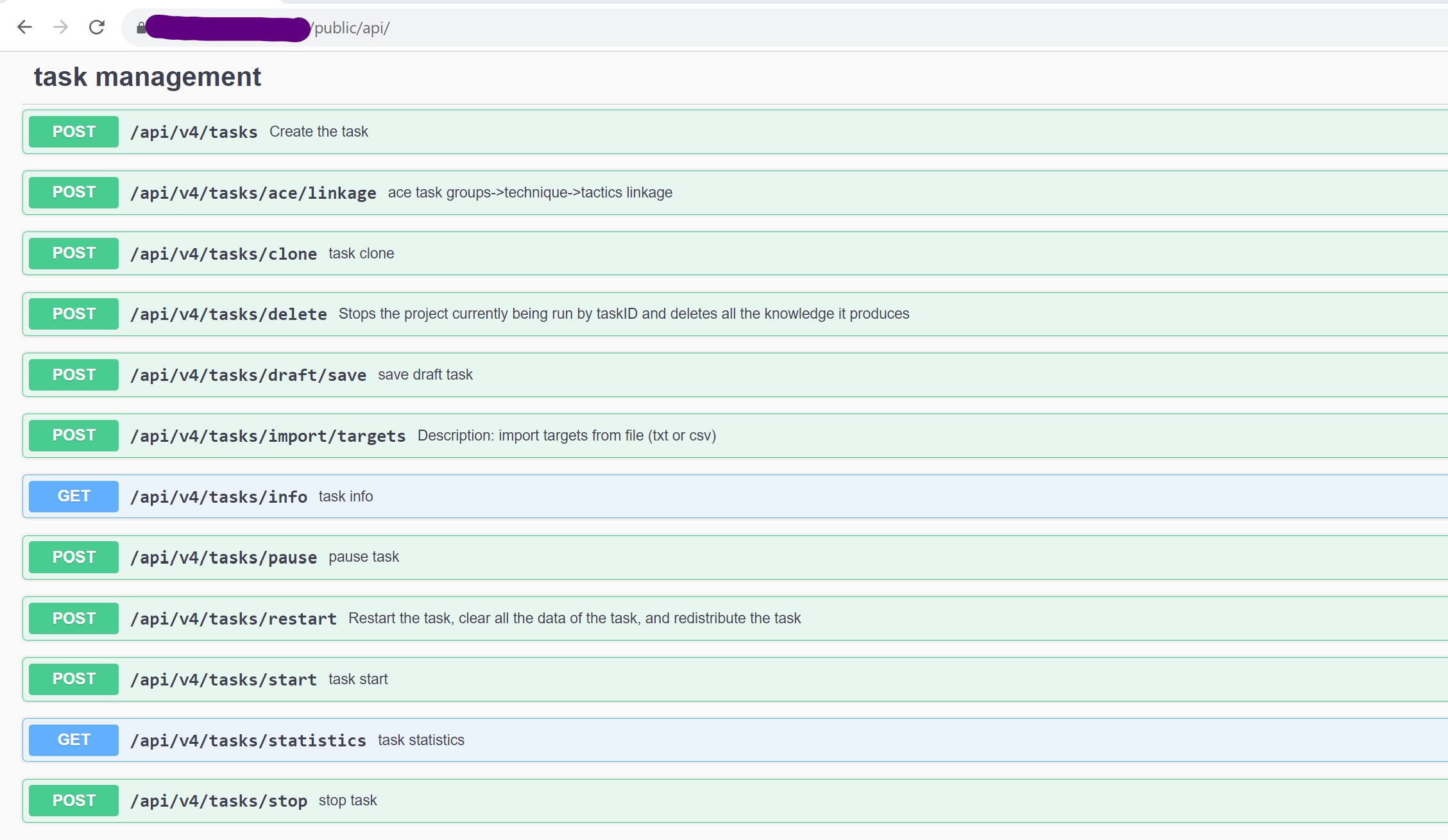
****

1. Now provide the RidgeBot server API URL and API Key to communicate with RidgeBot server. Then click “**Test Connection**” button to test the communication and save the configuration.

****

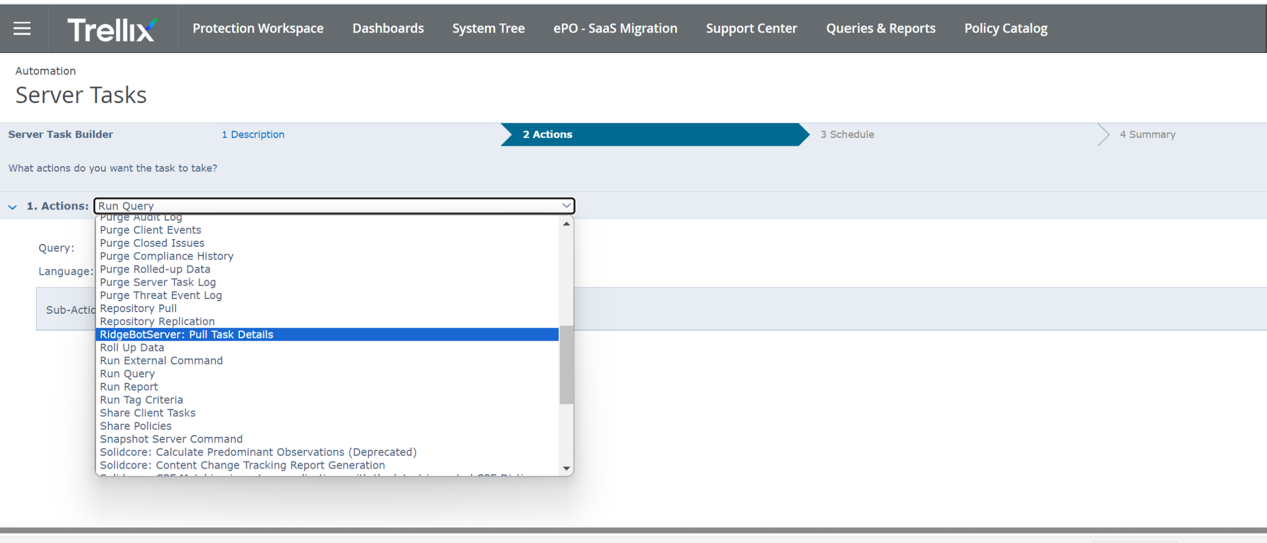
Follow “**API Compatibility**” section in “Ridge Security RidgeBot User Manual v4.2.4\_52484.pdf” to generate the Identity token and the API URL.

To access RidgeBot API, type in the below URL in the web browser: **https://<RidgeBot\_IPADDR>/public/api**

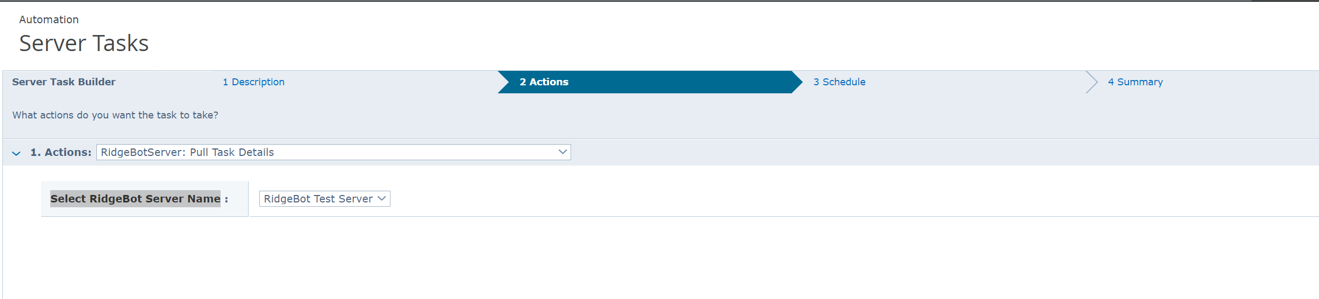


### Steps to Configure RidgeBot Server Task:

1. Go to **Menu | Automation | Server Tasks | New Task**
2. Provide any name (Ex: RidgeBot Task) and click “**Next**” button.
3. Now select the “**RidgeBot Server: Pull Task Details**” in Actions dropdown.

****

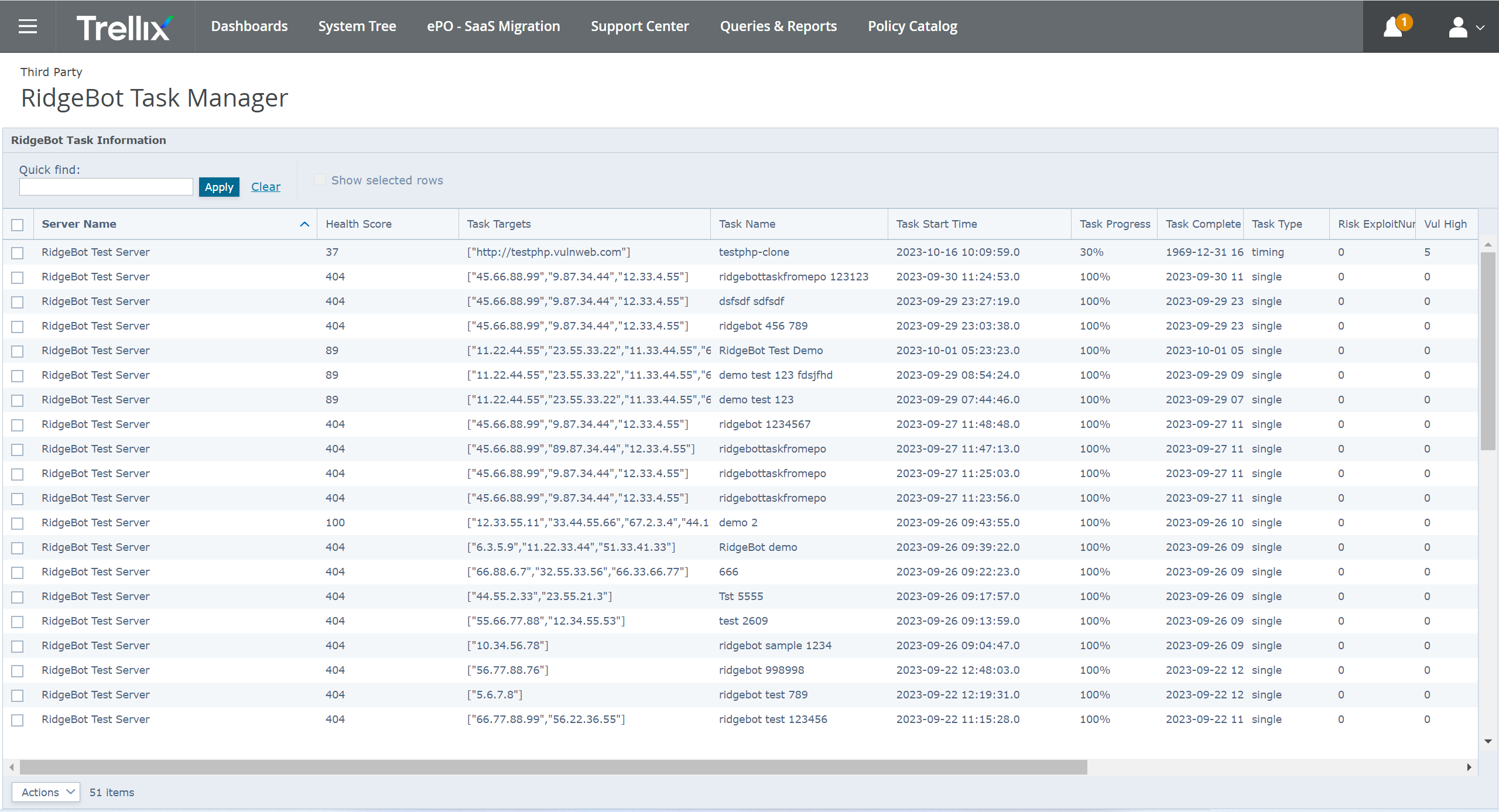
1. Now select the previously created Registered Server for RidgeBot from the “**Select RidgeBot Server Name**” dropdown and click next.

****

1. Select “**Advance**” option for “**Schedule Type**”, select start date as current date and time and select end date as “**no end date**”.
2. Then provide “**0 0/5 \* \* \* ?**” as Cron syntax (to schedule this task) for every 5 minutes. Now client “**Next**” and then click “**Save**” button to save the configuration.
3. Now go to **Menu | Automation | Server Tasks** and run the “**RidgeBot Task**” which pulls the task data from RidgeBot server to ePO.

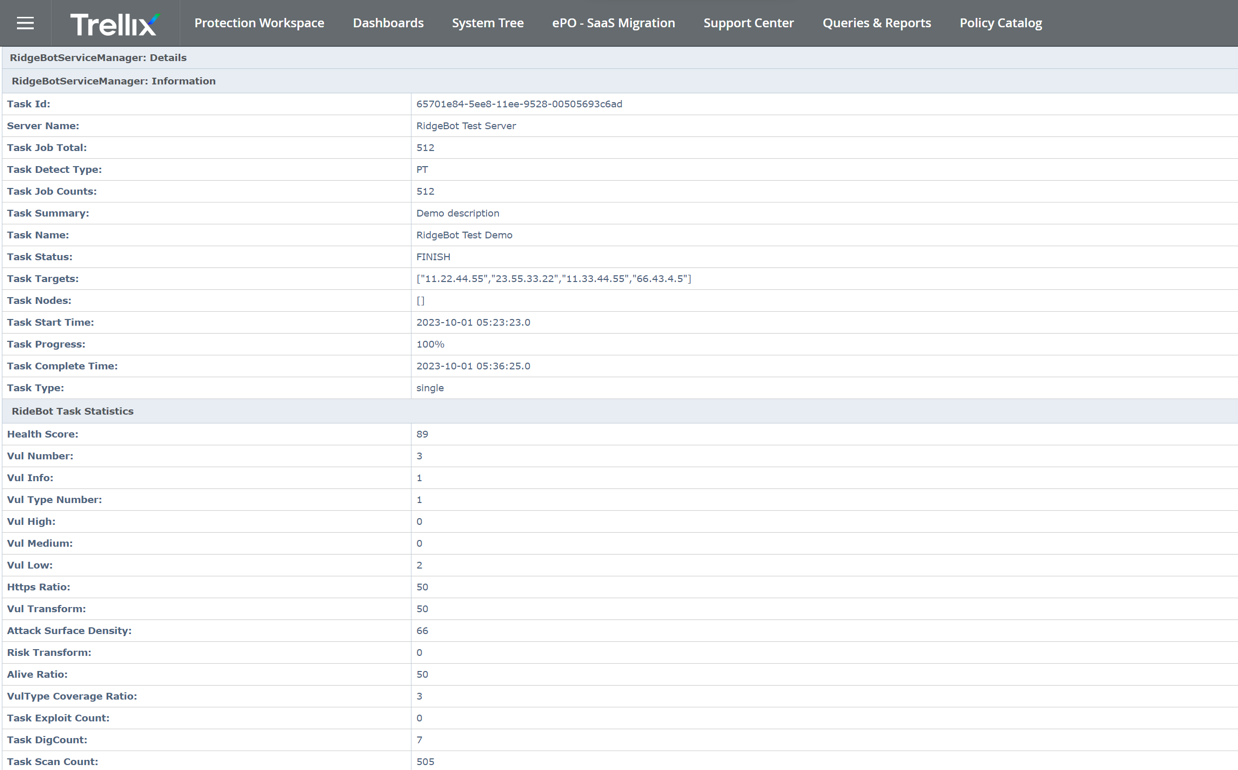
### Manage RidgeBot Task:

1. As part of this integration, we have created a custom tab under “**Third Party**” section.
2. Go to **Menu | Third Party | RidgeBot Task Manager** tab.
3. This tab will show all the RidgeBot tasks and its details pulled by the ePO server task.

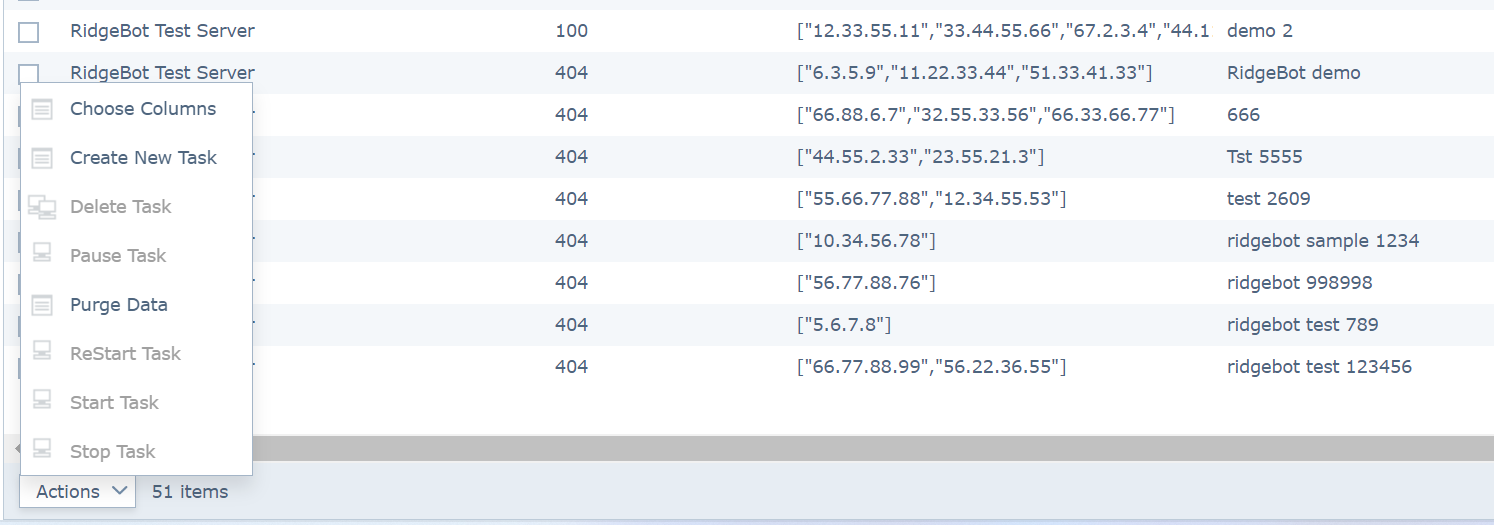


**Note**: The total number of tasks under this section should match with the number of tasks that are present in RidgeBot server.

1. The RidgeBot task details will be shown if you click on any task row.



1. Also, we have few actions that can be performed from our custom tab UI to mange RidgeBot server task. The actions are, Create New Task, Delete Task, Pause Task, Restart Task, Start Task, Stop Task and Purge Data.



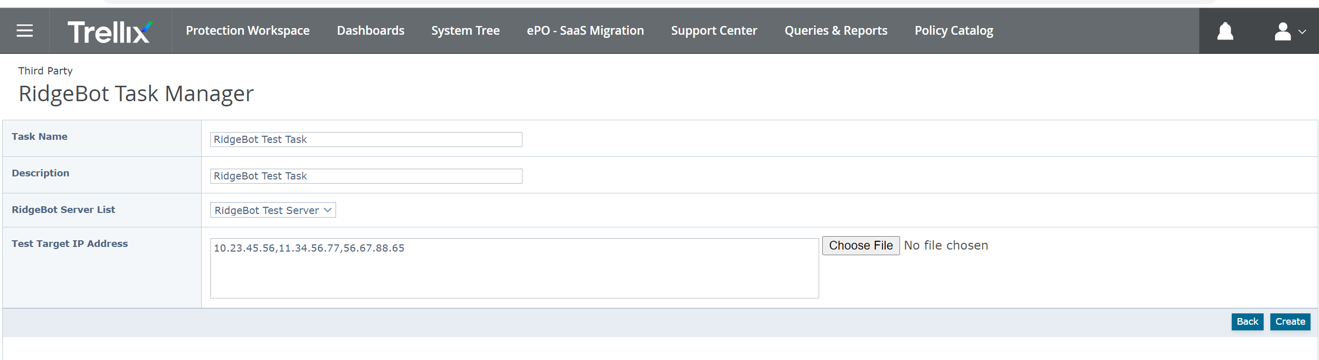
### Create New RidgeBot Task:

1. The Create Task action will allow the user to create a new RidgeBot task to from ePO UI.

**Note:** This Create New task will be applicable only for the “**Host Penetration**” task type on the RidgeBot server side.

**API URL:** **https://<RidgeBot\_IPADDR>/api/v4/tasks**

1. Goto **Menu | Third Party | RidgeBot Task Manager | Actions** and click “**Create New Task**” action.
2. This will open a new UI page where user have to provide the required details to create a task. Refer the below screenshot.



In this UI,

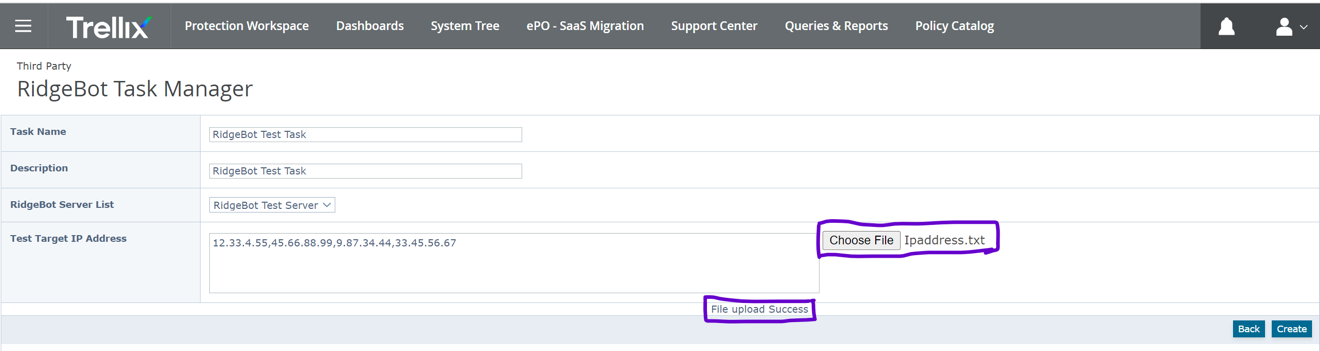
**Task Name:** User defined name for the RidgeBot task

**Description :** User defined description for the RidgeBot task

**RidgeBot Server List :** Selec the RidgeBot registerd server isntance in which this new task needs to be created.

**Test Target IP Address:** The coma seperated list of IP address to be passed as an argument to the new Task.

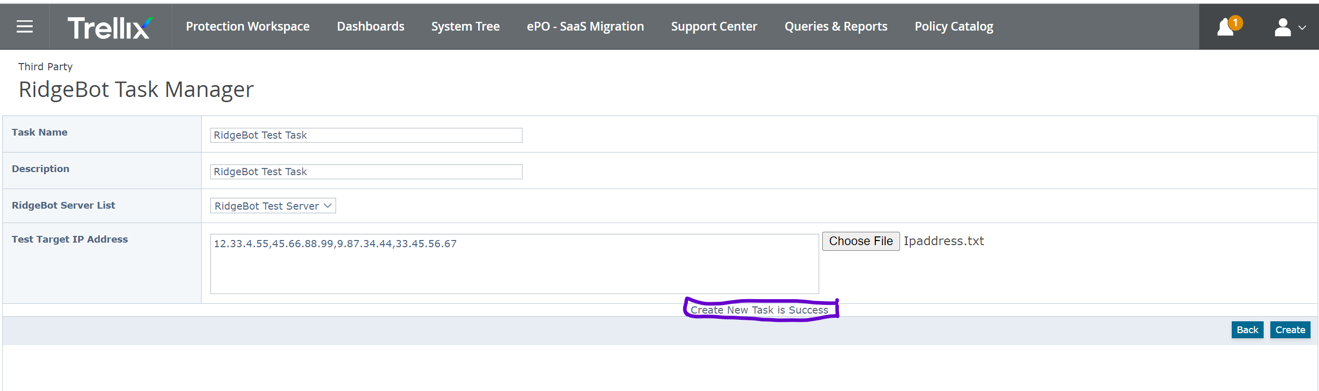
**Note:** User can selec the “**Choose File**” option to import the text file which contains the coma sepreated list of ip address instead of typeing all the IP Address. Only .txt file with coma sepereted ip list is support.

****

If the user select the file upload option, the file content will be imported and the status of the file import will be displayed in the UI, as shown in the screenshot.

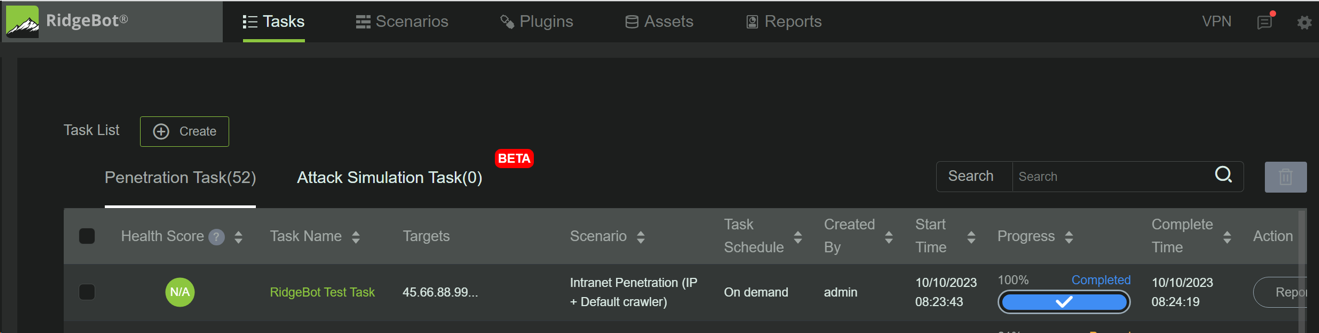
**Note:** If any issue occures during file import the error meesage will be shown in the UI and the “Create” button will be disabled.

1. Once all the information provides, then click on “**Create**” button to create this task in RidgeBot server. The status (Success (or) Failure) will be shown on the UI. Refer the below screenshot.

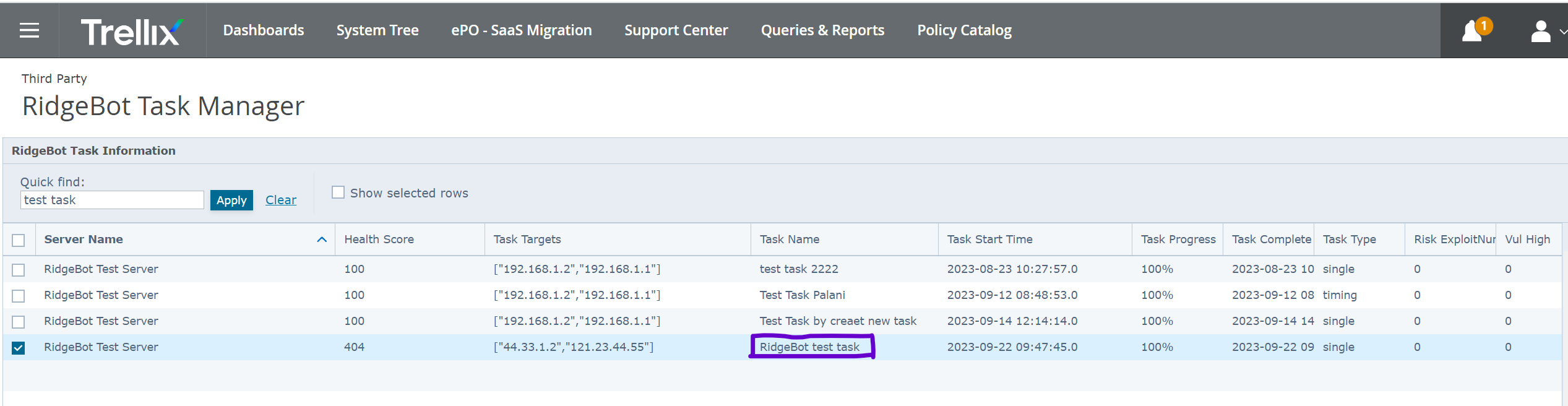


**Note:** The “**Back**” button in this page will take the user back to **Menu | Third Party | RidgeBot Task Manager** page.

1. If the create task is successful in ePO UI, this action will create a new task in the RidgeBot server with the same name that we have provided in ePO UI. Refer the below screenshot.



1. The action will create a new task in the ePO server aswell. The new task enrty will be added into the tasl list.

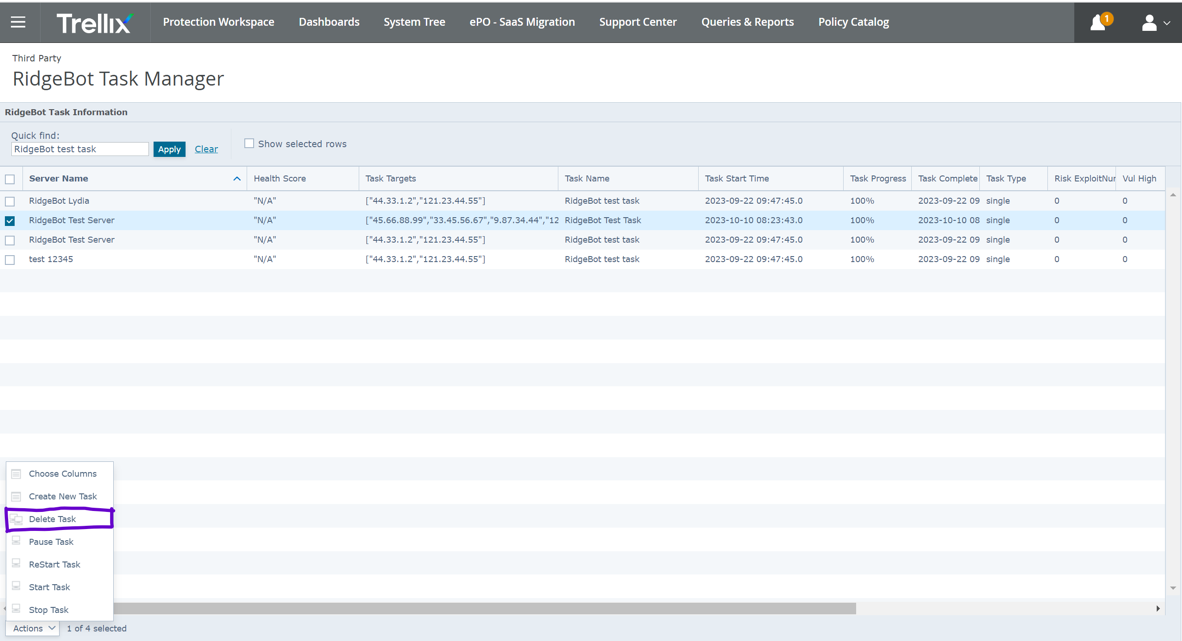


### Delete RidgeBot Task(s):

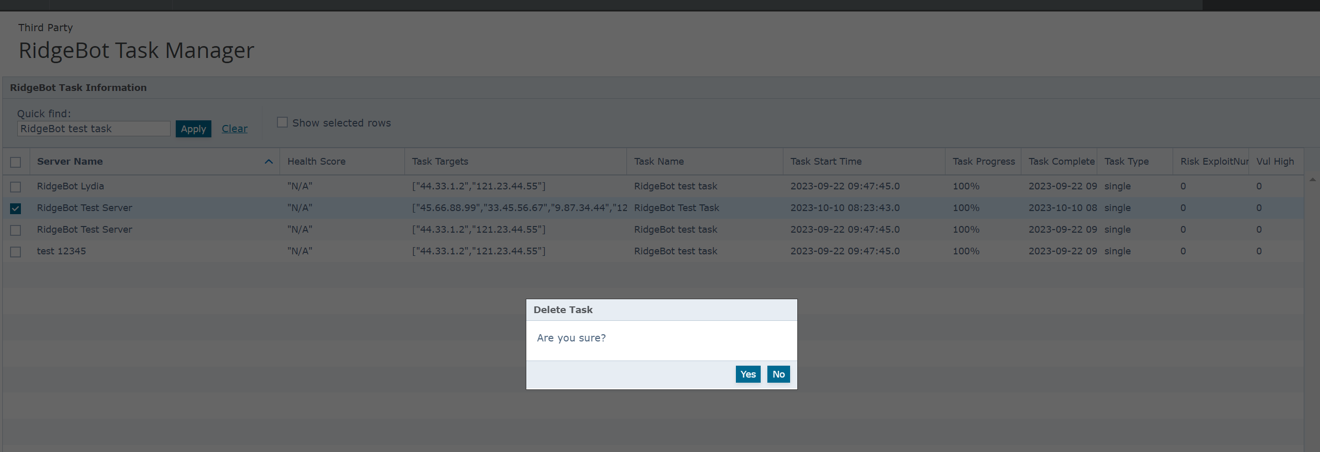
1. The Delete Task action will allow the user to delete one or more RidgeBot task from ePO UI.

**API URL:** **https://<RidgeBot\_IPADDR>/api/v4/tasks/delete**

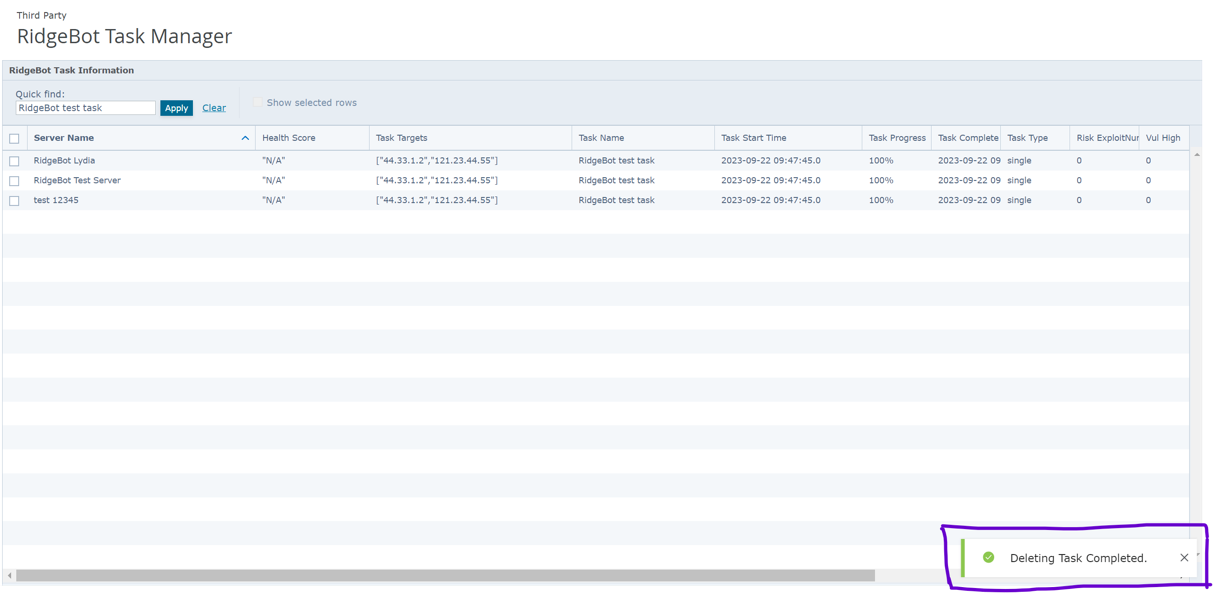
1. Goto **Menu | Third Party | RidgeBot Task Manager** Tab.
2. Select one or more tasks by clicking the checkbox and click **Actions | Delete Task** option.



1. This action will open up the popup and ask for the user confirmation.



1. If the user clicks “**Yes**” then the selected tasks will be removed from RidgeBot server as well as from the ePO database tables of RidgeBot extension.



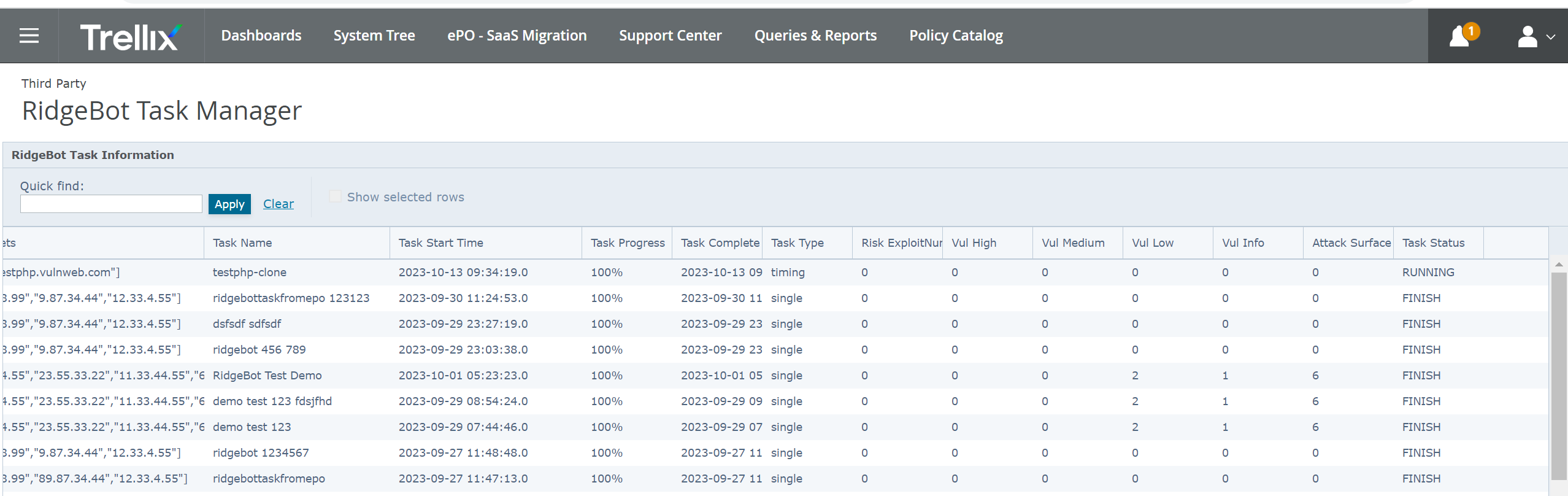
**Note**: If the delete operation fails then this action will show “**Error While Deleting Task.**” message.

### Pause RidgeBot Task:

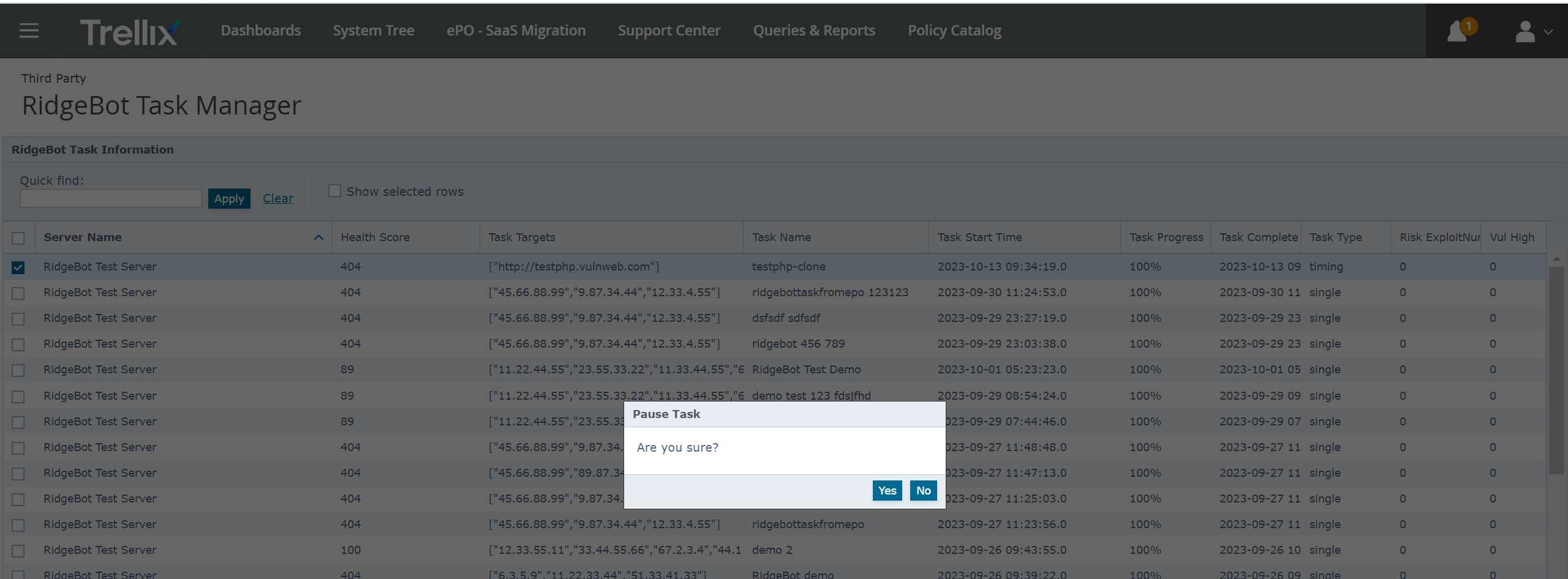
1. The Pause Task action will allow the user to Pause a RidgeBot task from ePO UI.
2. Goto **Menu | Third Party | RidgeBot Task Manager** Tab.
3. Select one task by clicking check box and click **Actions | Pause Task** option.

**Note:** The “Pause Task” option applicable only for the task with “RUNNING” as status.

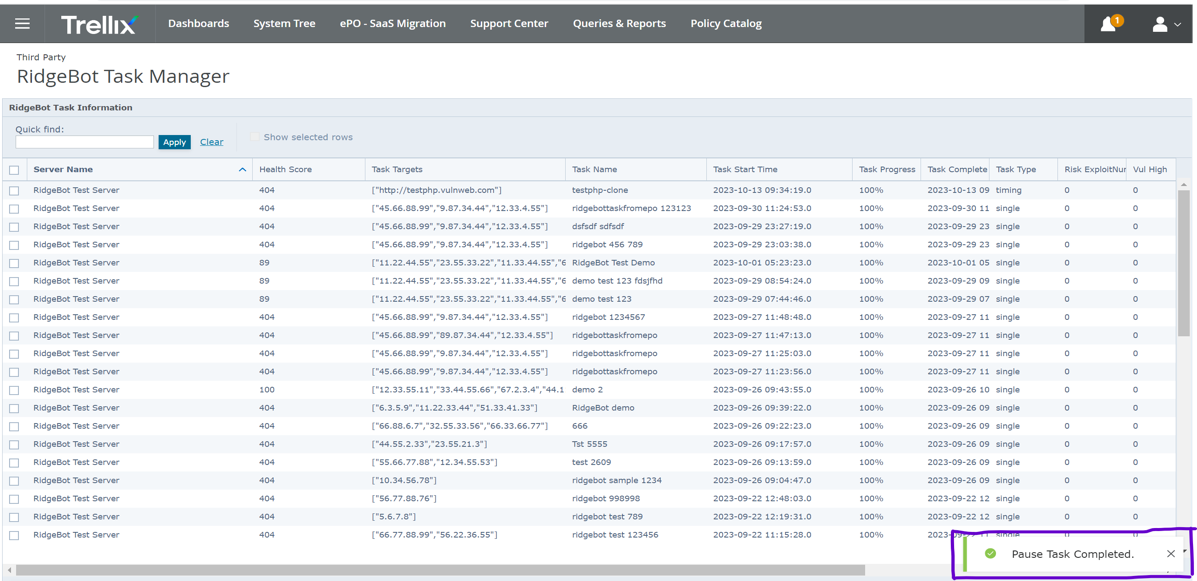
**API URL:** **https://<RidgeBot\_IPADDR>/api/v4/tasks/pause**



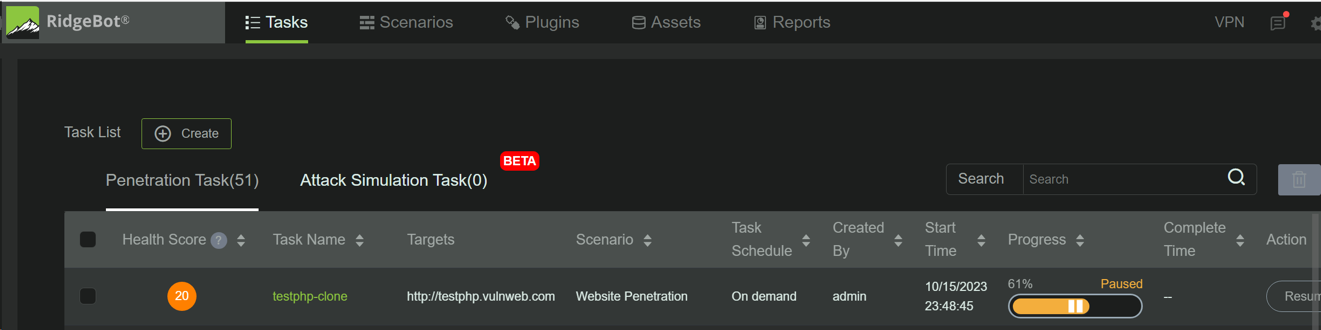
1. This action will open up the popup and ask for the user confirmation.



1. If the user clicks “**Yes**” then the selected tasks will be “PAUSED” in RidgeBot server as well as in ePO server.



**Note**: If the Pause operation fails then this action will show “**Error While Pausing Task.**” message.



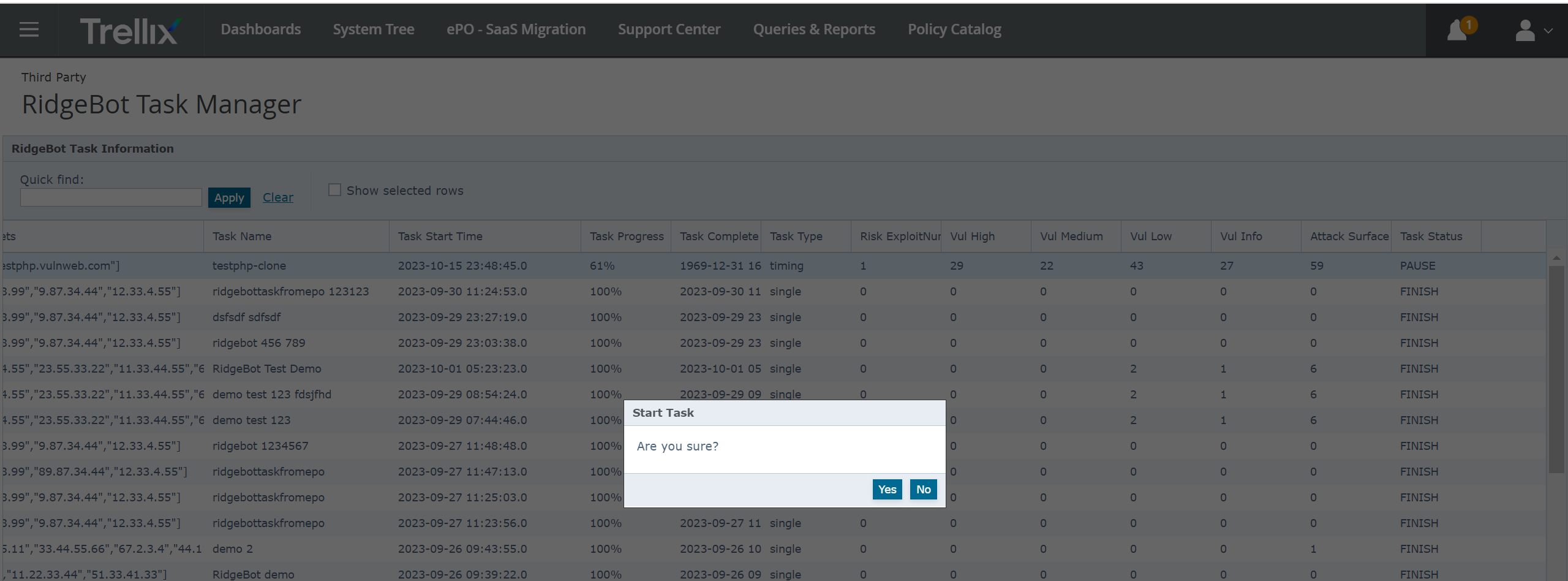
### Start (Resume) RidgeBot Task:

1. The Start Task action will allow the user to Resume a RidgeBot task from ePO UI.
2. Goto **Menu | Third Party | RidgeBot Task Manager** Tab.
3. Select one tasks which is in “PAUSED” state by clicking the check box and click **Actions | Start Task** option.

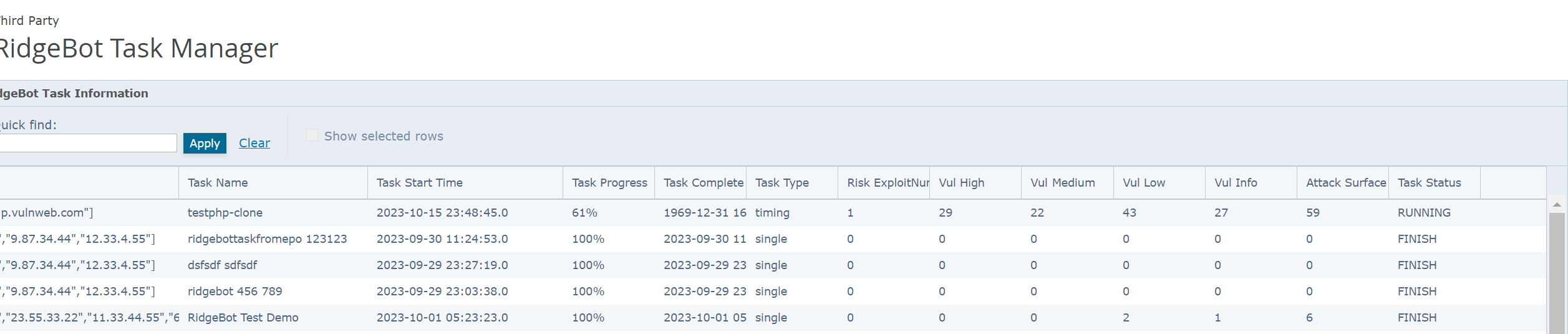
**Note:** The “Start Task” option applicable only for the task with “PAUSE” as status.

**API URL:** **https://<RidgeBot\_IPADDR>/api/v4/tasks/start**

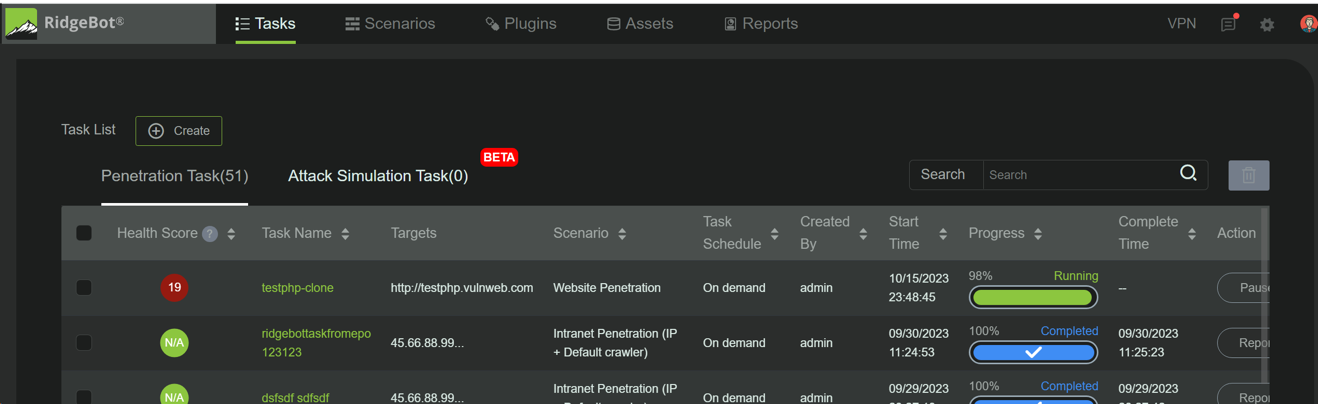
1. This action will open up the popup and ask for the user confirmation.



1. If the user clicks “**Yes**” then the selected tasks will be resumed and its status will change from “PAUSED” to “RUNNING” in RidgeBot server as well as in ePO server.



**Note**: If the Start operation fails then this action will show “**Error While Starting Task.**” message.



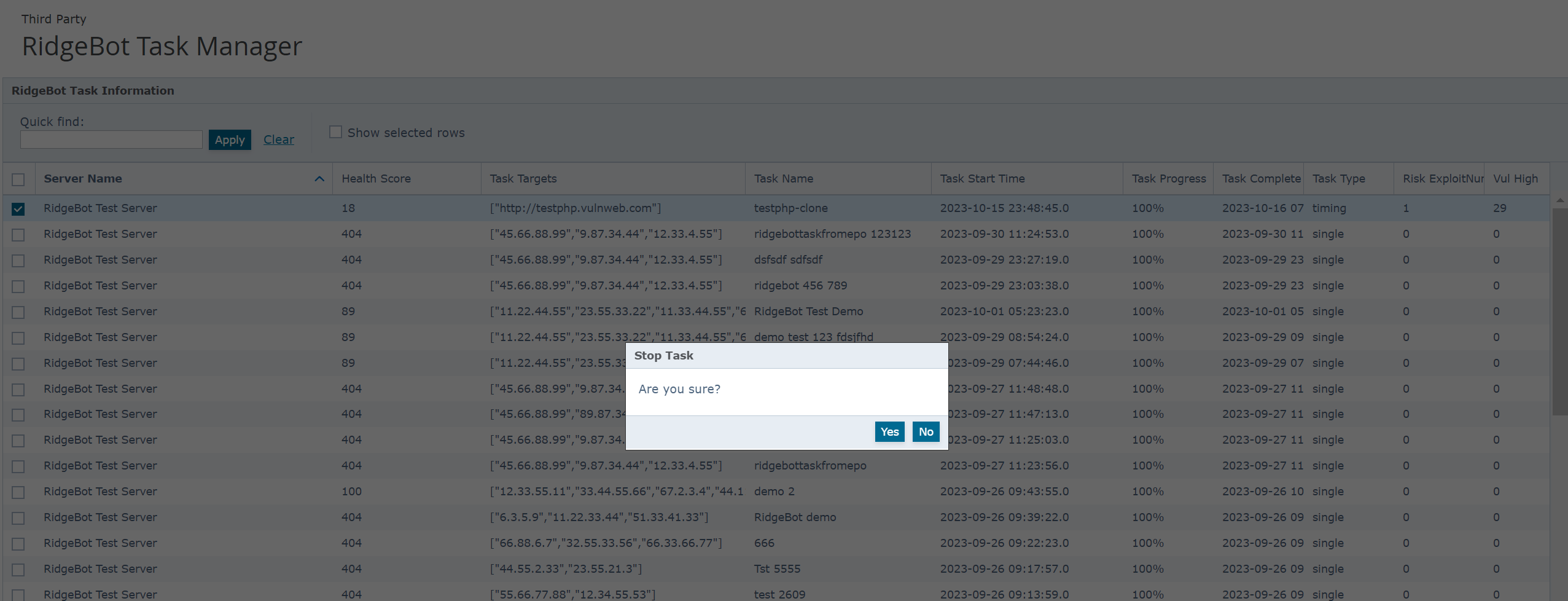
### Stop (Cancel) RidgeBot Task:

1. The Stop Task action will allow the user to Stop (Cancel) a RidgeBot task from ePO UI.
2. Goto **Menu | Third Party | RidgeBot Task Manager** Tab.
3. Select one tasks by clicking the check box and click **Actions | Stop Task** option.

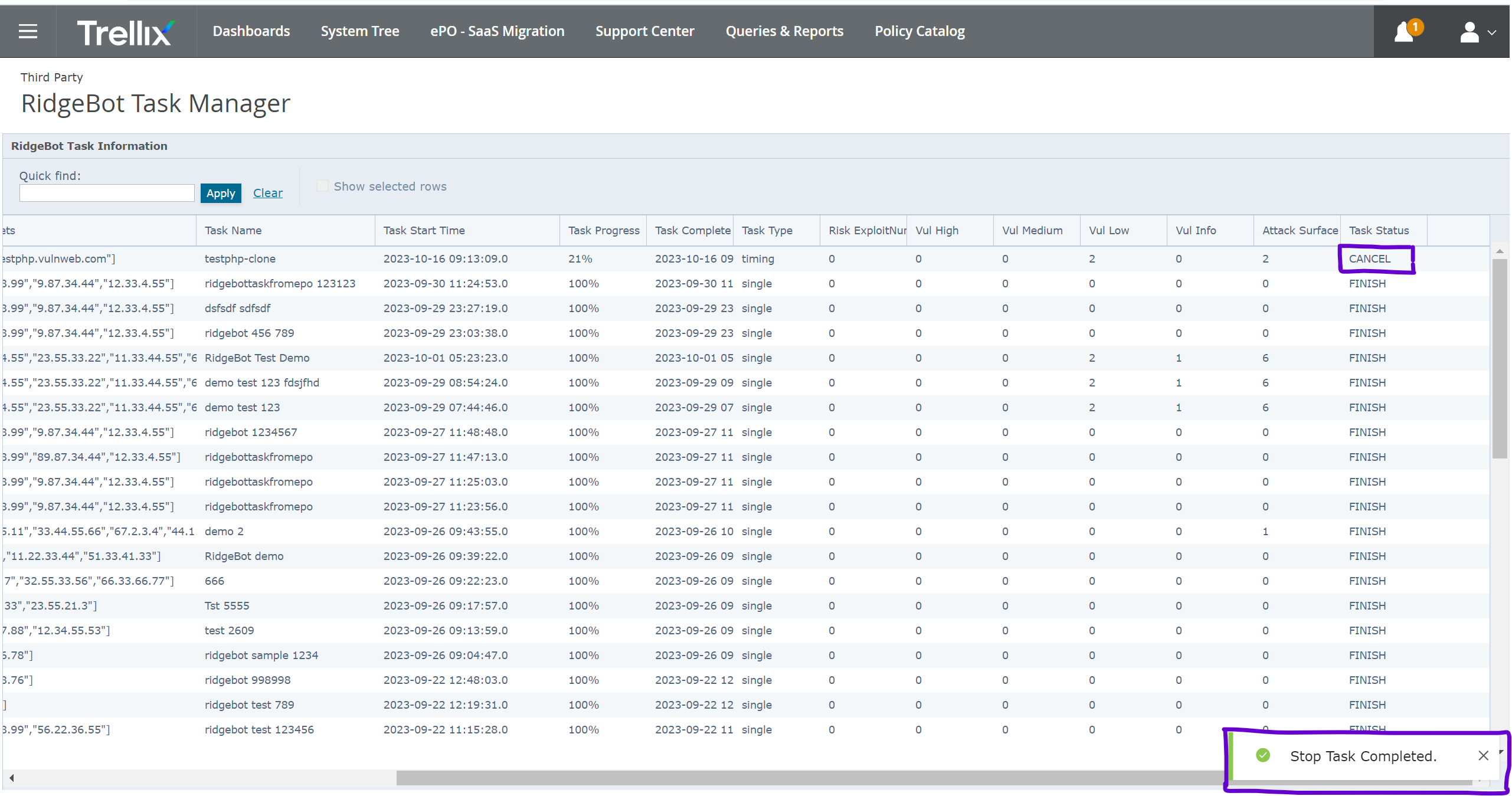
**Note:** The “Stop Task” option applicable only for the task with “RUNNING” as status.

**API URL:** **https://<RidgeBot\_IPADDR>/api/v4/tasks/stop**

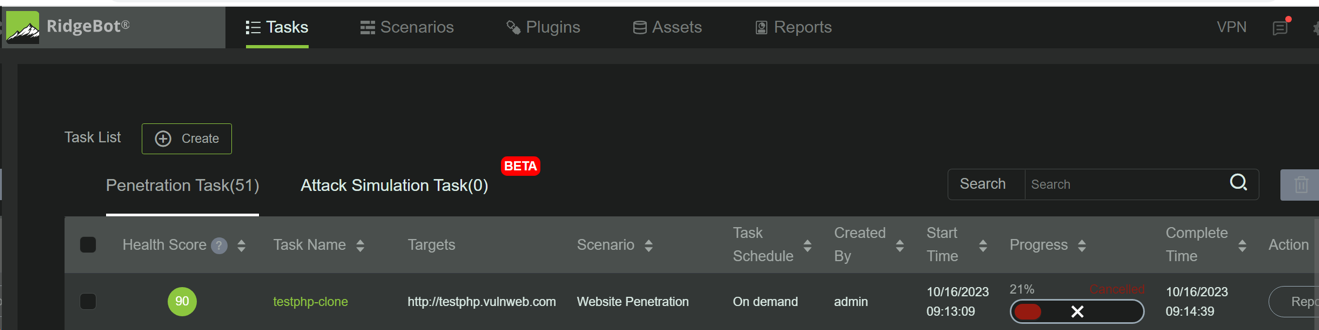
1. This action will open up the popup and ask for the user confirmation.



1. If the user clicks “**Yes**” then the selected tasks will be “CANCEL” in both ePO server and RidgeBot server.



**Note**: If the Stop operation fails then this action will show “**Error While Stopping Task.**” message.



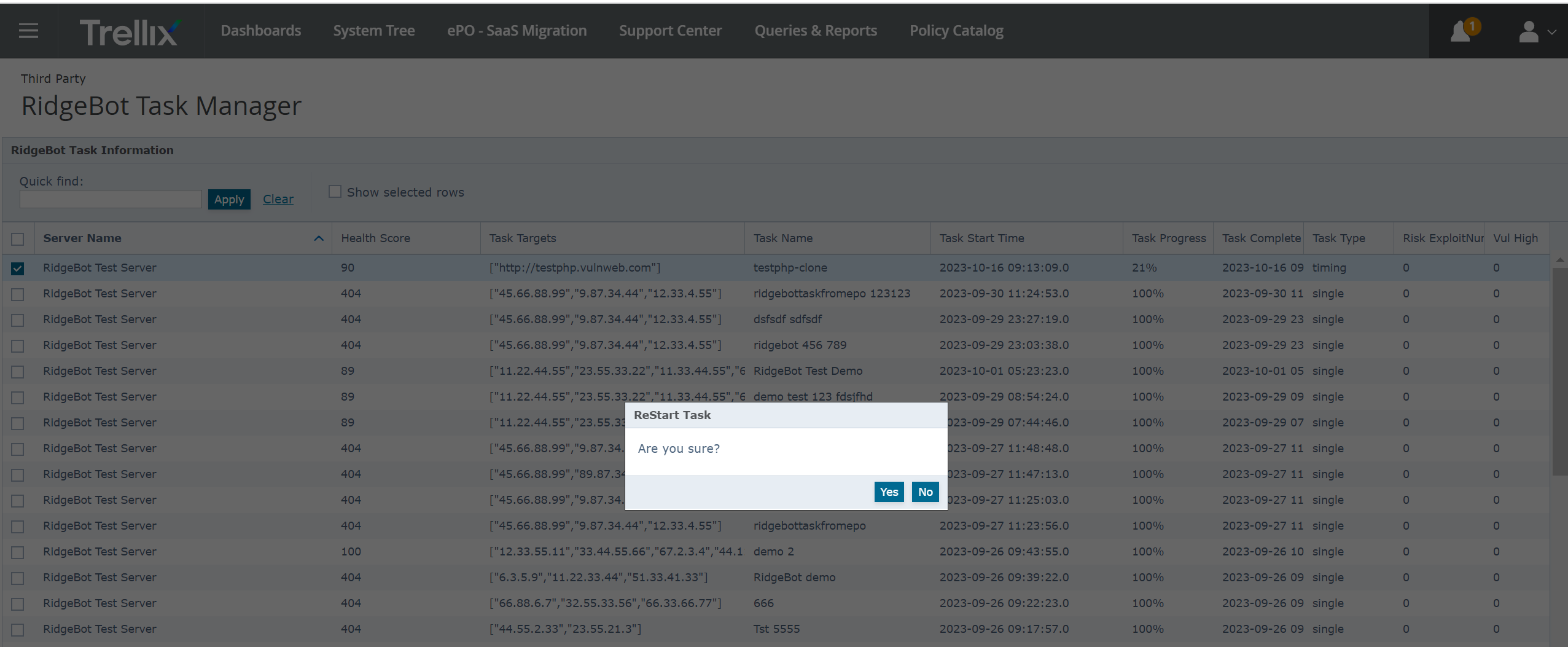
### ReStart RidgeBot Task:

1. The ReStart Task action will allow the user to Restart a RidgeBot task from ePO UI.
2. Goto **Menu | Third Party | RidgeBot Task Manager** Tab.
3. Select one or more than tasks by selecting the check box and click **Actions | ReStart Task** option.

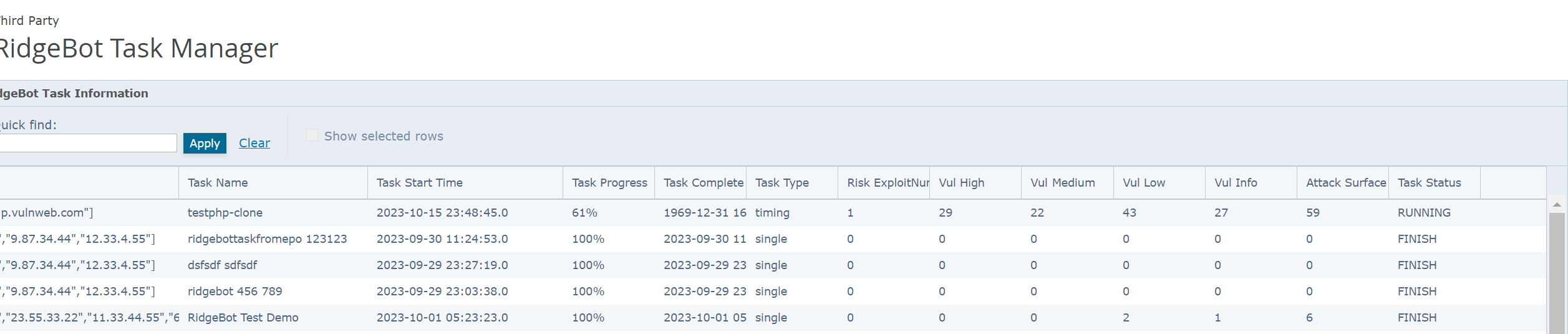
**Note:** The “ReStart Task” option applicable for the task with “PAUSE”, “CANCEL” and “FINISH” as status. This action will not work for the task with “RUNNING” as status.

**API URL:** **https://<RidgeBot\_IPADDR>/api/v4/tasks/restart**

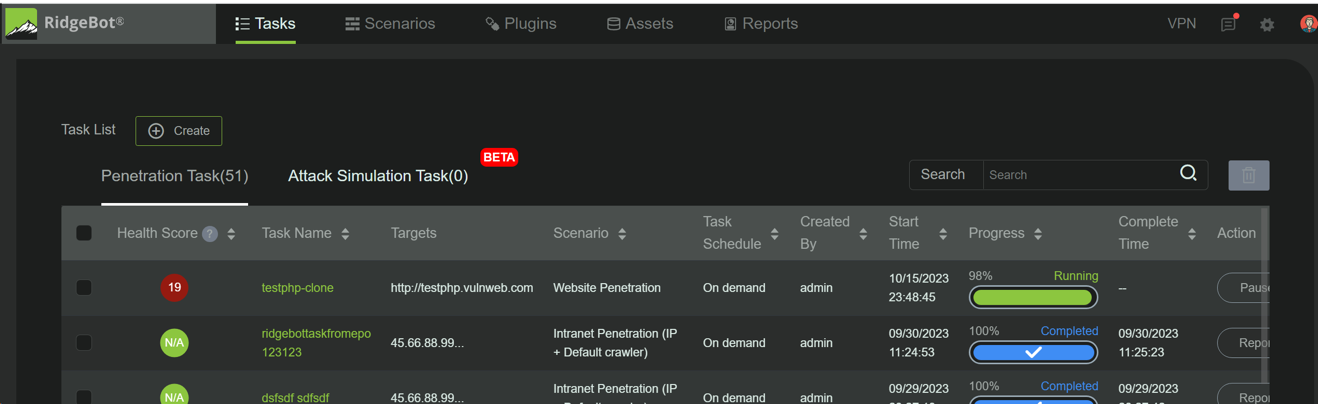
1. This action will open up the popup and ask for the user confirmation.



1. If the user clicks “**Yes**” then the selected tasks will be “RUNNING” in RidgeBot server as well as in ePO server.

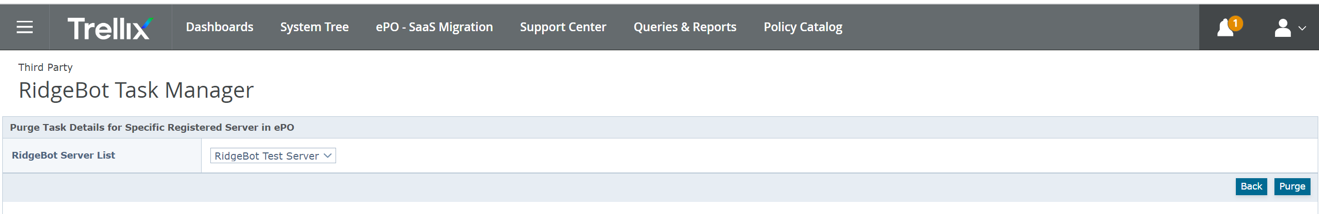


**Note**: If the ReStart operation fails then this action will show “**Error While ReStarting Task.**” message.



### Purge Data:

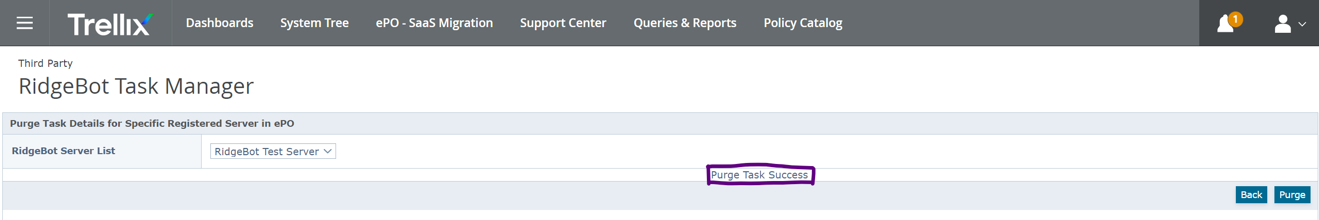
1. The purge data action can be used to delete the task data only from ePO server, that are pulled by specific registered server of RidgeBot. This action can be used to delete the stale task from **RidgeBotTaskInfo** and **RidgeBotStatistics** table in ePO server database.
2. Goto **Menu | Third Party | RidgeBot Task Manager | Actions** and click “**Purge data**” action.
3. This will open a new UI page where user have to provide the required details to create a task. Refer the below screenshot.



In this UI,

**RidgeBot Server List:** the registerd server instance name from which the RidgeBot tasks are pulled.

1. Once the information provided, then click on “**Purge**” button to delete the task data from ePO server. The status (Success (or) Failure) will be shown on the UI. Refer the below screenshot.



**Note:** The “**Back**” button in this page will take the user back to **Menu | Third Party | RidgeBot Task Manager** page.

1. Once the purge data action is success, the RidgeBot task data pulled from the selected registered server will be removed and the same should be reflected in the **Menu | Third Party | RidgeBot Task Manager** page.

# Testing the Integration

## Deploying Partner Agents to an Endpoint

N/A

### Manual Partner Agent Deployment Options

N/A

### Event Reporting through Common Event XML

N/A

### Policy Enforcement

N/A

### Task Enforcement

N/A

## Verifying Agent deployment from ePO

N/A

# Uninstalling ePO Integration

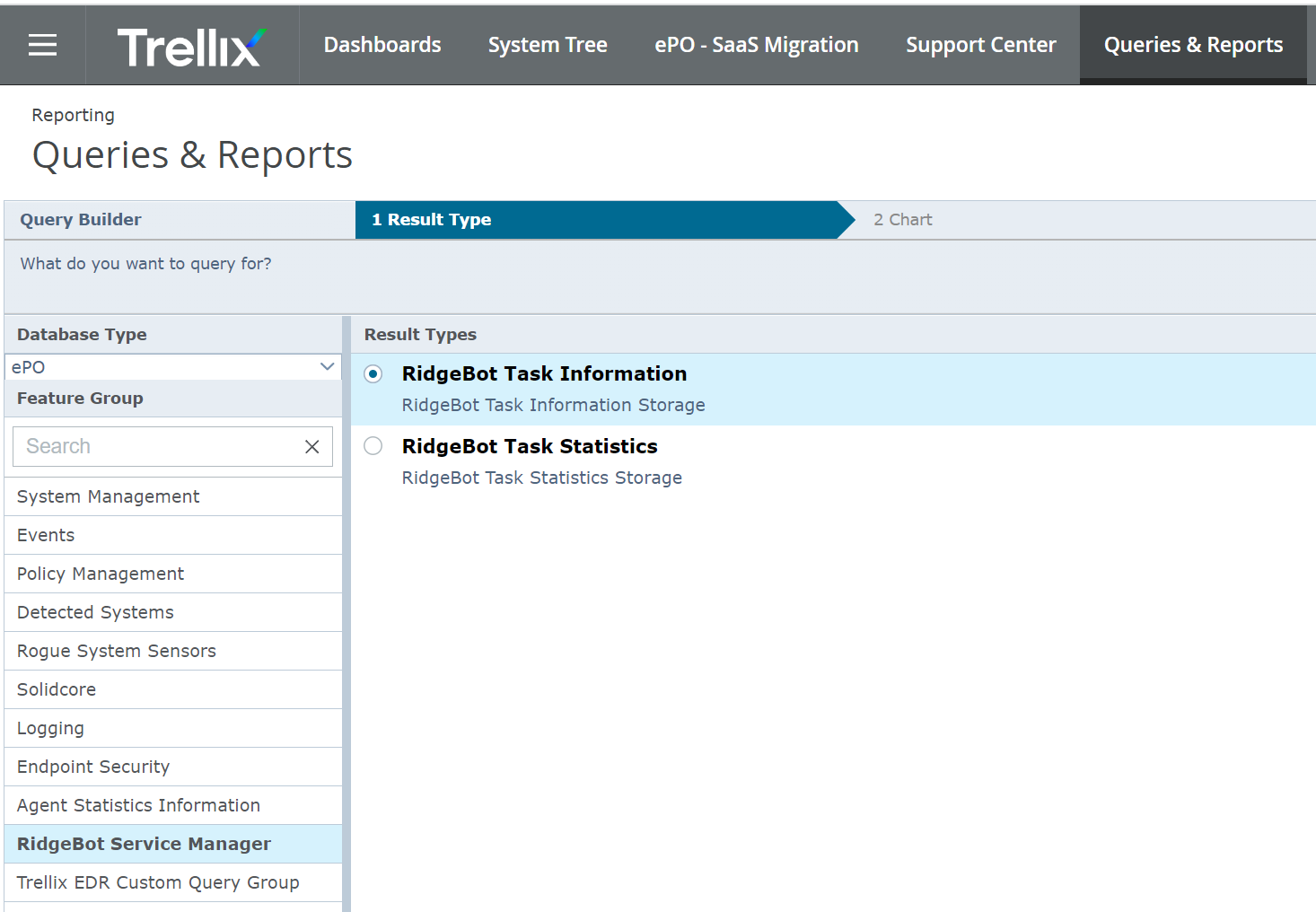
RidgeBot ePO integration can be uninstalled by removing “**RidgeBot Service Manager**” extension from ePO server. Go to **Menu | Extensions | RidgeBot Service Manager** andclick **Remove** link to uninstall the extension.

# Reporting

## Query Targets

As part of RidgeBot integration we are creating two query targets in ePO server, they are

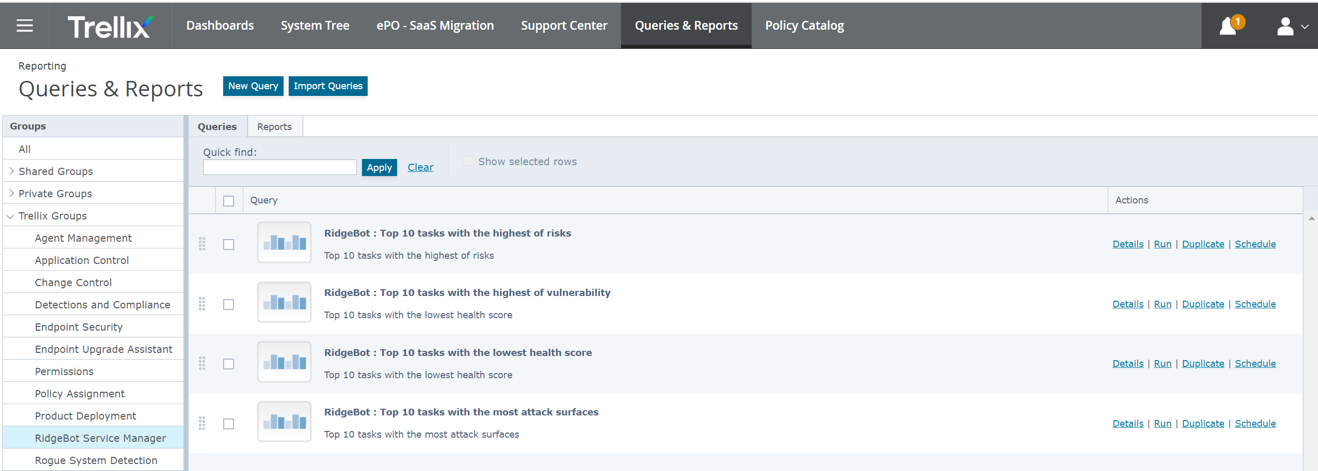
1. RidgeBot Task Information
2. RidgeBot Task Statistics



## Canned Queries

As part of RidgeBot integration we are creating four canned queries in ePO server, they are

1. RidgeBot: Top 10 tasks with the lowest health score
2. RidgeBot: Top 10 tasks with the most attack surfaces
3. RidgeBot: Top 10 tasks with the highest of risks
4. RidgeBot: Top 10 tasks with the highest of vulnerability



## Custom Tables

As part of RidgeBot integration we are creating two custom tables to store RidgeBot task details in ePO server.

1. RidgeBotTaskInfo
2. RidgeBotStatistics

**Table Schema:**

IF NOT EXISTS

(

SELECT \* FROM sys.objects

WHERE object\_id = OBJECT\_ID(N'[dbo].[RidgeBotTaskInfo]')

AND type in (N'U')

)

BEGIN

CREATE TABLE [dbo].[RidgeBotTaskInfo] (

[AutoId] [bigint] NOT NULL PRIMARY KEY IDENTITY(1,1),

[TaskId][nvarchar] (256) NOT NULL,

[ServerName][nvarchar] (1024) NOT NULL,

[ServerId][int] NOT NULL,

[TaskJobTotal] [int],

[TaskDetectType] [nvarchar] (256),

[TaskJobCounts] [int],

[TaskSummary] [nvarchar] (512),

[TaskName][nvarchar] (512) NOT NULL,

[TaskTargets][nvarchar] (max) NOT NULL,

[TaskNodes][nvarchar] (max),

[TaskStartTime][nvarchar] (256),

[TaskProgress][nvarchar] (256) NOT NULL,

[TaskStatus][nvarchar] (256) NOT NULL,

[TaskCompleteTime][nvarchar] (256),

[TaskType] [nvarchar] (512)

--CONSTRAINT PK\_RidgeBotTaskInfo PRIMARY KEY(TaskId,ServerName)

) ON [PRIMARY]

END

GO

IF NOT EXISTS

(

SELECT \* FROM sys.objects

WHERE object\_id = OBJECT\_ID(N'[dbo].[RidgeBotStatistics]')

AND type in (N'U')

)

BEGIN

CREATE TABLE [dbo].[RidgeBotStatistics] (

[AutoId] [bigint] NOT NULL PRIMARY KEY IDENTITY(1,1),

[TaskId] [nvarchar] (256) NOT NULL,

[ServerName] [nvarchar] (1024) NOT NULL,

[ServerId][int] NOT NULL,

[SecurityHttpsRatio] [int],

[SecurityVulTransform] [int],

[SecurityAttackSurfaceDensity] [int],

[SecurityRiskTransform] [int],

[SecuritySafetyIndex] [int] , -- This will be the health score for the task

[SecurityAliveRatio] [int],

[SecurityVulTypeCoverageRatio] [int],

[TaskExploitCount] [int],

[TaskDigCount] [int],

[TaskScanCount] [int],

[RiskCredentialsNum] [int],

[RiskPenetrationNum] [int],

[RiskInfiltratedAssetsNum] [int],

[RiskExploitNum] [int],

[RiskCodeNum] [int],

[RiskNumber] [int],

[RiskShellNum] [int],

[RiskDatabaseNum] [int],

[ChainSensitiveAttackAverage] [int],

[ChainVulAttackAverage] [int],

[VulNumber] [int],

[VulInfo] [int],

[VulTypeNumber] [int],

[VulHigh] [int],

[VulMedium] [int],

[VulLow] [int],

[AttackIpAliveNum] [int],

[AttackIpAsstesNum] [int],

[AttackIpUnaliveNum] [int],

[AttackSiteAsstesNum] [int],

[AttackSiteAliveNum] [int],

[AttackSiteUnaliveNum] [int],

[AttackAsstesNum] [int],

[AttackSurfaceNum] [int]

--CONSTRAINT FK\_RidgeBotStatistics FOREIGN KEY (TaskId, ServerName)

--REFERENCES RidgeBotTaskInfo (TaskId, ServerName)

--ON DELETE CASCADE

--ON UPDATE CASCADE

)

END

GO

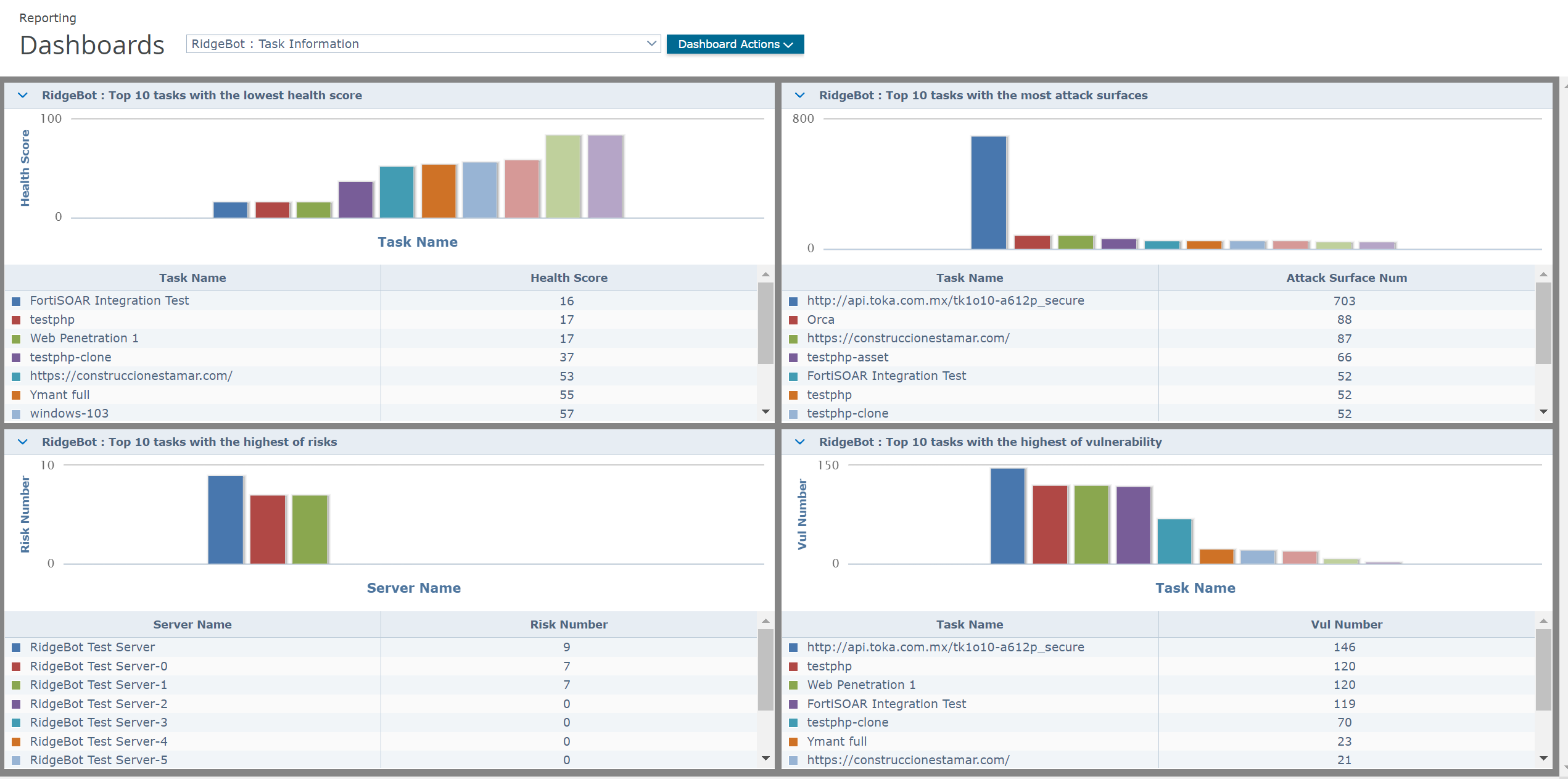
## Dashboards

As part of RidgeBot integration we are creating only one dashboard and it will contain four monitors,

Dashboard Name: **RidgeBot: Task Information**

Dashboard Monitors:

1. RidgeBot: Top 10 tasks with the lowest health score
2. RidgeBot: Top 10 tasks with the most attack surfaces
3. RidgeBot: Top 10 tasks with the highest of risks
4. RidgeBot: Top 10 tasks with the highest of vulnerability



# Appendix A. Logs and Troubleshooting

## Troubleshooting

< In this section, specify the troubleshooting options in case of deployment problems, event mishandling etc. This will also contain known defects / issues that are encountered by the partner during the testing done at the Partner’s end and how to avoid / overcome them.>

## Useful Logs

The RidgeBot server extension in ePO sever will write debug logs into ePO’s orion.log file. Any error (or) exception occurs in RidgeBot extension will be logged into ePO server’s orion.log file as debug log.

## Known Issues

The status and progress inforamtion of running, passued and cancled task will not reflect in real time in ePO, because the RidgeBot task infoatmion is pulled by ePO server task and it runs periodically, hence there might be a delay/mismatch in task progress and task status.

**Note:** To update the RidgeBot task details in ePO, user must run the **Menu | Automation | Server Tasks** | “**RidgeBot Task**” manually which pulls the task data from RidgeBot server and update the same in ePO. Please refer section “[**Steps to Configure RidgeBot Registered Server**](#_Steps_to_Configure)” for better understanding.