

opensight - intune appstate prtg sensor

Monitor intune application installation states in prtg

Content

- [opensight - intune appstate prtg sensor](#)
- [Content](#)
 - [Script Features](#)
 - [Prerequisites](#)
 - [PRTG Probe Configuration](#)
 - [Microsoft Azure Configurations](#)
 - [Installation](#)
 - [PRTG](#)
 - [Script Parameters](#)
 - [Manual Testing](#)
 - [Some more examples](#)

Script Features

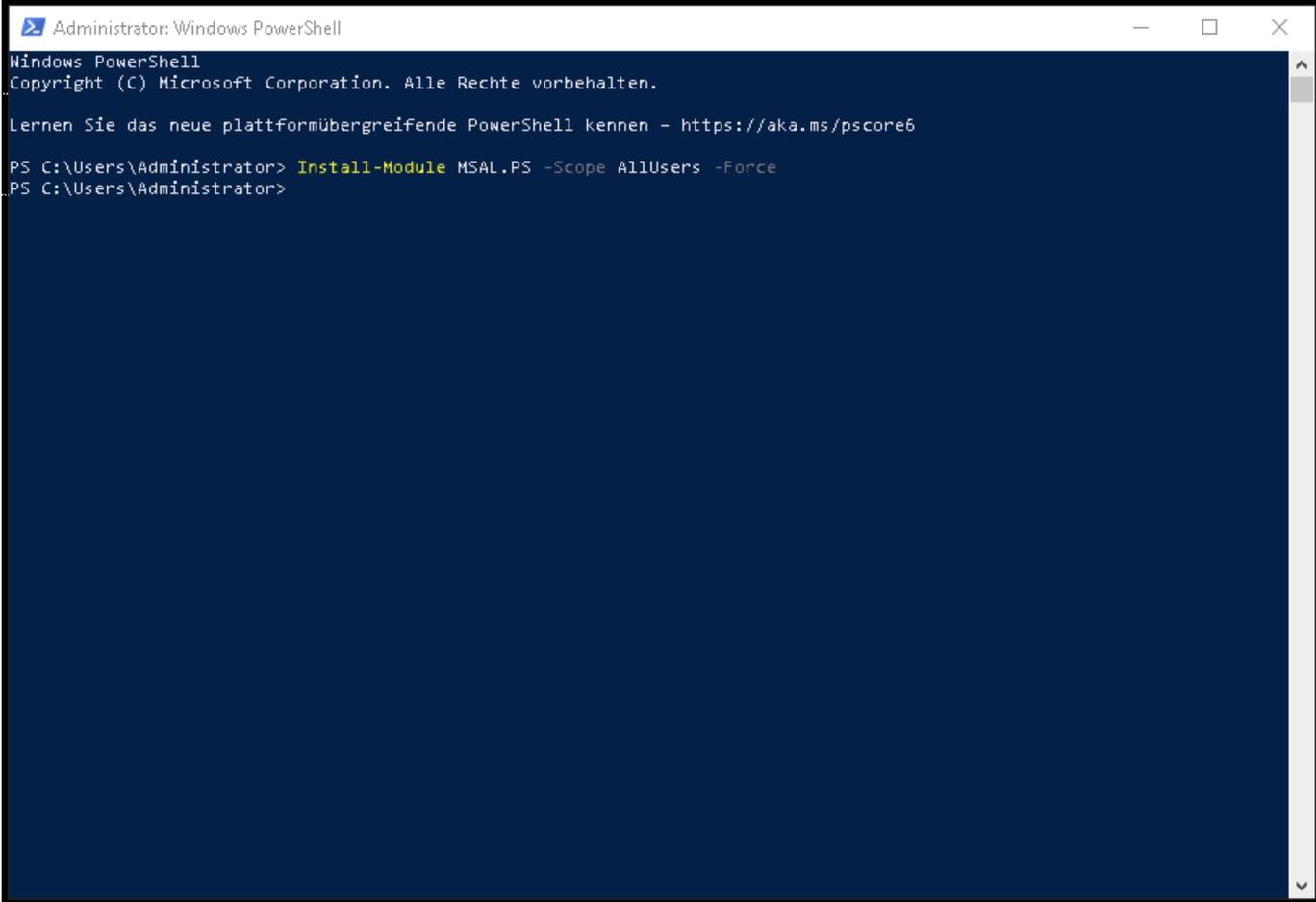
- Authentication with an Azure Service Principal
- List all application install states

Prerequisites

PRTG Probe Configuration

- On the machine, where the sensor script will run (aka the prtg probe), install the msal.ps module. (microsoft authentication library)

```
Install-Module MSAL.PS -Scope AllUsers -Force
```



```
Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) Microsoft Corporation. Alle Rechte vorbehalten.

Lernen Sie das neue plattformübergreifende PowerShell kennen - https://aka.ms/powershell6

PS C:\Users\Administrator> Install-Module MSAL.PS -Scope AllUsers -Force
PS C:\Users\Administrator>
```

Also make sure that running scripts is actually possible. Open the **32-bit / x86** version of powershell. Set The ExecutionPolicy

```
set-executionpolicy unrestricted -Scope LocalMachine
```

```
Administrator: Windows PowerShell (x86)
Windows PowerShell
Copyright (C) Microsoft Corporation. Alle Rechte vorbehalten.

Lernen Sie das neue plattformübergreifende PowerShell kennen - https://aka.ms/pscore6

PS C:\Users\Administrator> Get-ExecutionPolicy -list

Scope ExecutionPolicy
-----
MachinePolicy      Undefined
UserPolicy         Undefined
Process           Undefined
CurrentUser       Undefined
LocalMachine      Undefined

PS C:\Users\Administrator> Set-ExecutionPolicy unrestricted -Scope LocalMachine

Ausführungsrichtlinie ändern
Die Ausführungsrichtlinie trägt zum Schutz vor nicht vertrauenswürdigen Skripten bei. Wenn Sie die Ausführungsrichtlinie
ändern, sind Sie möglicherweise den im Hilfethema "about_Execution_Policies" unter
"https://go.microsoft.com/fwlink/?LinkID=135170" beschriebenen Sicherheitsrisiken ausgesetzt. Möchten Sie die
Ausführungsrichtlinie ändern?
[?] Ja [A] Ja, alle [N] Nein [K] Nein, keine [H] Anhalten [?] Hilfe (Standard ist "N"): a
PS C:\Users\Administrator>
```

Microsoft Azure Configurations

First create a new app registration in intune (service principal)

Microsoft Azure Search resources, services, and docs (G+)

Home > opensight.ch | App registrations >

Register an application

*** Name**
The user-facing display name for this application (this can be changed later).

prtq-senso

Supported account types
Who can use this application or access this API?

- Accounts in this organizational directory only (opensight.ch only - Single tenant)
- Accounts in any organizational directory (Any Azure AD directory - Multitenant)
- Accounts in any organizational directory (Any Azure AD directory - Multitenant) and personal Microsoft accounts (e.g. Skype, Xbox)
- Personal Microsoft accounts only

[Help me choose...](#)

Redirect URI (optional)
We'll return the authentication response to this URI after successfully authenticating the user. Providing this now is optional and it can be changed later, but a value is required for most authentication scenarios.

Select a platform e.g. https://example.com/auth

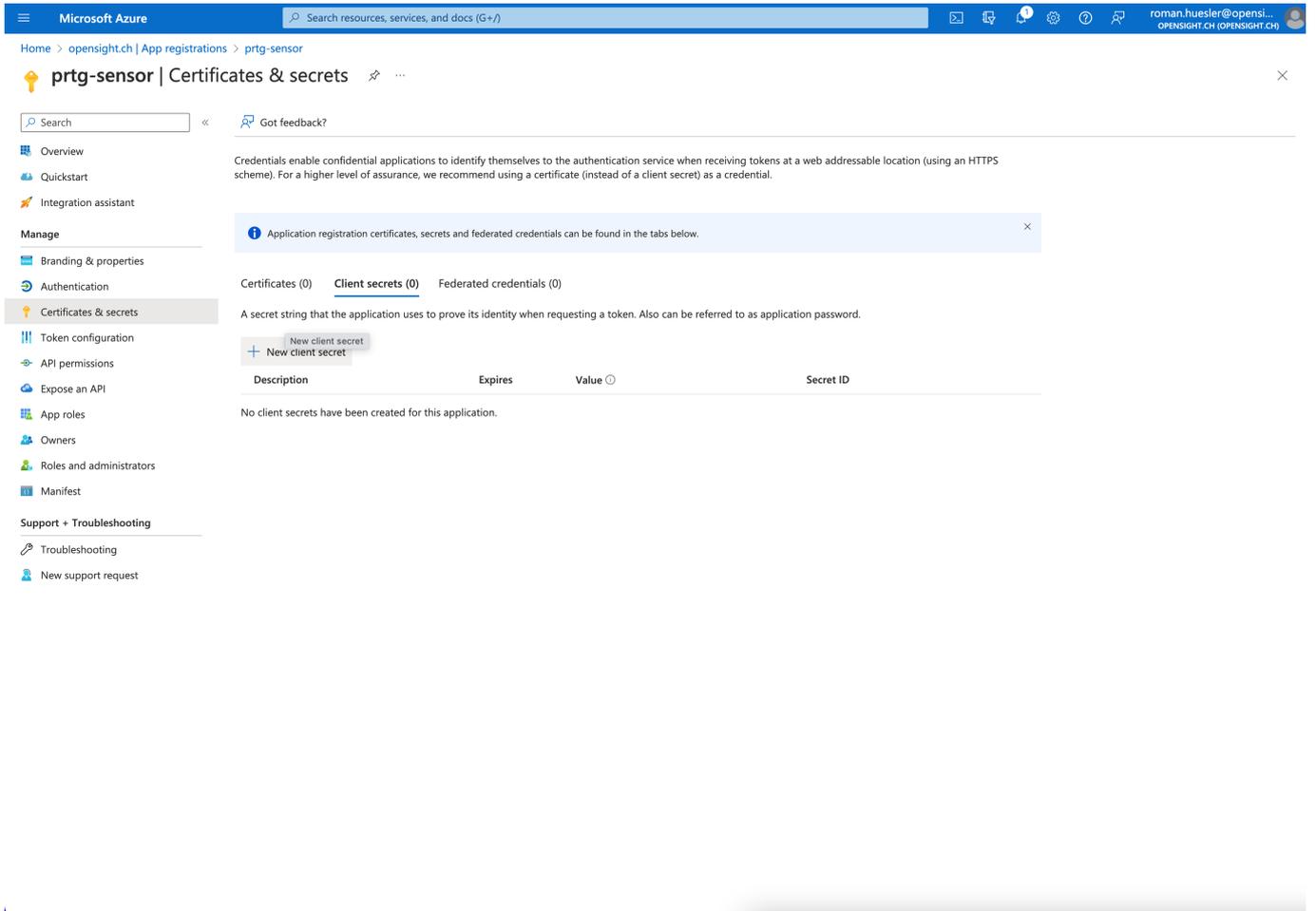
Register an app you're working on here. Integrate gallery apps and other apps from outside your organization by adding from [Enterprise applications](#).

By proceeding, you agree to the [Microsoft Platform Policies](#)

Register

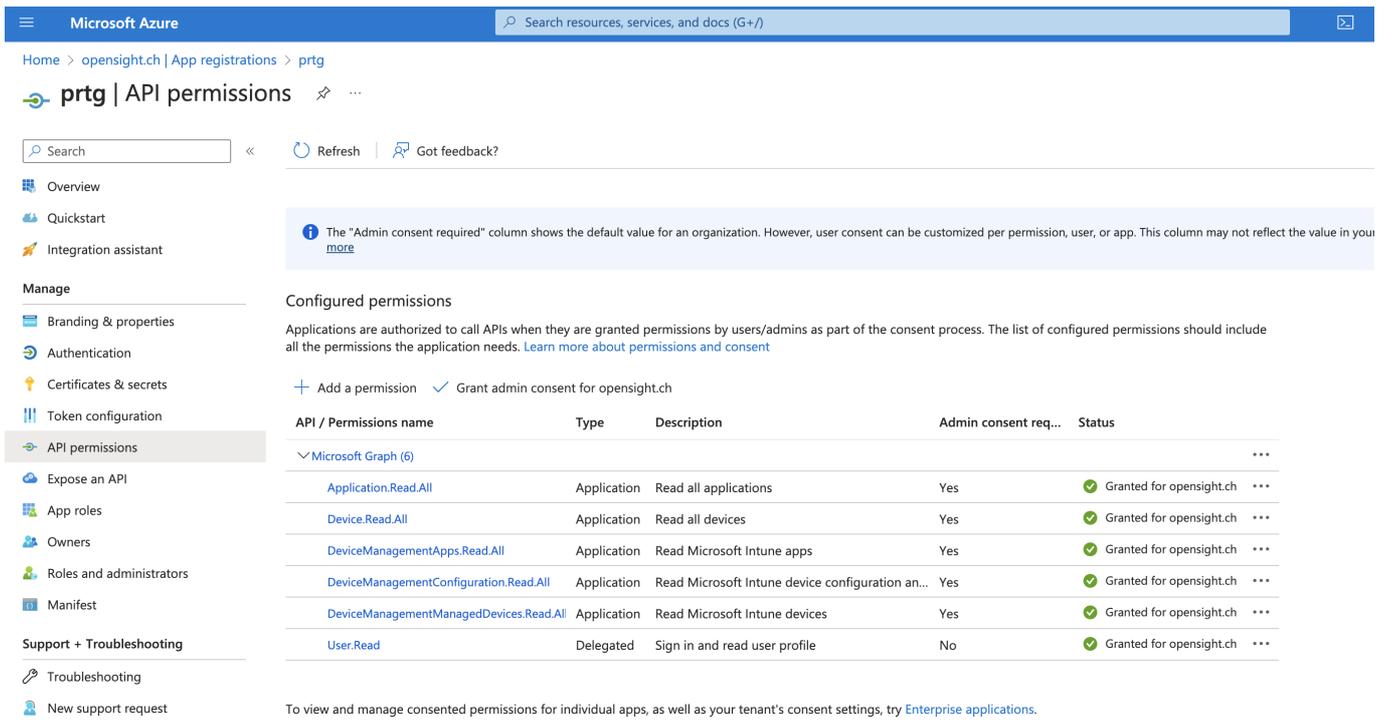
- Make note of the application id (script parameter -app_id)
- Make note of the tenant id (script parameter -tenant_id)

Create a new client secret in the app registration



- Make note of the secret value (script parameter -client_secret)

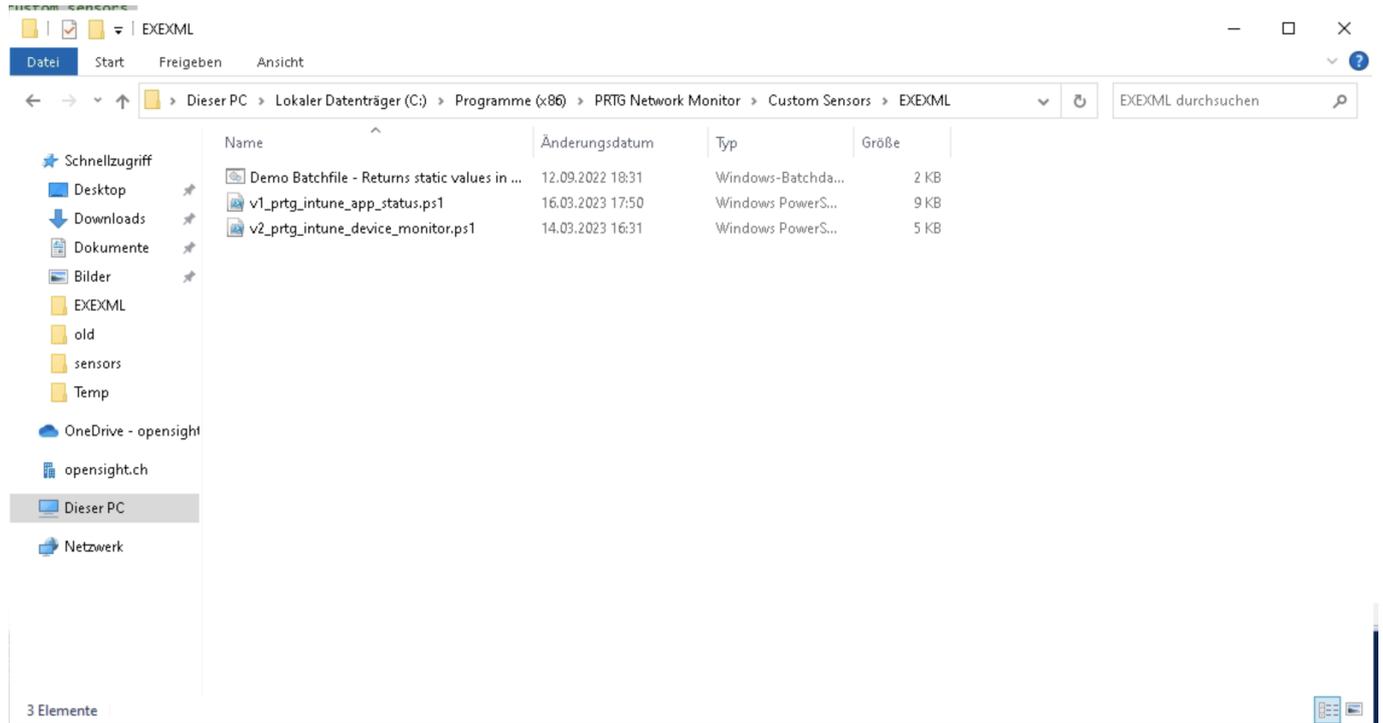
Grant the required permissions and give admin consent



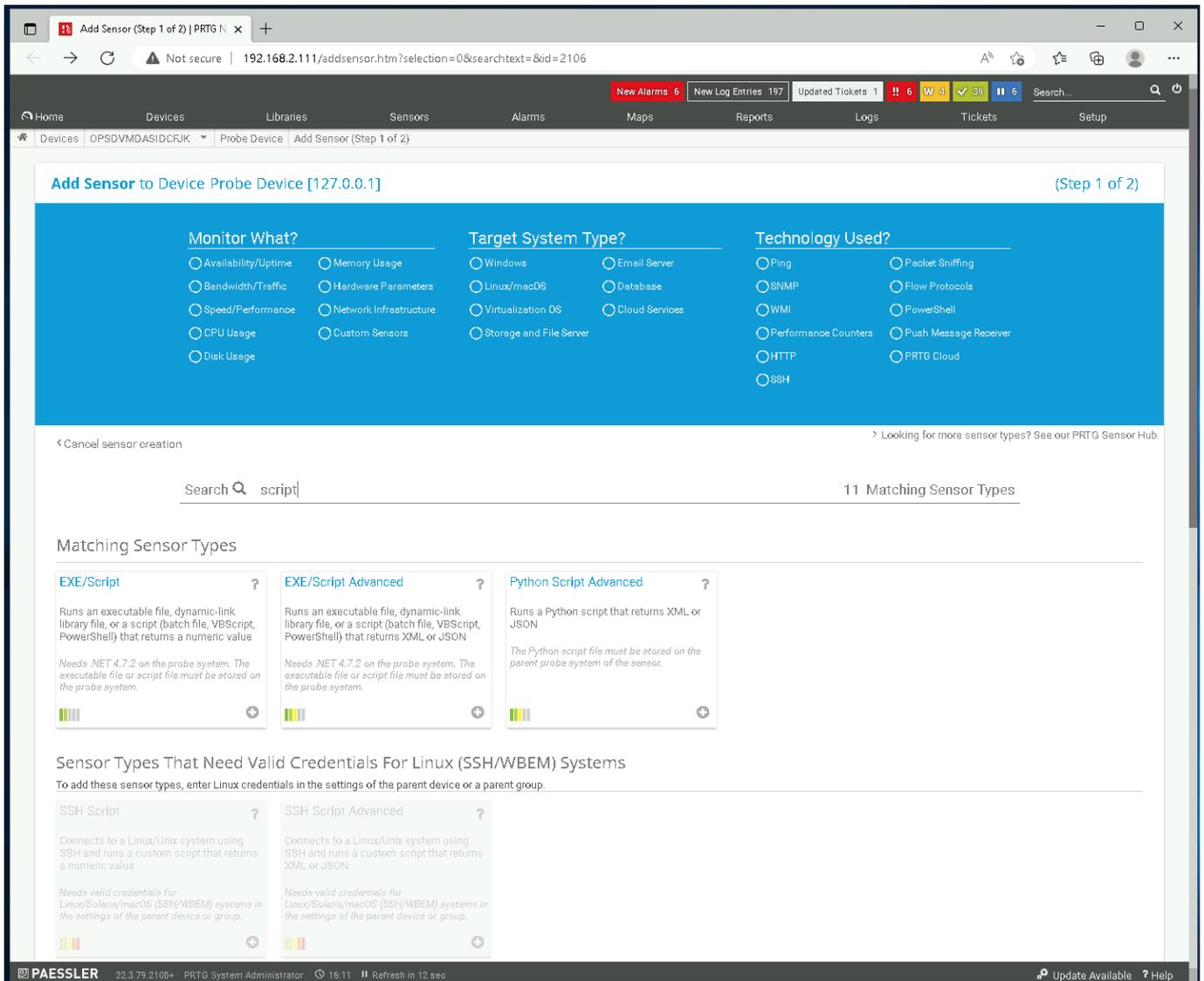
Installation

PRTG

Put the sensor in the right location on the prtg probe in the EXEXML folder



In PRTG create a new EXE/advanced probe



Script Parameters

Add the parameters that were noted above to the sensor configuration. Use **single quotes**

- app_id
- tenant_id
- client_secret

Then you can also use the 2 parameters:

- states
filter the device states that you like to show in prtg with this parameter. you can use "total;all;installed;failed;notInstalled;uninstallFailed;pendingInstall;unknown;notApplicable"
 - total
show the total of all states (example: 2 "installed" plus 3 "failed" plus 0 "unkown" etc result in a total of 5)
 - all
just show all states in prtg (installed, failed, ...)
 - installed;failed
just show installed or failed packages in prtg

- softwarenames

filter the software that you like to show in prtg

- o overall

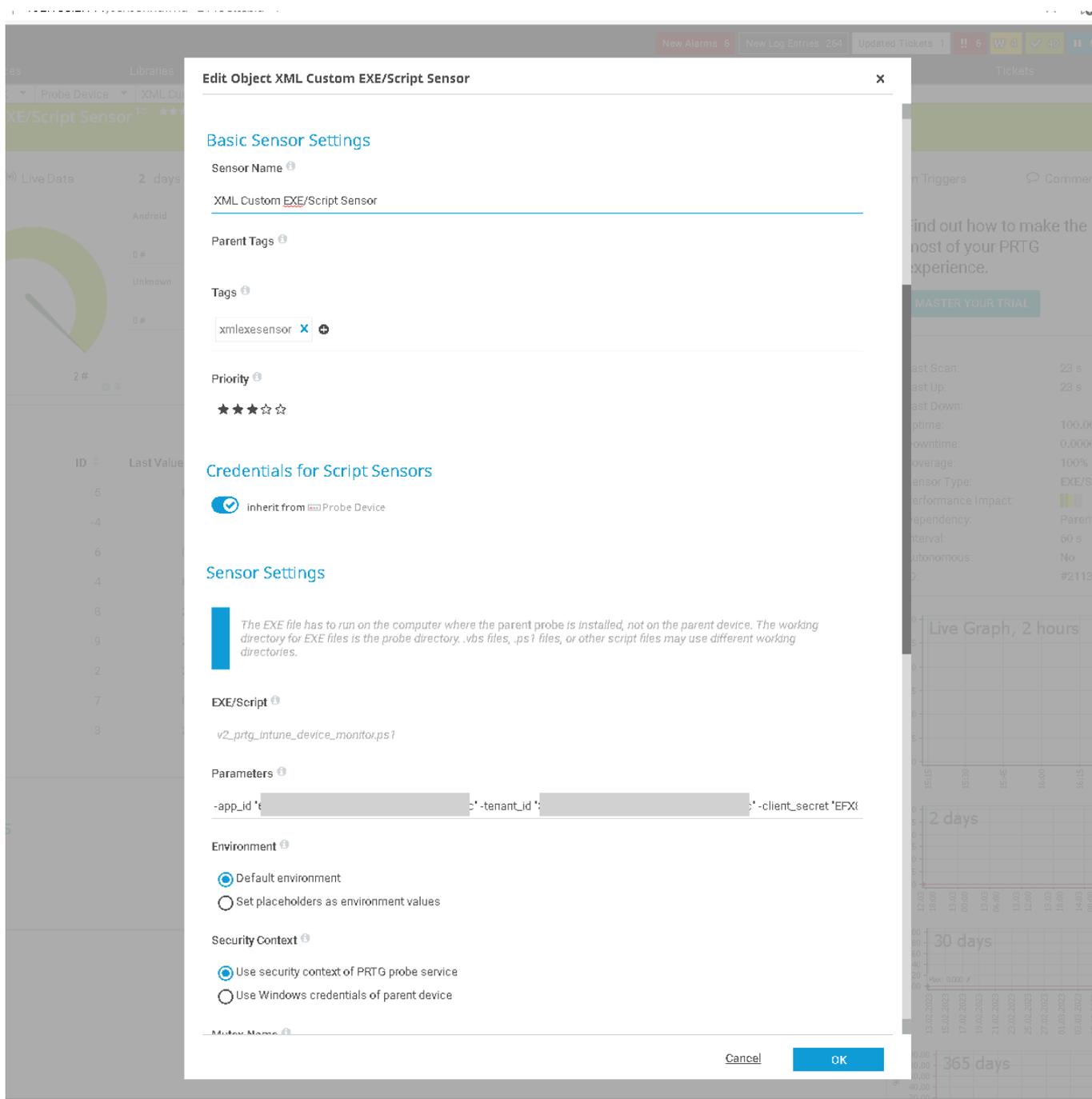
show overall stats in prtg. example: winscp has 2 "installed" and 7zip has 3 "installed". Results in overall 5 "installed"

- o all

show stats for all detected apps from intune in prtg.

- o winscp;7zip

show stats for winscp and 7zip in prtg



Manual Testing

On the PRTG Probe, you can also test the sensor manually. Just open a powershell and type

```
. "C:\Program Files (x86)\PRTG Network Monitor\Custom  
Sensors\EXEXML\v1_prtg_intune_app_status.ps1" -app_id 'xxx-xxx-xxx-xxx' -  
tenant_id 'xxx-xxx-xxx-xxx' -client_secret 'xxxxxxx'
```

Some more examples

all data

```
. "C:\Program Files (x86)\PRTG Network Monitor\Custom  
Sensors\EXEXML\v1_prtg_intune_app_status.ps1" `  
-app_id 'xxx-xxx-xxx-xxx' `  
-tenant_id 'xxx-xxx-xxx-xxx' `  
-client_secret 'xxxxxxx' `  
-states 'all' `  
-softwarenames 'all;overall'
```

all installed and failed for packages 7zip and winscp

```
. "C:\Program Files (x86)\PRTG Network Monitor\Custom  
Sensors\EXEXML\v1_prtg_intune_app_status.ps1" `  
-app_id 'xxx-xxx-xxx-xxx' `  
-tenant_id 'xxx-xxx-xxx-xxx' `  
-client_secret 'xxxxxxx' `  
-states 'installed;failed' `  
-softwarenames '7zip;winscp'
```

all failed installations for all apps

```
. "C:\Program Files (x86)\PRTG Network Monitor\Custom  
Sensors\EXEXML\v1_prtg_intune_app_status.ps1" `  
-app_id 'xxx-xxx-xxx-xxx' `  
-tenant_id 'xxx-xxx-xxx-xxx' `  
-client_secret 'xxxxxxx' `  
-states 'failed' `  
-softwarenames 'all'
```