



SecuPi Implementation for CyberArk PSM

Database access control and monitoring



SecuPi can extend CyberArk capability to provide enhanced monitoring and fine-grained access control for privileged users accessing databases, data warehouses, data lakes, and lake houses. SecuPi can provide the following benefits for Datastore privileged users:

- Activity monitoring Including logging access to all data
 - Classification of data (e.g. PII, PHI, PCI, email address)
 - Risk score for every data element
 - Full SQL or NoSQL command
 - Sample data returned
- Fine-grained access control
 - Restrict access to schema and tables
 - Restrict specific administrative operations (e.g. user management, drop table, alter schema, permissions, key management, etc.)
 - Restrict access to sensitive rows (e.g. VIP customers, employees who are customers)
 - Restrict access to sensitive columns (e.g. mask Social Security Number, partially mask credit card number, format preserving encryption for email address)
 - Restrict sensitive cells (e.g. nullify the credit score of employees who are customers)
- De-identification and Encryption
 - Encrypt using format preserving encryption credit card numbers
 - Change birthdate to a date in 5 years buckets
 - Replace the last 3 digits of a zip code with 0

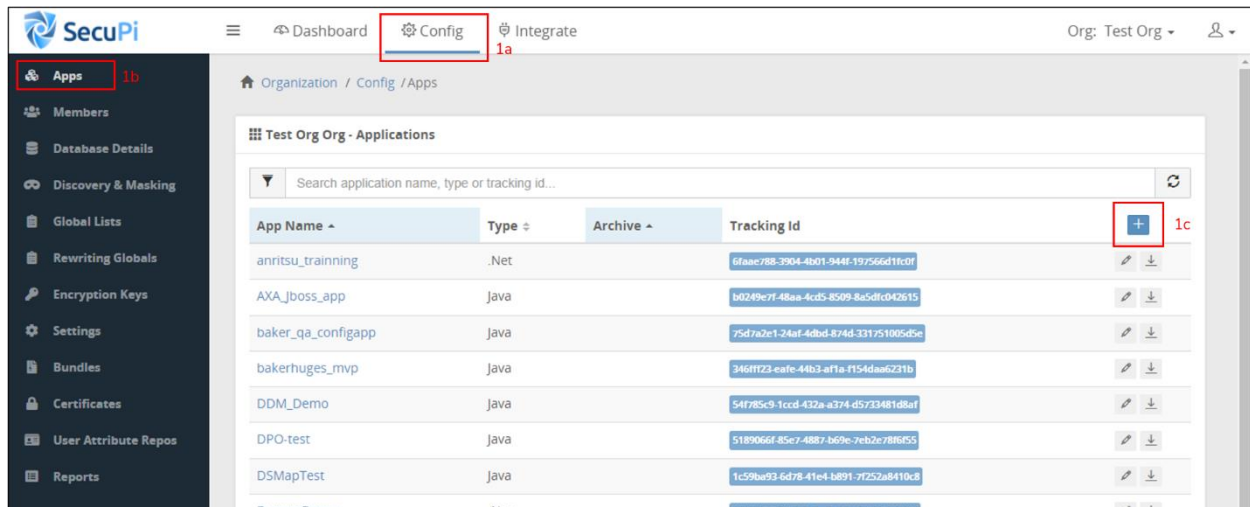
The SecuPi Integration with CyberArk is via the install of java and .NET enforcer on the CyberArk Privileged Session Manager (this document covers Windows only).

Please consult with your CyberArk Team to determine the optimal architecture for the integration. The executable should be installed exclusively on designated PSM Servers

Here is an example of how to integrate the Microsoft SQL Server Management Studio that is used to manage MS SQL database servers and Azure SQL.

SQL Server Management Studio (SSMS)

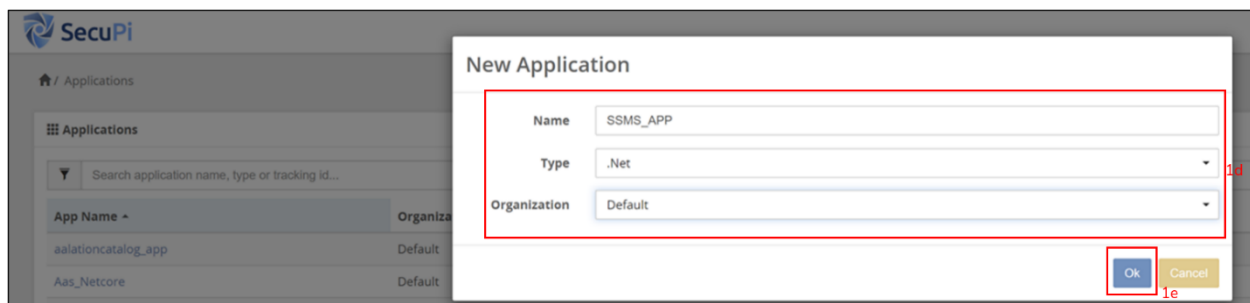
Select **Config** (1a) in the Organization top menu bar and then select **Apps** (1b) on the left hand side menu. To add a new application select **[+]** (1c).



Enter the New Application details, for example:

- **Name** - Test_APP
- **Type** - Select .Net
- **Organization** - Select Default

To save the new application details, select **Ok**.

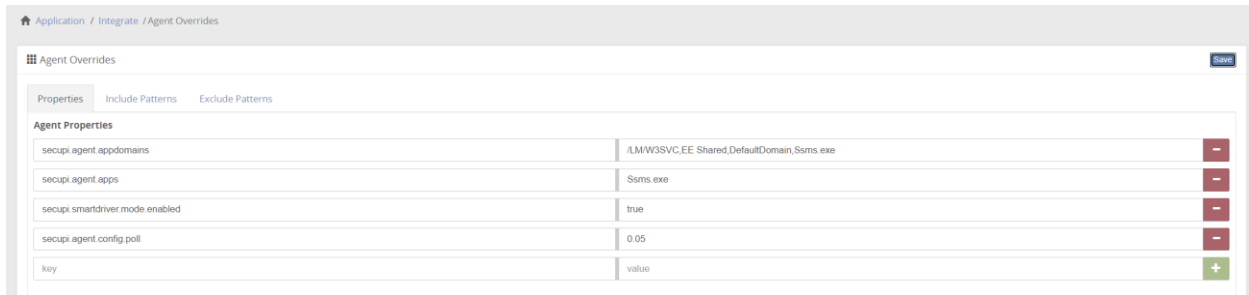


2. To integrate Agent Properties through Agent Overrides, select **Integrate** (2a) in the Application top menu bar and then select **Agent Overrides** (2b) on the left hand side menu.

To add Agent Properties, enter the required parameters and select the **[+]** logo (2c), then select **Save** (2d).

Agent Properties Parameters for SSMS :

- **Key** - secupi.agent.appdomains
- **Value** - /LM/W3SVC,EE Shared,DefaultDomain,Ssms.exe
- **Key** - secupi.agent.apps
- **Value** - Ssms.exe
- **Key** - secupi.smartdriver.mode.enabled
- **Value** - true
- **Key** - secupi.agent.config.poll
- **Value** - 0.05

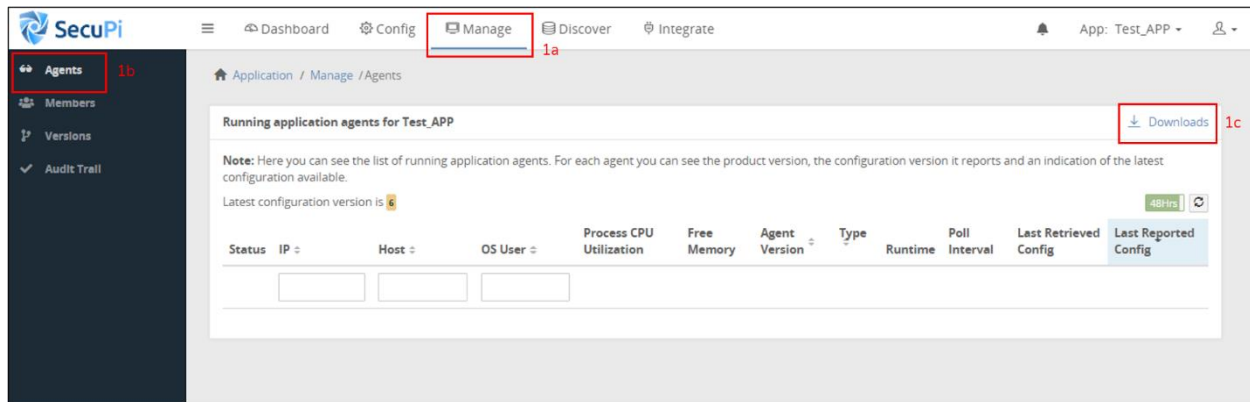


The screenshot shows the 'Agent Overrides' configuration page in the SecuPi application. The breadcrumb trail at the top is 'Application / Integrate / Agent Overrides'. The page has three tabs: 'Properties' (selected), 'Include Patterns', and 'Exclude Patterns'. Below the tabs is a table titled 'Agent Properties' with five rows. Each row has a 'key' column, a 'value' column, and a control icon (minus or plus) on the right. The rows are: 1. key: 'secupi.agent.appdomains', value: '/LM/W3SVC,EE Shared,DefaultDomain,Ssms.exe', icon: minus. 2. key: 'secupi.agent.apps', value: 'Ssms.exe', icon: minus. 3. key: 'secupi.smartdriver.mode.enabled', value: 'true', icon: minus. 4. key: 'secupi.agent.config.poll', value: '0.05', icon: minus. 5. key: 'key', value: 'value', icon: plus. A 'Save' button is located in the top right corner of the table area.

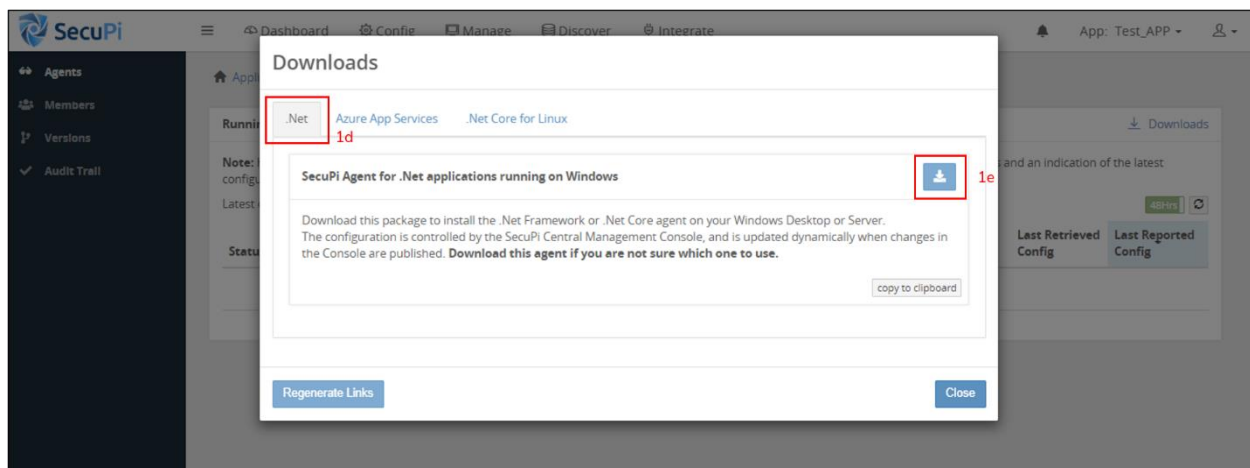
key	value	
secupi.agent.appdomains	/LM/W3SVC,EE Shared,DefaultDomain,Ssms.exe	-
secupi.agent.apps	Ssms.exe	-
secupi.smartdriver.mode.enabled	true	-
secupi.agent.config.poll	0.05	-
key	value	+

3. Download the .NET Agent

Select **Manage** (3a) in the top menu bar and then select **Agents** (3b) on the left hand side menu. To download a running agent, select **Downloads** (3c).



From the downloads screen, select the agent **.Net** (3d), then select the **Download** (3e) logo to download the .Net agent.



4. Once downloaded, extract the zip file. The contents of the file will look like this:

☐ Name	Date modified	Type	Size
pubcert.txt	21-10-2021 14:49	Text Document	2 KB
redisCa.crt	21-10-2021 14:49	Security Certificate	2 KB
SecuPi DotNet Agent.exe	21-10-2021 14:49	Application	30,087 KB
secupi.crt	21-10-2021 14:49	Security Certificate	2 KB
secupi.properties	21-10-2021 14:49	PROPERTIES File	1 KB
secupi_dotnet.properties	21-10-2021 14:49	PROPERTIES File	1 KB
version	21-10-2021 14:49	File	1 KB

5. Open the **secupi.properties** file.

☐ Name	Date modified	Type	Size
pubcert.txt	21-10-2021 14:49	Text Document	2 KB
redisCa.crt	21-10-2021 14:49	Security Certificate	2 KB
SecuPi DotNet Agent.exe	21-10-2021 14:49	Application	30,087 KB
secupi.crt	21-10-2021 14:49	Security Certificate	2 KB
secupi.properties ⁵	21-10-2021 14:49	PROPERTIES File	1 KB
secupi_dotnet.properties	21-10-2021 14:49	PROPERTIES File	1 KB
version	21-10-2021 14:49	File	1 KB

and the check for the properties which are there OR not that were added in Agent >>Integrate >> Override properties on SecuPiconsole.

6. Install the .NET Agent

By default, the .NET Framework installation will execute (If not, click on **SecuPi DotNet Agent.exe** application in the .NET Framework agent extracted folder and follow the installation wizard.)

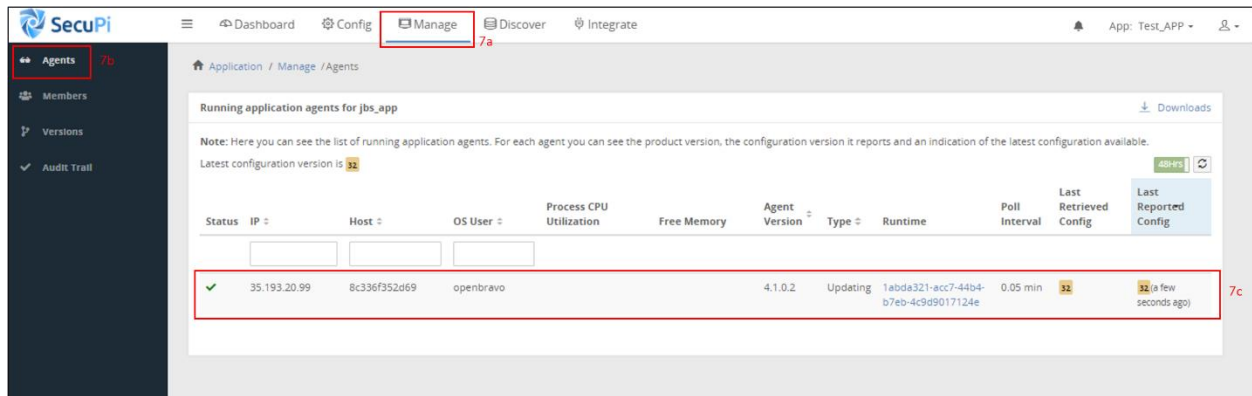
Select “C:\Program Files (x86)\CyberArk\PSM\Components” folder for install

To install **both** .NET Framework and .NET Core, they **must** be installed together.

☐ Name	Date modified	Type	Size
pubcert.txt	21-10-2021 14:49	Text Document	2 KB
redisCa.crt	21-10-2021 14:49	Security Certificate	2 KB
SecuPi DotNet Agent.exe ⁶	21-10-2021 14:49	Application	30,087 KB
secupi.crt	21-10-2021 14:49	Security Certificate	2 KB
secupi.properties	21-10-2021 14:49	PROPERTIES File	1 KB
secupi_dotnet.properties	21-10-2021 14:49	PROPERTIES File	1 KB
version	21-10-2021 14:49	File	1 KB

7. Once the agent is installed, test .net ODBC connection to your DB server via command `odbcad32` and login to your DB

To verify the agent is connected to the SecuPi server, select **Manage** (7a) in the top menu bar and then select **Agents** (7b) on the left hand side menu and check the **Agent Status** (7c).



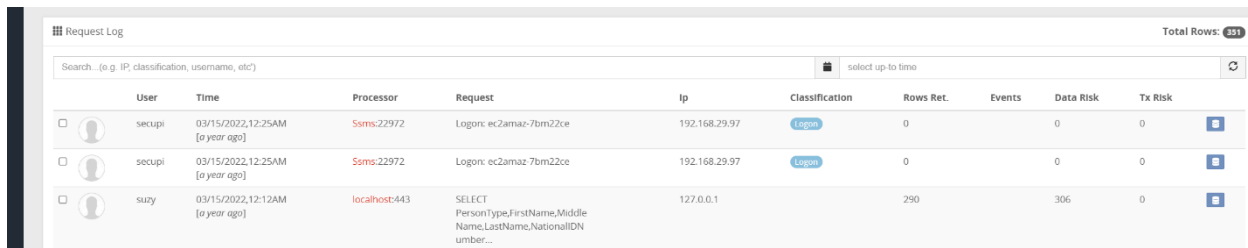
Running application agents for jbs_app

Note: Here you can see the list of running application agents. For each agent you can see the product version, the configuration version it reports and an indication of the latest configuration available.

Latest configuration version is 32

Status	IP	Host	OS User	Process CPU Utilization	Free Memory	Agent Version	Type	Runtime	Poll Interval	Last Retrieved Config	Last Reported Config
✓	35.193.20.99	8c336f352d69	openbravo			4.1.0.2	Updating	1abda321-ec7-44b4-b7eb-4c9d9017124e	0.05 min	32	32 (a few seconds ago)

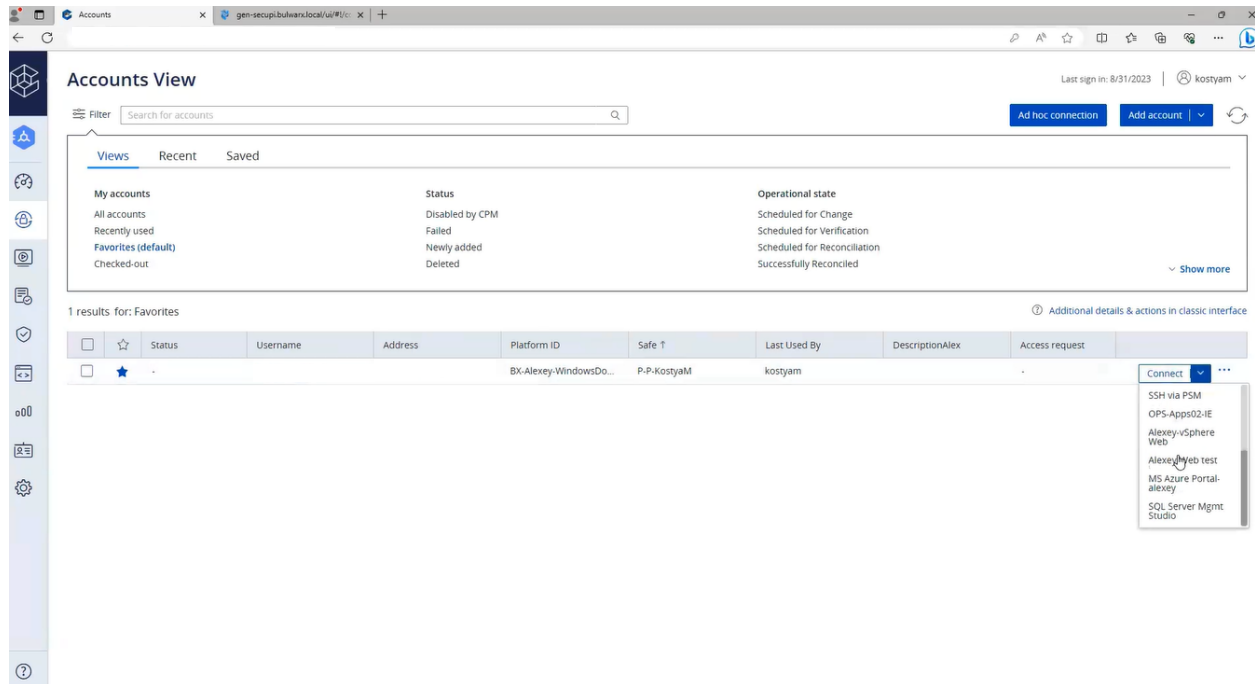
8. Now, you may open SSMS tool and query the Database and you will see transactions on SecuPi Console >>Dashboard like below.



User	Time	Processor	Request	Ip	Classification	Rows Ret.	Events	Data Risk	Tx Risk
secupi	03/15/2022,12:25AM [a year ago]	Ssms:22972	Logon: ec2amaz-7bm22ce	192.168.29.97	Logon	0	0	0	0
secupi	03/15/2022,12:25AM [a year ago]	Ssms:22972	Logon: ec2amaz-7bm22ce	192.168.29.97	Logon	0	0	0	0
suzy	03/15/2022,12:12AM [a year ago]	localhost:443	SELECT PersonType,FirstName,MiddleName,LastName,NationalIDNumber...	127.0.0.1		290	306	0	0

For .NET Agents, it is possible to create policies and apply masking, encryption, etc. For more information, see [Resource Access](#)

Once .NET enforcer Is Installed and working on the CyberArk Privileged Session Manager, configure your SSMS login with a privileged user to an SSMS privileged session:



Once you're In the SSMS privileged session, all access to databases will show up In the SecuPi management Server dashboard:

