Splunk and Avecto Defendpoint

Software Version: Splunk Enterprise 6.5+ and Defendpoint 4.5+

Document Version: 1.0

Document Date: November 2017

Table of Contents

Chapter 1 - Setting up Splunk Enterprise to Collect Avecto Defendpoint Events

Splunk Enterprise is a data collection service that indexes events from a variety of sources. Splunk Enterprise can be used to capture and report on events from Avecto Defendpoint.

1.1 - Splunk Enterprise and Enterprise Reporting Versions

The following versions of Splunk Enterprise and Enterprise Reporting are supported:

- Splunk Enterprise 6.5 or greater.
- Enterprise Reporting 4.5 or greater.

1.2 - Getting Data into Splunk Enterprise

Splunk Enterprise allows you to collect Avecto events two different ways. This guide covers:

- From your endpoints or from your Windows Event Collector node using the Splunk Universal Forwarder, see **Splunk Universal Forwarder** detailed on page 6. This approach is useful if you're collecting multiple events from multiple products including Avecto Defendpoint
- Importing events from the Enterprise Reporting database using Splunk DB Connect, see **Splunk DB Connect** detailed on page 8. This approach can be used with Avecto Enterprise Reporting database version 4.5 or later deployed with any of our management platforms. With this approach you don't need to deploy further agents to your endpoints.

1.2.1 - Data Quantity

Typically, a well configured Defendpoint endpoint will generate about fifteen to twenty events per endpoint each day but this is highly dependent on configuration and can be significantly higher.

For DB Connect, the 'Execution Frequency' should be set to a period of at least a minute though we recommend every five minutes as a reasonable default. The 'cron' style set up allows updates at quiet times (for example, overnight) if timely delivery to Splunk is less important than conserving network bandwidth or database server resources.

For DB Connect, the 'Fetch Size' in the database connections can remain as the default (300). The 'Max rows to retrieve' can be configured to limit load (for example, after an outage), but leaving this as unlimited is recommend (0 or blank). This ensures that all the data is collected and the Splunk server does not fall behind which would be possible if this value is set too small.

Data that is held in the Enterprise Reporting database is de-duplicated. This can be beneficial if you have a tiered approach to your event collection as you can use the rising column value to assist with batch processing in this instance.

You can also filter the data when you query it so you only import what you need using DB Connect, see **Working with Data in Splunk Enterprise** detailed on page 14.

Chapter 2 - Configuring Splunk Enterprise

You need to configure Splunk Enterprise to receive events from either the Splunk Universal Forwarder or the Splunk DB Connect application.

For this installation we have assumed you have a Splunk Enterprise installation, you have the appropriate access to the system and you are familiar with the Splunk interface.

To configure Splunk Enterprise to receive events:

1. Click **Settings** > **Forwarding Receiving** (under the **Data** menu).
2. Click **Configure Receiving** and then **New** to create a new entry.
3. Enter '9997' in the **Listen on this port** field and click **Save**.

Splunk Enterprise is now configured to listen for events that are being sent using any method.

Chapter 3 - Splunk Universal Forwarder

You can either install the Splunk Universal Forwarder on your endpoints or you can install it on your Windows Event Collector node. The installation for both is largely the same. Differences are explained in the installation steps where applicable.

If you want to get events from the Enterprise Reporting database instead, see **Splunk DB Connect** detailed on page 8.

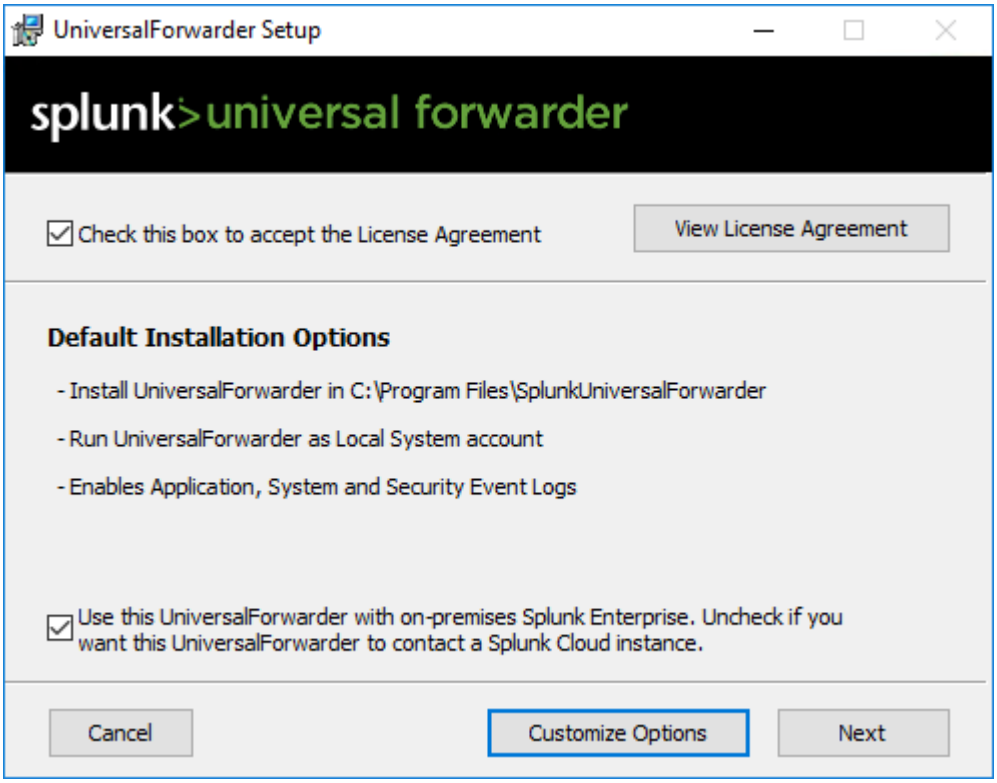
3.1 - Installing the Splunk Universal Forwarder

The Splunk Universal Forwarder can be used to collect data from your endpoints or your Windows Event Collector node.

The Splunk Universal Forwarder can be downloaded from Splunk: https://www.splunk.com/en_us/download/universal-forwarder.html.

Installing the Splunk Universal Forwarder

1. Double click the Splunk Universal Forwarder and select the check box at the top of the Setup to accept the license agreement. Click **Customize Options**.



2. Select your installation location and click **Next**.
3. You can use an SSL certificate to encrypt the events you are sending to Splunk Enterprise in this section. Please follow the instructions to do this if required. Click **Next**.
4. You can leave the default as **Local System** as the Splunk Universal Forwarder only needs to read events stored locally, regardless of whether it is installed on an endpoint or a Windows Event Collector. Click **Next**.

5. If you are installing the Splunk Universal Forwarder on your endpoint, select the **Application Logs** check box to collect your application events from the endpoint. Alternatively, if you are installing Splunk on your Windows Event Collector node, select the **Forwarded Logs** check box to collect events that have been forwarded to the Windows Event Collector node. You can change this to just Defendpoint events after the installation if required. Click **Next**.

In the next section you can choose to configure your **Deployment Server** and **Receiving Indexer**. You need to have either a **Deployment Server** or a **Receiving Indexer**.

6. You can enter details of your Splunk Enterprise **Deployment Server** here if you're using one. Splunk deployment servers allow you to distribute configurations, applications and content to groups of Splunk Enterprise instances. Click **Next**.
7. You can enter details of your Splunk **Receiving Indexer** here if you're using one. Splunk Receiving Indexers allow you to receive events from one or more source. Click **Next**.
8. Click **Install** to complete the installation of the Splunk Universal Forwarder.

The next step is to configure the types of events you want to collect, see **Configuring Splunk Universal Forwarder** detailed below.

3.2 - Configuring Splunk Universal Forwarder

Once you have installed the Splunk Universal Forwarder you can configure the types of events that you want to be sent to Splunk Enterprise.

To configure the type of events that are sent to Splunk Enterprise, you need to edit the `Inputs.Conf` file. In a default installation of the Splunk Universal Forwarder the file is stored in this path:

```
C:\Program Files\SplunkUniversalForwarder\etc\system\local
```

Depending on your user access you may need to change the permissions of this file in Windows to allow you to edit it.

Example to just collect Defendpoint events
This example will just collect Defendpoint events from that endpoint or the Windows Event Forwarder node.

```
[default]
host = DESKTOP-OU2VDC4

[WinEventLog://Avecto Defendpoint Service]
disabled = false
```

You need to restart the Splunk Universal Forwarder service after you've saved your changes for them to take effect.

Please refer to the additional Splunk Enterprise documentation for editing this file if required: https://docs.splunk.com/Documentation/Splunk/6.6.2/Admin/Inputsconf.

Chapter 4 - Splunk DB Connect

Splunk DB Connect is an application from Splunk Enterprise that you can install in your Splunk Enterprise instance. Splunk DB Connect retrieves events from the database you define, such as Avecto Enterprise Reporting and inserts them into Splunk Enterprise.

You can use Splunk DB Connect to query the Export Views for Defendpoint. For more information see **Using Export Views** detailed on page 16

You can use SQL authentication or any of the default Enterprise Reporting accounts to authenticate with the Avecto database. The default accounts are Report Reader, Event Parser and Data Admin.

If you want to get events from your endpoints or your Windows Event Collection node instead, see **Splunk Universal Forwarder** detailed on page 6.

4.1 - Installing DB Connect

Prerequisites

- Splunk Enterprise 6.4.0 or later
- Java Platform, Standard Edition Development Kit (JDK) from Oracle, see http://www.oracle.com/technetwork/java/javase/downloads/index.html. The JRE alone is not sufficient, you need the JDK.
- Java Database Connection (JDBC) to allow you to connect to databases

Please see the Splunk DB Connect documentation if you need additional information: http://docs.splunk.com/Documentation/DBX/3.1.0/DeployDBX/Prerequisites

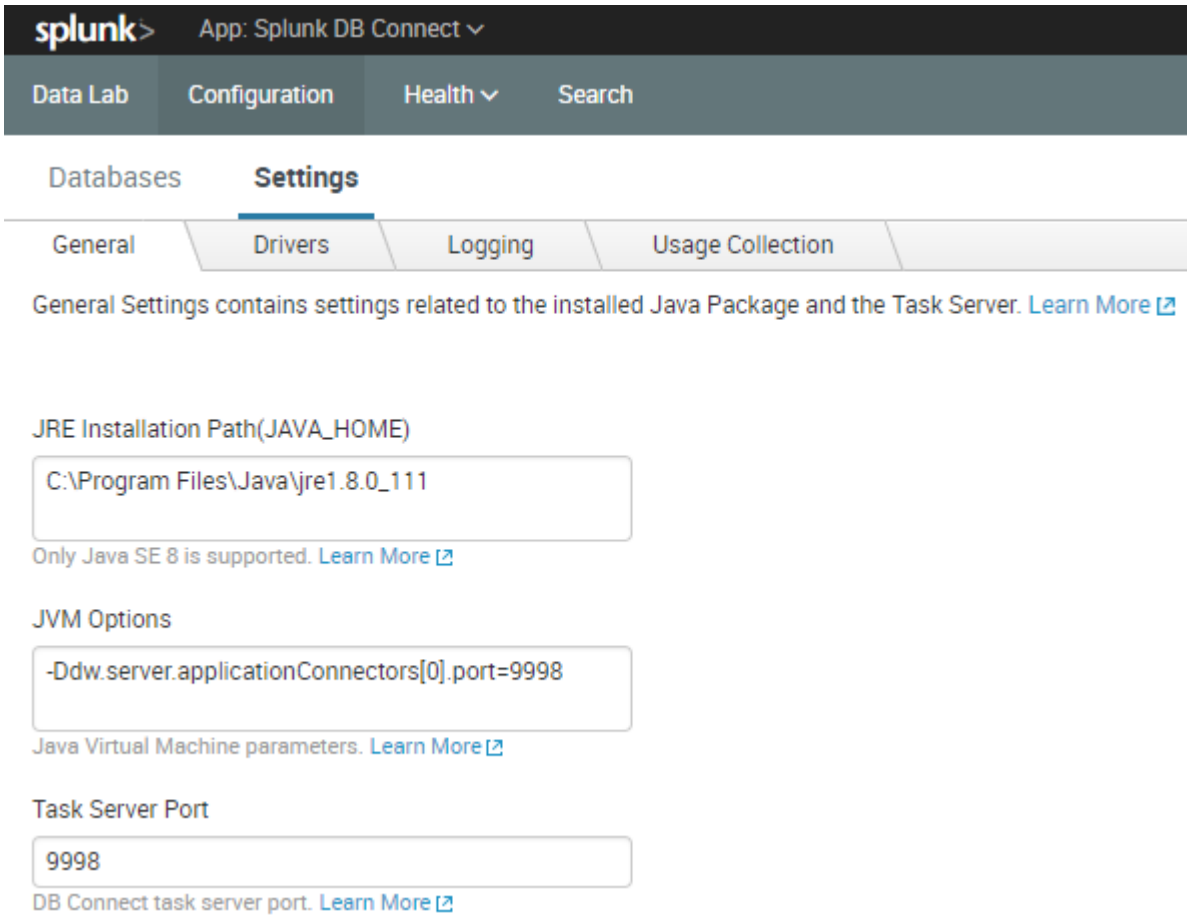
Installing on Splunk Enterprise:

1. Open your Splunk Enterprise instance and click **App: Search & Reporting** from the top menu bar.
2. If **DB Connect** is installed it will appear in the list. Otherwise click **Find More Apps**.
3. Type 'DB Connect' in to the Search box if Splunk can connect to the Internet. Follow the onscreen instructions to install DB Connection. Alternatively you can download **DB Connect** directly from the Splunk store and install it manually: https://splunkbase.splunk.com/app/2686/.
4. Click **App: Search & Reporting** > **Manage Apps** to install **DB Connect** from a separate installer.
5. Click **Install app from file** and browse to the location of **DB Connect** that you downloaded.
6. Click **Upload** and follow the onscreen instructions to install **DB Connect**.
7. Once **DB Connect** has been installed you can access it from the **App: Search & Reporting** top menu.

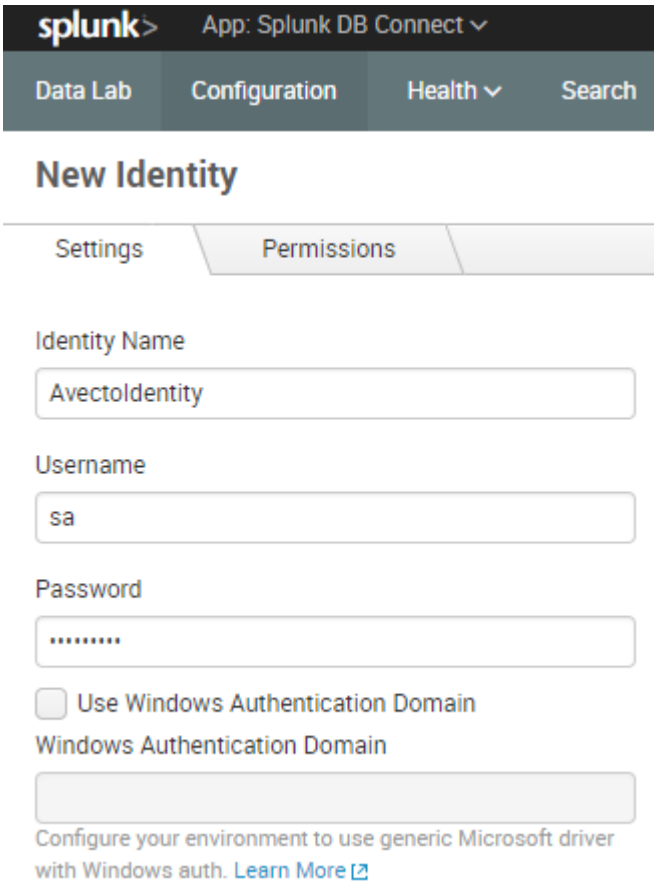
4.2 - Configuring DB Connect

Configuring Splunk DB Connect:

1. Click **App: Search & Reporting** > **Splunk DB Connect**.
2. Click **Configuration** > **Settings**. In the **General** tab you need to configure the path to your JRE Installation path on the machine hosting Splunk. The JVM Options and Task Server Port will be configured by Splunk, more information can be found in the Splunk documentation: http://docs.splunk.com/Documentation/DBX/3.0.2/DeployDBX/ConfigureDBConnectsettings.
3. Click **Save** to confirm your settings.

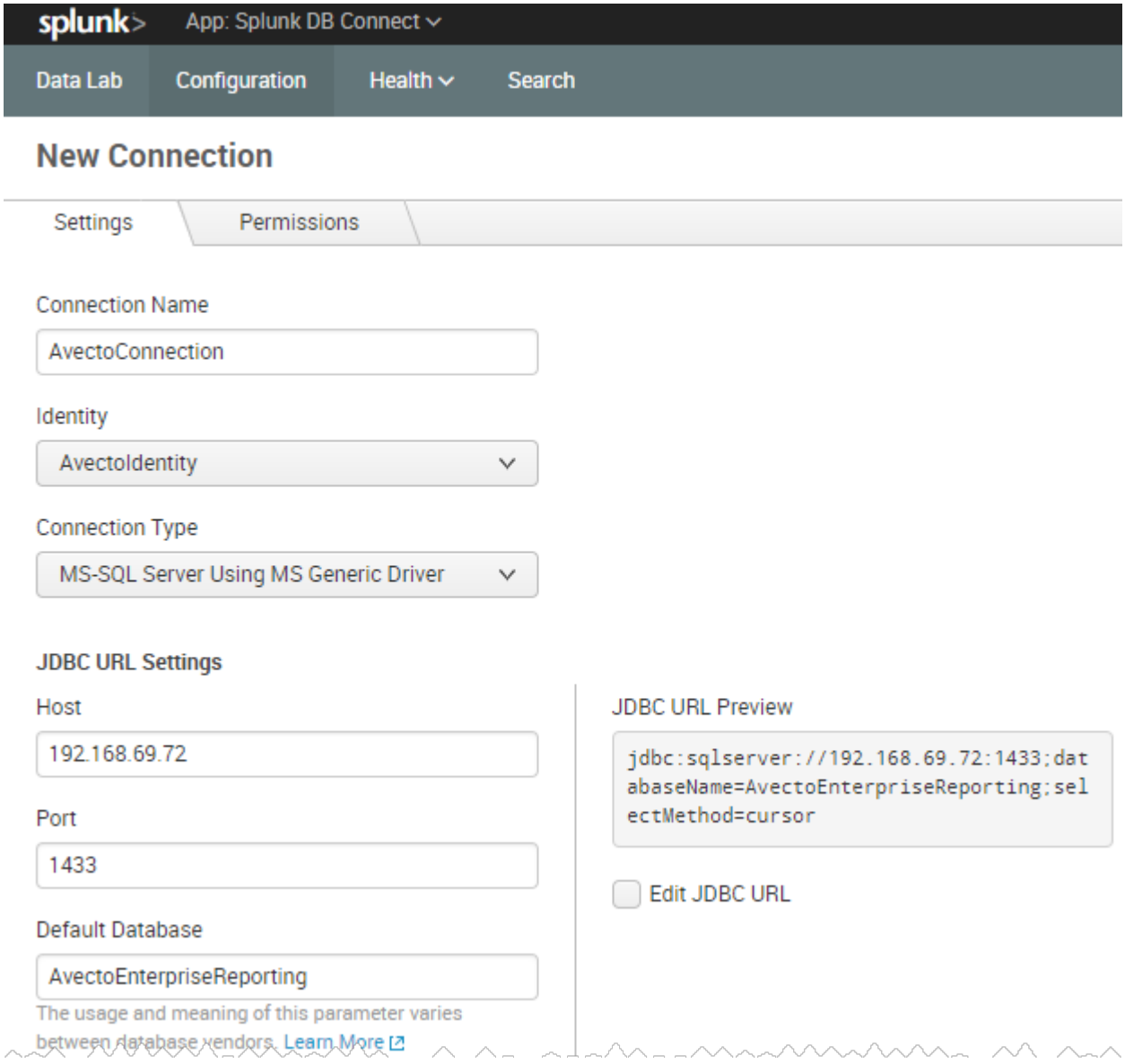


4. Click the **Databases** tab > **Identities** tab. Click **New Identity**. This is the identity (user) that Splunk uses to authenticate to the Avecto database to export events.
    - Enter an **Identity Name** that you will use to identify the user.
    - You can either use SQL authentication as shown here or you can use Windows authentication and any of the standard Enterprise Reporting accounts that are set up by the installer. These are ReportReader, Event Parser and Data Admin, see the Enterprise Reporting installation guide for more information. Click **Save** to confirm your identity.



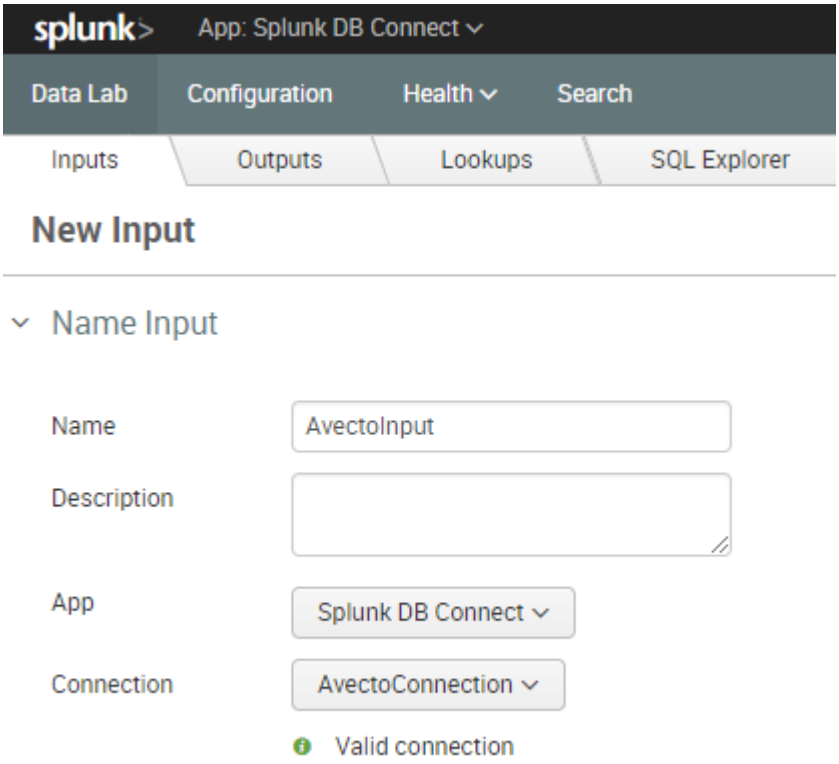
Leave the default permission set that Splunk Enterprise provides on the **Permissions** tab.

5. Click the **Connections** tab. This is where you configure the database that you will connect to.
   - Enter a **Connection Name**. This is to identify the connection in Splunk.
   - Select the Identity you created from the drop-down list.
   - Select the **Connection Type** 'MS SQL Server Using MS Generic Driver'.
   - Enter the host IP address of your database server. Leave the port as the default '1433'.
   - Enter the Default Database as the one containing your Avecto Enterprise Reporting data.
   - You can choose to configure the additional options if they are relevant for your environment.
   - Click **Save** to save your connection. This will also validate the connection.

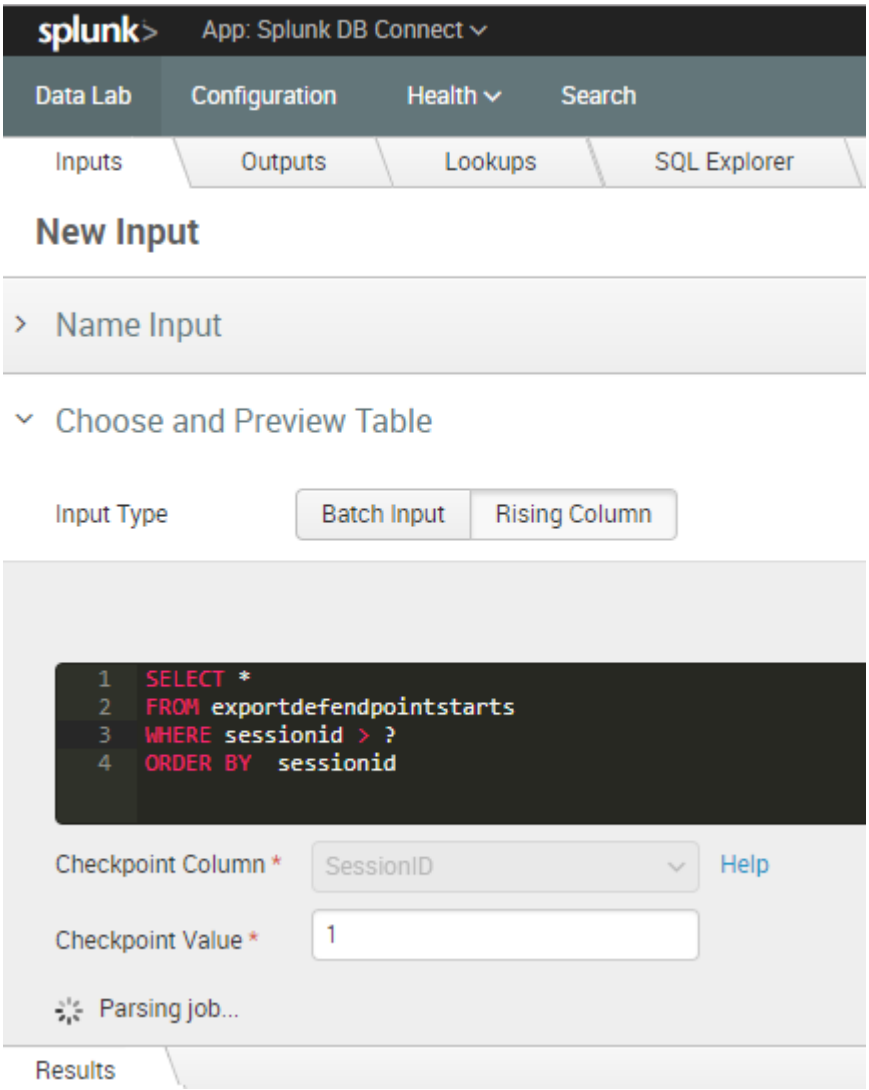


Leave the default permission set that Splunk Enterprise provides on the **Permissions** tab.

6. Click the **Data Lab** tab and click **New Input** on the right-hand side.
    - Enter a Name for you to identify the new Input by. You can also enter a Description if required.
    - Leave the **App** drop-down as 'Splunk DB Connect'.
    - Select your **Connection** from the drop-down menu. This also validates it.



7. Click **Continue**. This allows you to choose and preview a table. You can now import the Export Views into Splunk. These are ExportDefendpointStarts, ExportDefendpointLogins, ExportPrivilegedAccountProtection, and ExportProcesses. This example uses the ExportDefendpointStarts view.
    - Select **Rising Column**. This ensures the events you get from the Enterprise Reporting database are incremented rather than retrieving the same events repeatedly.
    - You can manually type a SQL query into the field here or select the **Checkpoint Column** and the **Checkpoint Value**. You should use a '?' as a placeholder in your SQL query for the Checkpoint Value as you set this manually below in the drop-down.
    - Click **Execute** to search for the specified events in the Enterprise Reporting database. This does not insert them into Splunk.



You can modify the SQL query to filter your results. This will help limit the data that is imported into Splunk Enterprise and your associated costs. For example, this SQL query imports events where the Defendpoint version is 4.3.349.0 only.

```
SELECT *
FROM exportdefendpointstarts
WHERE sessionid > ?
AND AgentVersion='4.0.349.0'
ORDER BY sessionid asc
```

8. Click **Execute** to search for the specified events in the Enterprise Reporting database. These are displayed below.
9. Click **Continue**. You can set parameters for the input here if required.
10. Click **Continue**. Each event that is imported into Splunk has the metadata you configure here as part of it. You can configure a new **Sourcetype** from the Settings menu on the top-right if required. See http://docs.splunk.com/Documentation/SplunkCloud/6.6.1/Data/Createsourcetypes.
11. Click **Save** to confirm your **Input Type** and start importing events into Splunk.

You need to repeat steps 7 to 11 for each of the Export Views.

4.3 - Working with Data in Splunk Enterprise

Avecto provides four de-normalized views for use in Splunk Enterprise:

- ExportDefendpointStarts
- ExportLogons
- ExportPrivilegedAccountProtection
- ExportProcesses

The fields for each Defendpoint export view is detailed in the appendix **Using Export Views** detailed on page 16.

These views allow you to import Avecto audit data into SIEM systems such as Splunk Enterprise. Each view has a rising column that allows the SIEM system to track what data has been imported already.

4.3.1 - ExportProcesses

This view returns the Process Control events such as elevating or blocking applications. The columns include **ApplicationDescription**, **Publisher**, **ProductVersion**, **UserName**, **HostName**, **WorkstyleName** as well as the event action flags including **Elevated**, **Blocked** or **Passive**.

ProcessID is the rising column and **ProcessStartTime** is the timestamp.

4.3.2 - ExportLogons

This view returns the Logon events in the database. The columns include **LogonTime**, **UserName**, **HostName** and **WorkstyleName**.

LogonID is the rising column and **LogonTime** is the timestamp.

4.3.3 - ExportDefendpointStarts

This view returns the Defendpoint started events in the database. The columns include **SessionStartTime**, **HostName**, **AgentVersion** and **OS**.

SessionID is the rising column and **SessionStartTime** is the timestamp.

4.3.4 - ExportPrivilegedAccountProtection

This view returns the Privileged Account Management events in the database. The columns include **TimeGenerated**, **Access**, **WorkstyleName**, **UserName**, **HostName** and **ApplicationDescription**.

ID is the rising column and **TimeGenerated** is the timestamp.

Appendix A - Using Export Views

Avecto provides four de-normalized export views for Defendpoint events:

- **ExportDefendpointStarts** detailed below
- **ExportDefendpointLogons** detailed on the next page
- **ExportPrivilegedAccountProtection** detailed on page 19
- **ExportProcesses** detailed on page 21

Each of these views can be queried in Splunk. For each view the following data is given to Splunk. These Export Views are correct as of Enterprise Reporting 4.5.

A.1 - ExportDefendpointStarts

Column_name	Type	Length	Index	Description	Example
SessionID	bigint		3	Ascending Identity	1
SessionGUID	uniqueidentifier			UUID of the session	5CD221E9-CEB5-441D-B380-CB266400B320
SessionStartTime	datetime			Time session started	2017-01-03 10:24:00.000
SessionEndTime	datetime			Always NULL (not used)	NULL
HostSID	nvarchar	200	1	Host SID	S-1-21-123456789-123456789-1635717638-390614945
AgentVersion	nvarchar	20		Defendpoint Client Version	4.0.384.0
ePOMode	int			1 if DP client is in ePO mode. 0 otherwise.	1
CertificateMode	int			Certificate Mode	0
PolicyAuditMode	int			Policy Audit Mode	7
DefaultUILanguage	int			Locale Identifier of UI Language	2057
DefaultLocale	int			Locale Identifier of Locale	2057

Column_name	Type	Length	Index	Description	Example
SystemDefaultTimezone	int			Not set so always “0”	0
ChassisType	nvarchar	40		Chassis Type	Other
HostName	nvarchar	1024	2*	Host name	EGHostWin1
HostNameNETBIOS	nvarchar	15	2*	Host NETBIOS	EGHOSTWIN1
OS	nvarchar	20		OS Version	6.3
OSProductType	int	4		OS Product Type.	1
PlatformType	nvarchar	10		Platform Type	Windows
HostDomainSID	nvarchar	200		Host Domain SID	S-1-21-123456789-123456789-1635717638
HostDomainName	nvarchar	1024		Host Domain	EGDomain
HostDomainNameNETBIOS	nvarchar	15		Host Domain NETBIOS	EGDOMAIN

A.2 - ExportDefendpointLogons

Column_name	Type	Length	Index	Description	Example
LogonID	bigint		3	Ascending Identity	1
LogonGUID	uniqueidentifier			UUID of the logon	819EF606-F9B6-40BE-9C0C-A033A34EC4F8
HostSID	nvarchar	200	1	Host SID	S-1-21-123456789-123456789-1635717638-390614945
UserSID	nvarchar	200		User SID	S-1-21-123456789-123456789-1635717638-1072059836
LogonTime	datetime			Logon Date/Time	2017-01-03 10:24:00.000
IsAdmin	bit			1 if an admin, 0 otherwise	0

Column_name	Type	Length	Index	Description	Example
IsPowerUser	bit			1 if a power user, 0 otherwise	0
UILanguage	int			Locale Identifier of the UI Language	1033
Locale	int			Locale Identifier of the Locale	2057
UserName	nvarchar	1024		User name	EGUser1
UserDomainSID	nvarchar	200		User Domain SID	S-1-21-123456789-123456789-1635717638
UserDomainName	nvarchar	1024		User Domain	EGDomain
UserNameNETBIOS	nvarchar	15		User NETBIOS	EGDOMAIN
ChassisType	nvarchar	40		Chassis Type	Docking Station
HostName	nvarchar	1024	2*	Host name	EGHostWin1
HostNameNETBIOS	nvarchar	15	2*	Host NETBIOS	EGHOSTWIN1
OS	nvarchar	20		OS Version	6.3
OSProductType	int			OS Product Type	1
PlatformType	nvarchar	10		Platform Type	Windows
HostDomainSID	nvarchar	200		Host Domain SID	S-1-21-123456789-123456789-1635717638
HostDomainName	nvarchar	1024		Host Domain	EGDomain
HostDomainNameNETBIOS	nvarchar	15		Host Domain NETBIOS	EGDOMAIN
PolicyName	nvarchar	1024		Policy Name	EventGen Test Policy
WorkstyleName	nvarchar	1024		Workstyle name	EventGen Test Workstyle

A.3 - ExportPrivilegedAccountProtection

Column_name	Type	Length	Index	Description	Example
ID	bigint		1	Ascending Identity	1
TimeGenerated	datetime			Event Generation Date/Time	
CommandLine	nvarchar	1024		Command Line	<None>
PrivilegedGroupName	nvarchar	200		Privileged Group Name	Administrators
PrivilegedGroupRID	nvarchar	10		Privileged Group Relative Identifier	544
Access	nvarchar	200		Group Access Details	Add Member, Remove Member, List Members, Read Information
PolicyGUID	uniqueidentifier			Policy UUID	E7654321-AAAA-5AD2-B954-12342918D604
PolicyName	nvarchar	1024		Policy Name	EventGen Test Policy
WorkstyleName	nvarchar	1024		Workstyle name	EventGen Test Workstyle
FileName	nvarchar	255		File name	<None>
ApplicationHash	nvarchar	40		Application SHA1	921CA2B3293F3FCB905B24A9536D8525461DE2A3
ProductCode	nvarchar	1024		Product Code	<None>
UpgradeCode	nvarchar	1024		Upgrade Code	<None>
FileVersion	nvarchar	1024		File Version	<None>
MD5	nvarchar	32		MD5 Hash	3279476E39DE235B426D69CFE8DEBF55
UserSID	nvarchar	200		User SID	S-1-21-123456789-123456789-1635717638-1072059836
UserName	nvarchar	1024		User Name	EGUser1
UserDomainSID	nvarchar	200		User Domain SID	S-1-21-123456789-123456789-1635717638

Column_name	Type	Length	Index	Description	Example
UserDomainName	nvarchar	1024		User Domain	EGDomain
UserNameNETBIOS	nvarchar	15		User Domain NETBIOS	EGDOMAIN
ChassisType	nvarchar	40		Chassis Type	Other
HostSID	nvarchar	200		Host SID	S-1-21-123456789-123456789-1635717638-390614945
HostName	nvarchar	1024		Host Name	EGHostWin1
HostNameNETBIOS	nvarchar	15		Host NETBIOS	EGHOSTWIN1
OS	nvarchar	20		OS Version	6.3
OSProductType	int			OS Product Type	1
HostDomainSID	nvarchar	200		Host Domain SID	S-1-21-123456789-123456789-1635717638
HostDomainName	nvarchar	1024		Host Domain	EGDomain
HostDomainNameNETBIOS	nvarchar	15		Host domain NETBIOS	EGDOMAIN
FileOwnerUserSID	nvarchar	200		File Owner SID	S-1-5-80-956008885-3418522649-1831038044-1853292631-2271478464
FileOwnerUserName	nvarchar	1024		File Owner	NT SERVICE\TrustedInstaller
FileOwnerDomainName	nvarchar	1024		File Owner Domain	NT SERVICE
ApplicationURI	nvarchar	1024		URI of a macOS application	com.apple.preference.datetime
ApplicationDescription	nvarchar	2048		Application description	lusrmgr.msc
FirstDiscovered	datetime			First time app was seen	2017-01-03 10:25:50.110
FirstExecuted	datetime			First time app was executed	2017-01-03 10:24:00.000
PlatformType	nvarchar	10		Platform Type	Windows

Column_name	Type	Length	Index	Description	Example
ProductName	nvarchar	1024		Product name	<None>
ProductVersion	nvarchar	1024		Product version	<None>
Publisher	nvarchar	1024		Publisher	Microsoft Windows
TrustedOwner	bit			1 if a trusted owner, 0 otherwise	1

A.4 - ExportProcesses

Column_name	Type	Length	Index	Description	Example
ProcessID	bigint		4	Ascending Identity	1
ProcessGUID	uniqueidentifier		2	UUID of the process	98C99D96-6DFA-4C95-9A87-C8665C166286
EventNumber	int			Event Number. See List of Events section.	153
TimeGenerated	datetime			Event generation date/time	2017-02-20 13:11:11.217
TimeReceived	datetime			Event received at ER date/time	2017-02-20 13:16:28.047
PID	int			Process ID	8723
ParentPID	int			Parent Process ID	142916
CommandLine	nvarchar		1024	Command Line	"C:\cygwin64\bin\sh.exe"
FileName	nvarchar		255	File Name	c:\cygwin64\bin\sh.exe
ProcessStartTime	datetime		1	Date/Time Process Started	2017-02-20 13:11:11.217
Reason	nvarchar		1024	Reason entered by user	<None>
ClientIPV4	nvarchar		15	Client IP Address	10.0.9.58
ClientName	nvarchar		1024	Client Name	L-CNU410DJJ7

Column_name	Type	Length	Index	Description	Example
UACTriggered	bit			1 if UAC shown	0
ParentProcessUniqueID	uniqueidentifier			Parent process UUID	C404C7F5-3A93-4C0E-81BC-9902D220C21E
COMCLSID	uniqueidentifier			COM CLSID	NULL
COMAppID	uniqueidentifier			COM Application ID	NULL
COMDisplayName	nvarchar	1024		COM Display Name	<None>
ApplicationType	nvarchar	4		Application Type	svc
TokenGUID	uniqueidentifier			UUID of token in policy	F30A3824-27AF-4D69-9125-C78E44764AC1
Executed	bit			1 if executed, 0 otherwise	1
Elevated	bit			1 if elevated, 0 otherwise	1
Blocked	bit			1 if blocked, 0 otherwise	0
Passive	bit			1 if passive, 0 otherwise	0
Cancelled	bit			1 if cancelled, 0 otherwise	0
DropAdmin	bit			1 if admin rights dropped, 0 otherwise	0
EnforceUsersDefault	bit			1 if user default permissions were enforced, 0 otherwise	0
Custom	bit			1 if custom token, 0 otherwise	0
SourceURL	nvarchar	2048		Source URL	<None>
AuthorizationChallenge	nvarchar	9		Challenge Response authorization code	<None>
WindowsStoreAppName	nvarchar	200		Windows Store application name (appx app type only)	<None>

Column_name	Type	Length	Index	Description	Example
WindowsStoreAppPublisher	nvarchar	200		Windows Store application publisher (appx app type only)	<None>
WindowsStoreAppVersion	nvarchar	200		Window Store application version (appx app type only)	<None>
DeviceType	nvarchar	40		Device Type	Fixed Disk
ServiceName	nvarchar	1024		Service name (svc events only)	<None>
ServiceDisplayName	nvarchar	1024		Service Display Name (svc app type only)	<None>
PowerShellCommand	nvarchar	1024		PowerShell Command (ps1/rpsc/rpss app types only)	<None>
ApplicationPolicyDescription	nvarchar	1024		Policy Description	<None>
SandboxGUID	uniqueidentifier			Sandbox UUID (sandbox events only)	NULL
SandboxName	nvarchar	1024		Sandbox Name (sandbox events only)	NULL
BrowseSourceURL	nvarchar	2048		Sandbox browse source (sandbox events only)	<None>
BrowseDestinationURL	nvarchar	2048		Sandbox destination source (sandbox events only)	<None>
Classification	nvarchar	200		Sandbox classification (sandbox events only)	Private (Local)
IEZoneTag	nvarchar	200		IE Zone Tag	<None>
OriginSandbox	nvarchar	40		Origin Sandbox	<None>
OriginIEZone	nvarchar	40		Origin IE Zone	<None>
TargetSandbox	nvarchar	40		Target Sandbox	<None>
TargetIEZone	nvarchar	40		Target IE Zone	<None>

Column_name	Type	Length	Index	Description	Example
AuthRequestURI	nvarchar	1024		Authorization request URL (osx challenge/response only)	<None>
PlatformVersion	nvarchar	10		Platform Version	<None>
ControlAuthorization	bit			1 is Defendpoint authorized this macOS application	0
ApplicationHash	nvarchar	40		SHA1 of the application	C22FF10511ECCEA1824A8DE64B678619C21B4BEE
ProductCode	nvarchar	1024		Product Code	<None>
UpgradeCode	nvarchar	1024		Upgrade Code	<None>
FileVersion	nvarchar	1024		File Version	<None>
MD5	nvarchar	32		MD5 hash of the app	6E641CAE42A2A7C89442AF99613FE6D6
TokenAssignmentGUID	uniqueidentifier			UUID of the token assignment in the policy	E7654321-BBBB-5AD2-B954-1234DDC7A89D
TokenAssignmentIsShell	bit			Token assignment is for shell	1
UserSID	nvarchar	200		User SID	S-1-21-123456789-123456789-16357176381125883508
UserName	nvarchar	1024		User Name	EGUser18
UserDomainSID	nvarchar	200		User Domain SID	S-1-21-123456789-123456789-1635717638
UserDomainName	nvarchar	1024		User Domain	EGDomain
UserDomain NameNETBIOS	nvarchar	15		User Domain NETBIOS	EGDOMAIN
ChassisType	nvarchar	40		Chassis Type	Laptop
HostSID	nvarchar	200		Host SID	S-1-21-123456789-123456789-1635717638775838649
HostName	nvarchar	1024	3*	Host Name	EGHostWin18
HostNameNETBIOS	nvarchar	15	3*	Host NETBIOS	EGHOSTWIN18

Column_name	Type	Length	Index	Description	Example
OS	nvarchar			OS Version	10.0
OSProductType	int			OS Product Type	
HostDomainSID	nvarchar	200		Host Domain SID	S-1-21-123456789-123456789-1635717638
HostDomainName	nvarchar	1024		Host Domain	EGDomain
HostDomain NameNETBIOS	nvarchar	15		Host Domain NETBIOS	EGDOMAIN
AuthUserSID	nvarchar	200		Authorizing User SID	<None>
AuthUserName	nvarchar	1024		Authorizing User	<None>
AuthUserDomainSID	nvarchar	200		Authorizing User Domain SID	<None>
AuthUserDomainName	nvarchar	1024		Authorizing User Domain	<None>
AuthUserDomain NameNETBIOS	nvarchar	15		Authorizing User Domain NETBIOS	<None>
FileOwnerUserSID	nvarchar	200		File Owner SID	S-1-5-80-956008885-3418522649-1831038044-1853292631-2271478464
FileOwnerUserName	nvarchar	1024		File Owner	NT SERVICE\TrustedInstaller
FileOwnerDomainSID	nvarchar	200		File Owner Domain SID	S-1-5-80
FileOwnerDomainName	nvarchar	1024		File Owner Domain	NT SERVICE
FileOwnerDomain NameNETBIOS	nvarchar	15		File Owner Domain NETBIOS	<None>
ApplicationURI	nvarchar	1024		URI of the macOS Application	com.apple.preference.datetime
ApplicationDescription	nvarchar	2048		Application Description	c:\cygwin64\bin\sh.exe
FirstDiscovered	datetime			Time application first seen	2017-02-07 09:14:39.413
FirstExecuted	datetime			Time application first executed	2017-02-07 09:07:00.000
PlatformType	nvarchar	10		Platform Type	Windows

Column_name	Type	Length	Index	Description	Example
ProductName	nvarchar	1024		Product Name	ADelRCP Dynamic Link Library
ProductVersion	nvarchar	1024		Product Version	15.10.20056.167417
Publisher	nvarchar	1024		Publisher	Adobe Systems, Incorporated
TrustedOwner	bit			1 if a trusted owner, 0 otherwise	0
MessageGUID	uniqueidentifier			UUID of the message in the policy	00000000-0000-0000-0000-000000000000
MessageName	nvarchar	1024		Name of the message in the policy	Block Message
MessageType	nvarchar	40		Message Type	Prompt
AppGroupGUID	uniqueidentifier			UUID of the Application Group in the Policy	47E4A204-FC06-428B-8E73-1E36E3A65430
AppGroupName	nvarchar	1024		Application Group Name in the Policy	Test Policy.test
PolicyID	bigint			Internal ID of the Policy	2
PolicyGUID	uniqueidentifier			UUID of the Policy	E7654321-AAAA-5AD2-B954-12342918D604
PolicyName	nvarchar	1024		Policy Name	EventGen Test Policy
WorkstyleName	nvarchar	1024		Workstyle Name	EventGen Test Workstyle
ContentFileName	nvarchar	255		Content File Name	c:\users\user.wp-epo-win7-64\downloads\con29 selectable feestable (1).pdf
ContentFileDescription	nvarchar	1024		Content File Description	<None>
ContentFileVersion	nvarchar	1024		Content File Version	<None>
ContentOwnerSID	nvarchar	200		Content Owner SID	S-1-21-123456789-123456789-1635717638-1072059836
ContentOwnerName	nvarchar	1024		Content Owner	EGUser1
ContentOwnerDomainSID	nvarchar	200		Content Owner Domain SID	S-1-5-21-2217285736-120021366-3854014904

Column_name	Type	Length	Index	Description	Example
ContentOwnerDomainName	nvarchar	1024		Content Owner Domain	AVECTOTEST58\AVECTOTEST58.QA
ContentOwnerDomain NameNetBIOS	nvarchar	15		Content Owner Domain NETBIOS	AVECTOTEST58
TrustedApplicationName	nvarchar	1024		Name of the trusted application	Microsoft Word
TrustedApplicationVersion	nvarchar	1024		Version of the trusted application	11.1715.14393.0
ParentProcessFileName	nvarchar	1024		Parent process file name	Google Chrome