IVANTI XTRACTION - Connector

SECURITY CONTROLS

Technical Documentation

06/25/2021

Table of Contents

Requirements

- Ivanti Security Controls 2019.1 +
  (Most likely will work on future releases but as yet not validated)
  If incompatibilities are found, please open a support case and report these so they can be addressed.
  Does **NOT** work with any version of Patch for Windows or ISeC Connector.
- Ivanti Xtraction installed – Any version.
- Port 1433 (or Custom if Used) port open between the Xtraction server and the Security Controls database.
- Read-Only account to the Security Controls database (May be Domain or SQL Account).

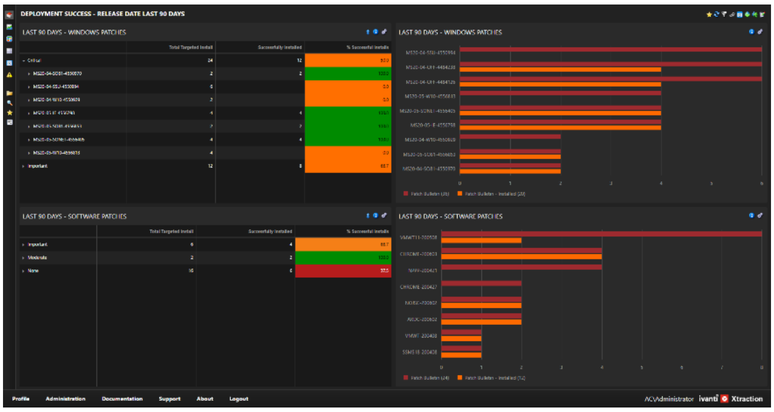
Description

- The Security Controls Connector allows, through the Xtraction application for data in the Security Controls database such as that related to scans, deployments, patch to vulnerability relationships and machine status to be visually reported in Real-Time.
- Consider the connector to be the interpretation layer between the database and Xtraction, when a field is dragged on to the dashboard, through the interpreter, Xtraction then dynamically writes the SQL to return the data. The coding is written behind the scenes. All the end-user needs to know is which field they wish to report on.

Out of the Box (OOTB) Dashboards and Documents

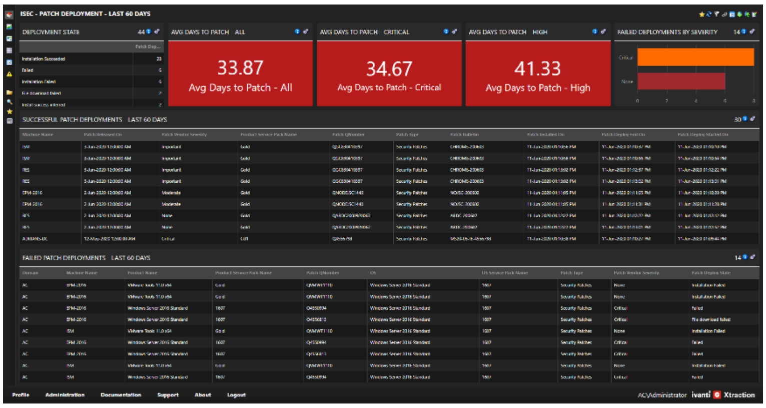
Deployment Success - Release Date Last 90 Days

- List of all Windows detected patches
  Targeted / Installed / Success Rate
- Windows Patches
  Targeted / Installed
- List of all Software detected patches
  Targeted / Installed / Success Rate
- Software Patches
  Targeted / Installed


DEPLOYMENT SUCCESS - RELEASE DATE LAST 90 DAYS
LAST 90 DAYS - WINDOWS PATCHES
LAST 90 DAYS - SOFTWARE PATCHES
Profile
Administration
Documentation
Support
About
Logout
AC\Administrator
ivanti
Xtraction

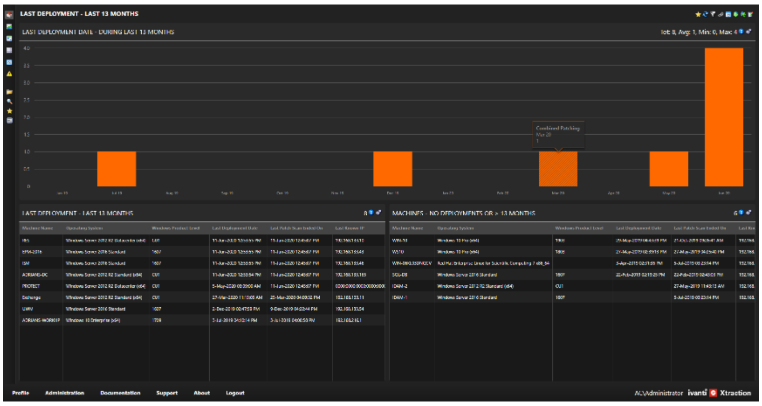
Patch Deployment – Last 60 Days

- All Patches Deployment State
- Avg Days to Patch from Publish Date
- Avg Days to Patch Critical Patches
- Avg Days to Patch Important Patches
- Failed Patch Deployments by Severity
- List of Successful Patch Deployments
- List of Unsuccessful Patch Deployments



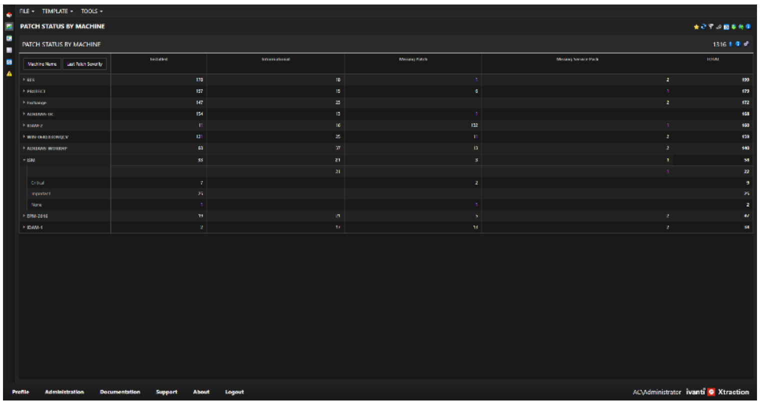
Last Deployment – Last 13 Months

- The last time a machine was deployed to.
- List of all machines that received a Deployment in the last 13 months along with date of deployment and last scan.
- List of all machines that have not received a Deployment in the last 13 months along with the last date of deployment if any and last scan.


LAST DEPLOYMENT - LAST 13 MONTHS
LAST DEPLOYMENT DATE - DURING LAST 13 MONTHS
LAST DEPLOYMENT - LAST 13 MONTHS
MACHINES - NO DEPLOYMENTS OR > 13 MONTHS
Profile
Administration
Documentation
Support
About
Logout
AC\Administrator
ivanti
Xtraction

Patch Status by Machine

- Pivot Table that shows Machine and Patch Severity from the Last Scan of that Machine. It then pivots on Install State

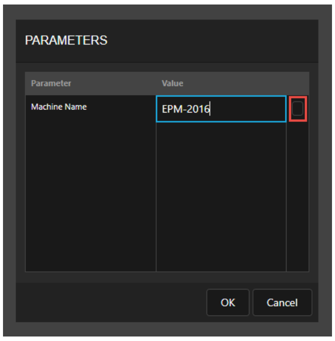


PATCH STATUS BY MACHINE

All Patches for a Machine

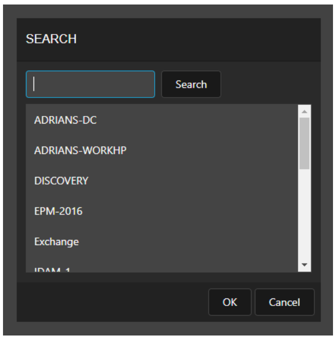
This is a document not a dashboard and has a different icon associated with it.

- By selecting the document, Xtraction will Ask for the Machine name
    - Either Enter Manually or
    - Click the Ellipse and select the Machine from the list



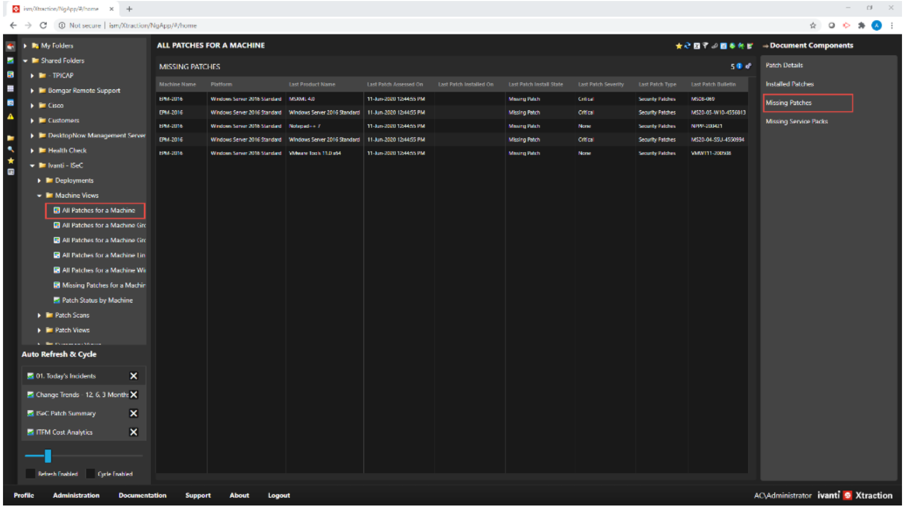
PARAMETERS

Parameter	Value
Machine Name	EPM-2016



SEARCH

ADRIANS-DC
ADRIANS-WORKHP
DISCOVERY
EPM-2016
Exchange



ALL PATCHES FOR A MACHINE

MISSING PATCHES

Machine Name	Platform	Last Product Name	Last Patch Assessed On	Last Patch Installed On	Last Patch Install State	Last Patch Severity	Last Patch Type	Last Patch Bulletin
EPM-2016	Windows Server 2016 Standard	MSXML 4.0	11-Jun-2020 12:44:55 PM		Missing Patch	Critical	Security Patches	MS08-069
EPM-2016	Windows Server 2016 Standard	Windows Server 2016 Standard	11-Jun-2020 12:44:55 PM		Missing Patch	Critical	Security Patches	MS20-05-W10-4556813
EPM-2016	Windows Server 2016 Standard	Notepad++ 7	11-Jun-2020 12:44:55 PM		Missing Patch	None	Security Patches	NPPP-200421
EPM-2016	Windows Server 2016 Standard	Windows Server 2016 Standard	11-Jun-2020 12:44:55 PM		Missing Patch	Critical	Security Patches	MS20-04-SSU-4550994
EPM-2016	Windows Server 2016 Standard	VMware Tools 11.0 x64	11-Jun-2020 12:44:55 PM		Missing Patch	None	Security Patches	VMWT11-200508

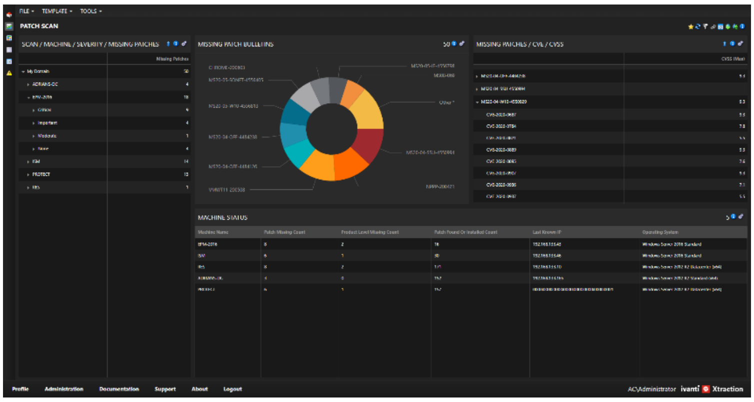
By selecting different components from the Document Components on the right, either

- All detected Patches
- Installed Patches
- Missing Patches
- Missing Service Packs

will be displayed.

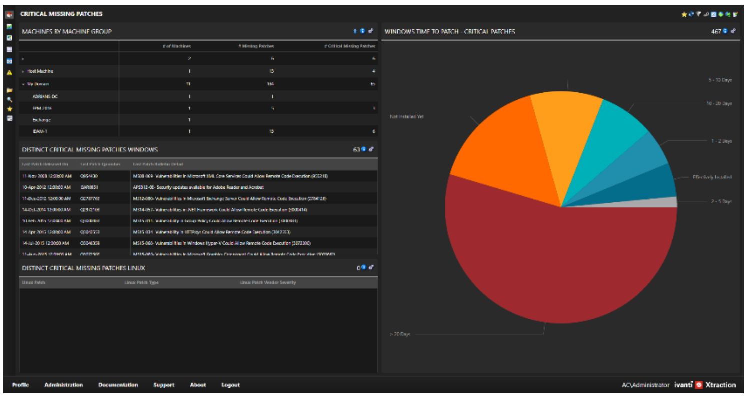
Patch Scan

- Scan Results by
  Machine Group / Machine / Bulletin
- Bulletins / Number of times detected
  in all Scans
- Missing Patches / Related CVE / CVSS
- Current Machine Status
  Missing Patch Count, Installed Patch Count,
  Product Level – Service Pack Missing Count


PATCH SCAN
SCAN / MACHINE / SEVERITY / MISSING PATCHES
MISSING PATCH BULLETINS
MISSING PATCHES / CVE / CVSS
MACHINE STATUS

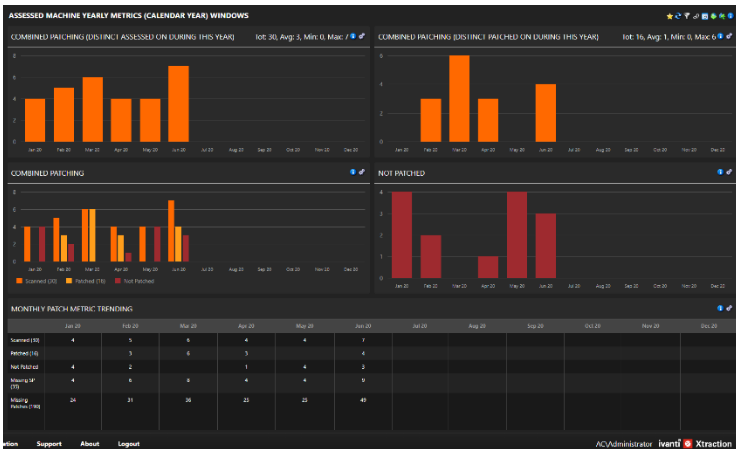
Critical Missing Patches

- Machine Group / Machine
  No. of Machines in the Group
  Missing Patches by Group and Machine
  Missing Critical Patches by Group and
  Machine
- Time to Patch Critical Patches grouped
  by time periods
- Distinct Missing Critical Windows Patches
- Distinct Missing Critical Linux Patches


CRITICAL MISSING PATCHES
MACHINES BY MACHINE GROUP
WINDOWS TIME TO PATCH - CRITICAL PATCHES
DISTINCT CRITICAL MISSING PATCHES WINDOWS
DISTINCT CRITICAL MISSING PATCHES LINUX

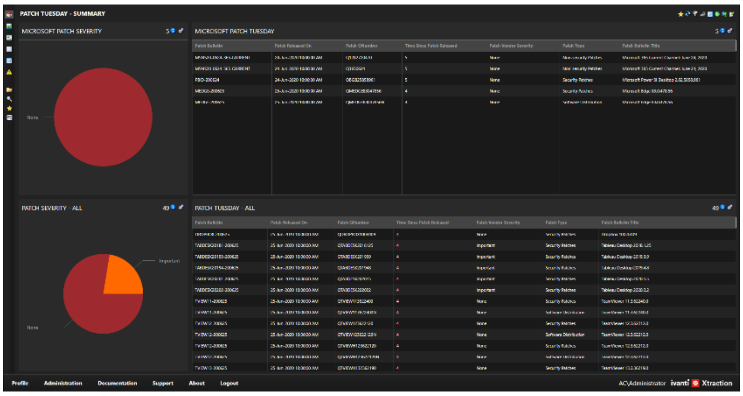
Assessed Machine Yearly Metrics

- Distinct No. of Machines Scanned Per Month
- Distinct No. of Machines with at Least One
  Deployment Per Month
- Number of Distinct Machines Scanned /
  Deployments / Scanned but No Deployment
- Machines Scanned but no Deployment
- Breakdown of Scans / Deployments Detected
  Patches and Service Packs by Month


ASSESSED MACHINE YEARLY METRICS (CALENDAR YEAR) WINDOWS
COMBINED PATCHING (DISTINCT ASSESSED ON DURING THIS YEAR)
COMBINED PATCHING (DISTINCT PATCHED ON DURING THIS YEAR)
COMBINED PATCHING
NOT PATCHED
MONTHLY PATCH METRIC TRENDING

Patch Tuesday – Summary

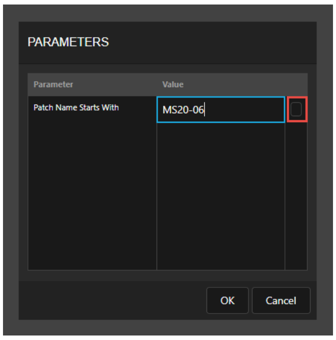
- Microsoft Patches from the Last Release By Severity
- List of Microsoft Patches from the Last Release
- Non-Microsoft Patches from the Last Release By Severity
- List of Non-Microsoft Patches from the Last Release



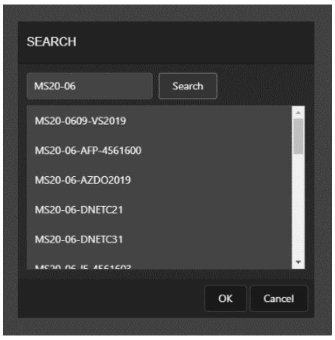
Patch State on Machines

This is a document not a dashboard and has a different icon associated with it.

- By selecting the document, Xtraction will Ask for the Bulletin name
    - ○ Either Enter Manually (Part or Full) By entering on part such as MS20-06 Xtraction will return all results for June 2020 release.
    - ○ Click the Ellipse and select the Bulletin from the list, filter if required

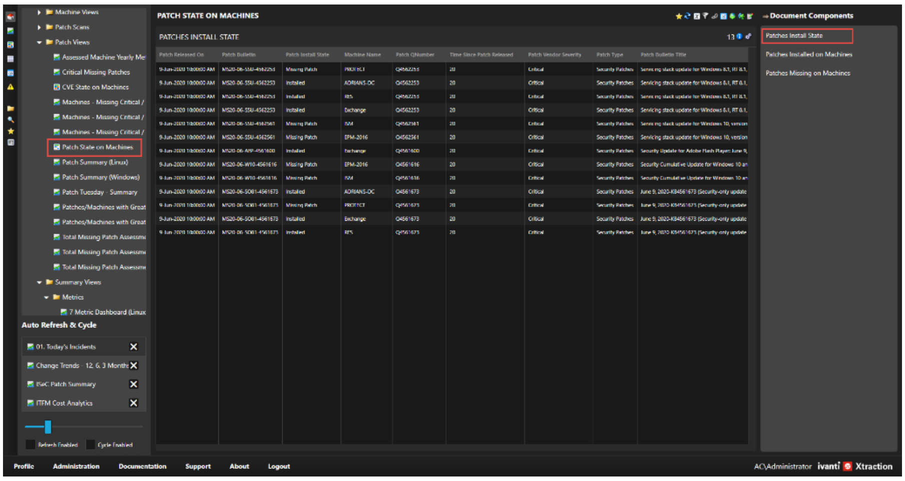


Patch Name Starts With: MS20-06



MS20-06

MS20-0609-VS2019
MS20-06-AFP-4561600
MS20-06-AZDO2019
MS20-06-DNETC21
MS20-06-DNETC31



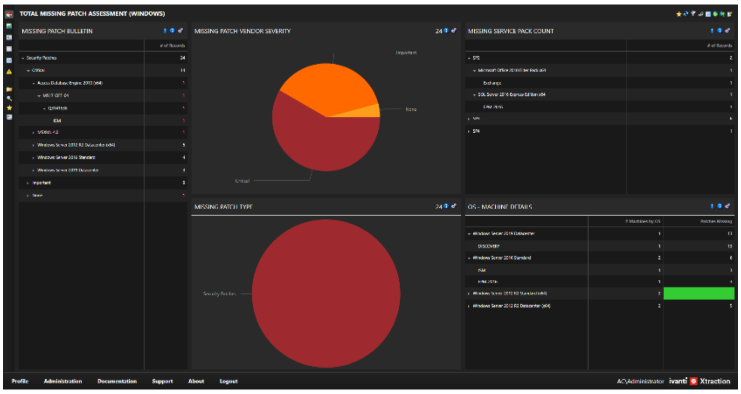
By selecting different components from the Document Components on the right, either

- All detected Patches
- Installed Patches
- Missing Patches

will be displayed.

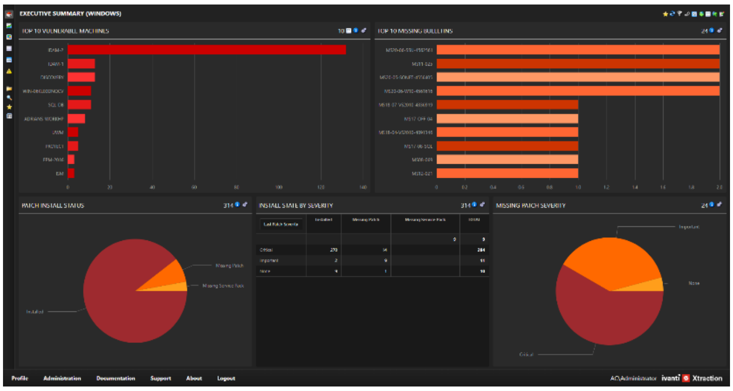
Total Missing Patch Assessment

- Missing Patch Bulletin by Severity / Bulletin / Title / Machine
- Severity of Missing Patches
- Missing Service Packs / Versions / Machine
- Patch Type of Missing Patches
- OS Count and Missing Patch Count on OS Version / Machine



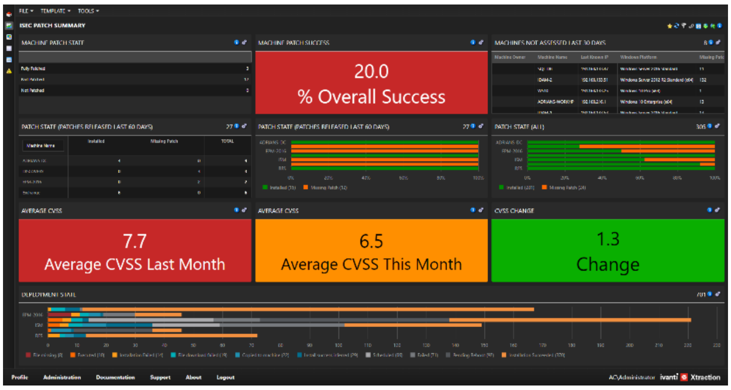
Executive Summary

- Top 10 Vulnerable Machines Based on Missing Patch Count and Criticality
- Top 10 Missing Bulletins Based Missing Patch Count
- Detected Patch Install State from Last Scan for Each Machine
- Severity Pivoting on Last Install State
- Missing Patches Based on Severity



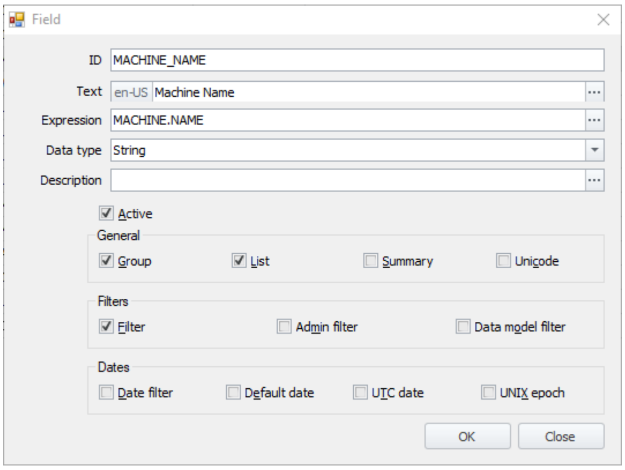
Patch Summary

- No. of Fully / Part / Not Patched Machines
- Percentage of Fully Patched Machines
- List of Machines Not Scanned in 30 Days
- Patch State for Machines Scanned in the Last 30 Days for Patches Published in the Last 60 Days
- Patch State for Patches Published in the Last 60 Days
- Patch State for All Detected Patches
- Average CVSS for Missing Patches Last Month
- Average CVSS for Missing Patches This Month
- Positive or Negative Movement in CVSS
- Deployment Status on All Machines with Deployments in the Last 30 Days



Attribute Definitions and Examples

Each field or column from the database that is mapped in the datamodel can have one or many attributes:



ID: MACHINE_NAME

Text: en-US Machine Name

Expression: MACHINE.NAME

Data type: String

Description:

☑ Active

General

☑ Group ☑ List ☐ Summary ☐ Unicode

Filters

☑ Filter ☐ Admin filter ☐ Data model filter

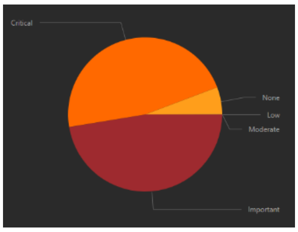
Dates

☐ Date filter ☐ Default date ☐ UTC date ☐ UNIX epoch

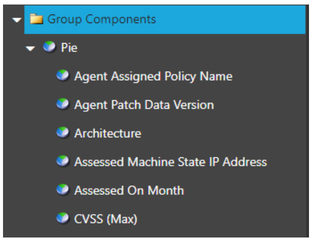
Below is a list, description and sample of each field attribute

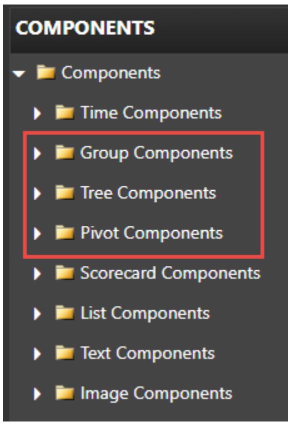
Attribute: **Group**

A non-unique field that can be grouped on such as **Vendor Severity**.



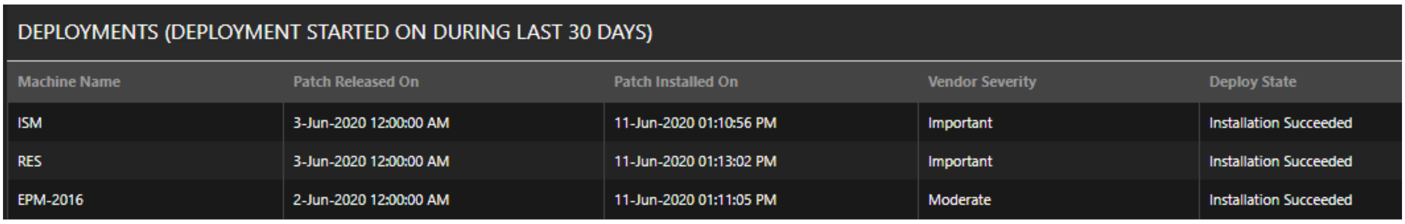
Fields appear in the Group, Tree and Pivot Components





Attribute: **List**

A field that is included in or can be added to a list, this will include almost all fields.

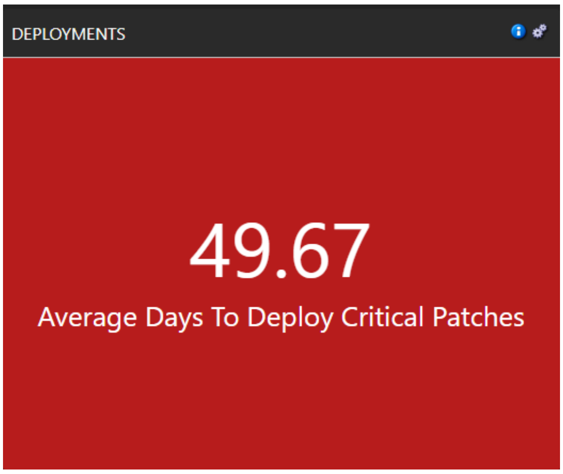


DEPLOYMENTS (DEPLOYMENT STARTED ON DURING LAST 30 DAYS)

Machine Name	Patch Released On	Patch Installed On	Vendor Severity	Deploy State
ISM	3-Jun-2020 12:00:00 AM	11-Jun-2020 01:10:56 PM	Important	Installation Succeeded
RES	3-Jun-2020 12:00:00 AM	11-Jun-2020 01:13:02 PM	Important	Installation Succeeded
EPM-2016	2-Jun-2020 12:00:00 AM	11-Jun-2020 01:11:05 PM	Moderate	Installation Succeeded

Attribute: **Summary**

A numerical field that can be used in a calculation such as **Time Since Patch Released (Days)** or **Missing Patch Count.**



DEPLOYMENTS

49.67

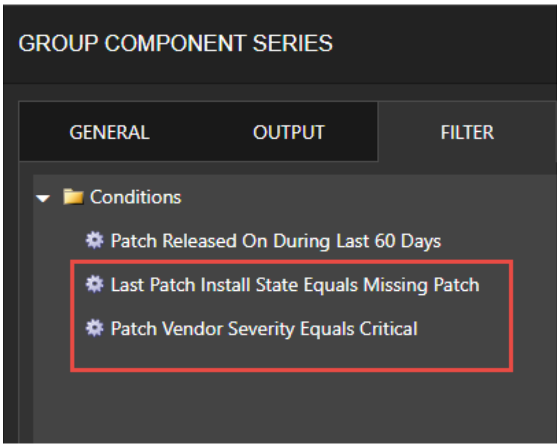
Average Days To Deploy Critical Patches

Attribute: **Unicode**

Rarely Used, designed for international characters sets.

Attribute: **Filter**

A field that can be filtered on, this will include most fields.



GROUP COMPONENT SERIES

Conditions

- Patch Released On During Last 60 Days
- Last Patch Install State Equals Missing Patch
- Patch Vendor Severity Equals Critical

Attribute: **Admin Filter**

When checked and no other filter checked, filter will only be visible and accessible by Admins.

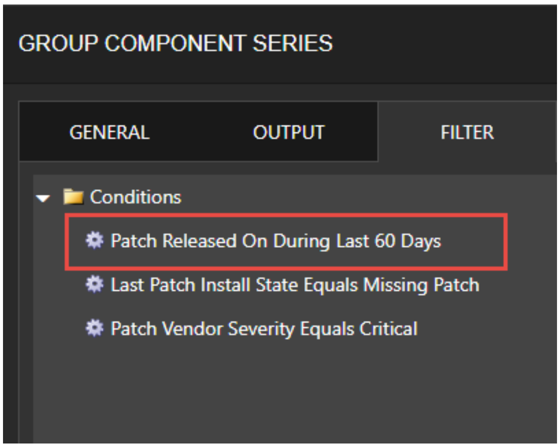
Attribute: **Data Model Filter**

When checked and no other filter checked, filter will only be visible and accessible within the data model, it will not be available in the front end.

Attribute: **Date Filter**

A field that can be used in a date range filter

Eg. **Patch Released On** During Last 60 Days.

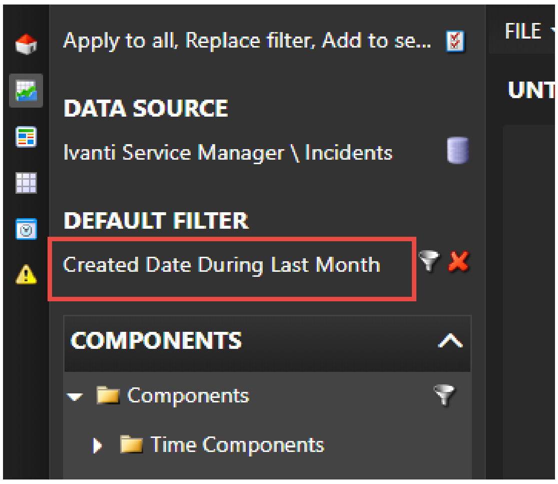


GROUP COMPONENT SERIES

Conditions
- Patch Released On During Last 60 Days
- Last Patch Install State Equals Missing Patch
- Patch Vendor Severity Equals Critical

Attribute: **Default Date**

The **Date Field** used in the **Default Filter** when selecting the Datasource in the front end of Xtraction. If more than one **Default Date** is selected, the first sequentially appearing field will be used by Xtraction. If no **Default Date** field is selected then no **Default Filter** will appear.



Apply to all, Replace filter, Add to se...

DATA SOURCE

Ivanti Service Manager \ Incidents

DEFAULT FILTER

Created Date During Last Month

COMPONENTS

Components
- Time Components

Attribute: **UTC Date**

UTC Dates are used in many applications, when selected, Xtraction will presume the date stored is in UTC or GMT+0. Xtraction will then convert the time relative to the location of the person logged on.

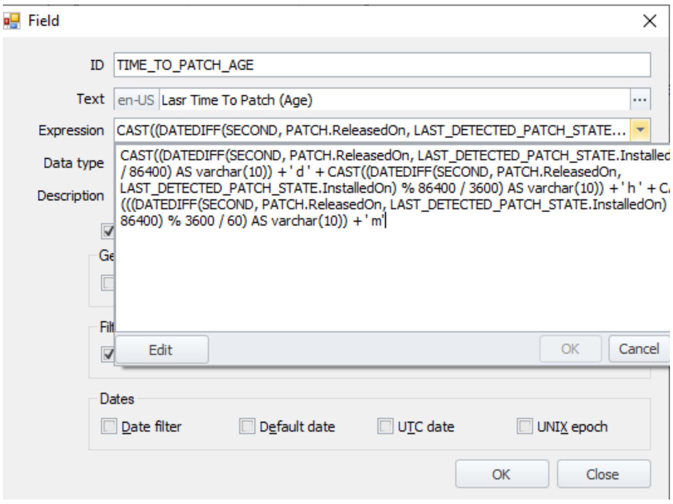
Attribute: **Unix Epoch**

Converts the field from a Unix Epoch format (an integer value that represents the number of seconds between 01/01/1970 00:00:00 and the point in time it was stored) to a readable date format.

Derived Values

Xtraction can derive values using fields in calculations.

In this example, Xtraction is measuring the time since a patch was released and when it was installed then converting it into a readable format of days, hours and minutes. Any expression that will run in SQL Server can be inserted into Xtraction.



ID: TIME_TO_PATCH_AGE

Text: en-US Lasr Time To Patch (Age)

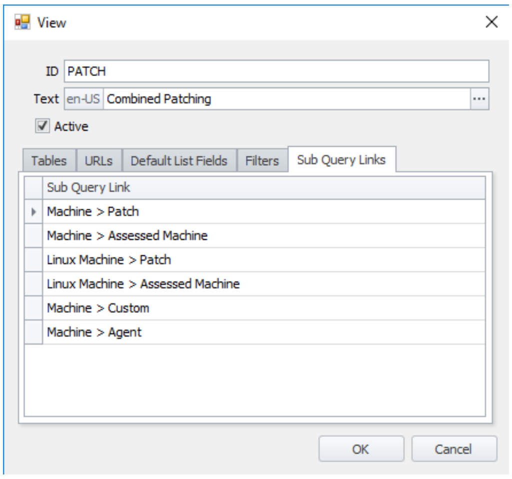
Expression: CAST((DATEDIFF(SECOND, PATCH.ReleasedOn, LAST_DETECTED_PATCH_STATE...

```
CAST((DATEDIFF(SECOND, PATCH.ReleasedOn, LAST_DETECTED_PATCH_STATE.Installe
/ 86400) AS varchar(10)) + ' d ' + CAST((DATEDIFF(SECOND, PATCH.ReleasedOn,
LAST_DETECTED_PATCH_STATE.InstalledOn) % 86400 / 3600) AS varchar(10)) + ' h ' + C
(((DATEDIFF(SECOND, PATCH.ReleasedOn, LAST_DETECTED_PATCH_STATE.InstalledOn)
86400) % 3600 / 60) AS varchar(10)) + ' m'
```

Dates

☐ Date filter ☐ Default date ☐ UTC date ☐ UNIX epoch

Sub Query Links



ID PATCH

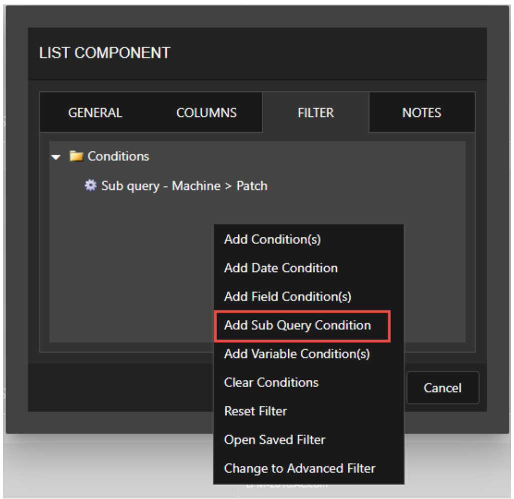
Text en-US Combined Patching

☑ Active

Sub Query Link
Machine > Patch
Machine > Assessed Machine
Linux Machine > Patch
Linux Machine > Assessed Machine
Machine > Custom
Machine > Agent

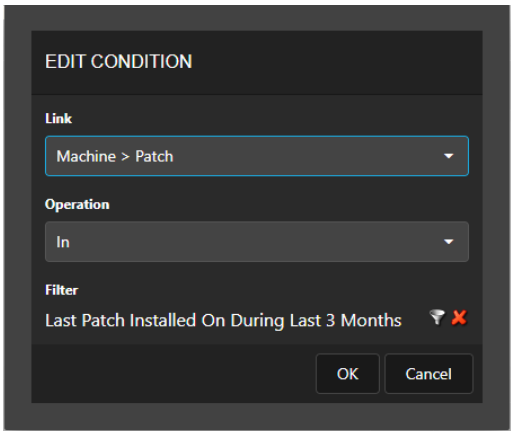
Where are they?

In the data model, the list of **Sub Query Links** is located in each view under the **Sub Query Links** tab.



In the Xtraction application, if there are Sub Queries available,

they will be accessible in the filters tab on any component.



Link: Machine > Patch

Operation: In

Filter: Last Patch Installed On During Last 3 Months

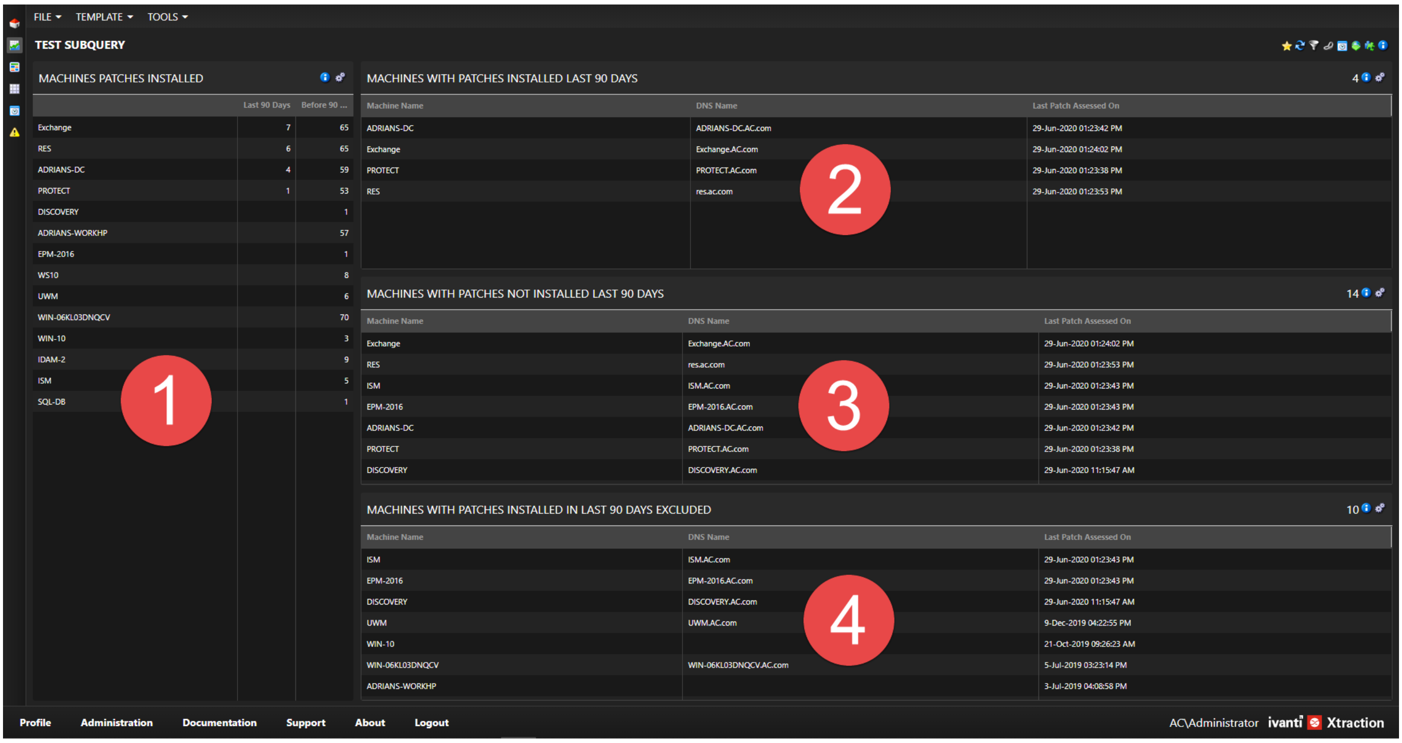
Select the appropriate link, in the **Operation**,

Select either **In** or **Not In** and apply a relevant filter.

What are they and what do they do?

Let’s look at an example below:

1. This component shows all machines that have had patches installed in the last 90 days and those that have had patches installed at any other time apart from the last 90 days. There are machines that fall into multiple categories. In addition, the result set displays the number of patches installed.
2. Without Sub Queries, if the component had a filter for installed patches in the last 90 days, then there would be 18 entries in this component. By using the Sub Query **Machine > Patches** and the filter, **Last Patch Installed During in the last 90 days**, the result set only returns the unique 4 machine records.
3. In the 3rd component, by using the Sub Query **Machine > Patches** and the filter, **Last Patch Installed NOT During in the last 90 days** the result set returns 14 records, it also includes the 4 machines that appear in both record sets.
4. In the 4th component, 2 instances of the Sub Query **Machine > Patches** are used, one with the **Operation** attribute **In** using the filter **Last Patch Installed NOT During in the last 90 days** and one with the **Operation** attribute **Not In** using the filter **Last Patch Installed During in the last 90 days.** The result set includes only the machines that do not appear in both records sets.



TEST SUBQUERY

MACHINES PATCHES INSTALLED

	Last 90 Days	Before 90 ...
Exchange	7	65
RES	6	65
ADRIANS-DC	4	59
PROTECT	1	53
DISCOVERY		1
ADRIANS-WORKHP		57
EPM-2016		1
WS10		8
UWM		6
WIN-06KL03DNQCV		70
WIN-10		3
IDAM-2		9
ISM		5
SQL-DB		1

MACHINES WITH PATCHES INSTALLED LAST 90 DAYS 4

Machine Name	DNS Name	Last Patch Assessed On
ADRIANS-DC	ADRIANS-DC.AC.com	29-Jun-2020 01:23:42 PM
Exchange	Exchange.AC.com	29-Jun-2020 01:24:02 PM
PROTECT	PROTECT.AC.com	29-Jun-2020 01:23:38 PM
RES	res.ac.com	29-Jun-2020 01:23:53 PM

MACHINES WITH PATCHES NOT INSTALLED LAST 90 DAYS 14

Machine Name	DNS Name	Last Patch Assessed On
Exchange	Exchange.AC.com	29-Jun-2020 01:24:02 PM
RES	res.ac.com	29-Jun-2020 01:23:53 PM
ISM	ISM.AC.com	29-Jun-2020 01:23:43 PM
EPM-2016	EPM-2016.AC.com	29-Jun-2020 01:23:43 PM
ADRIANS-DC	ADRIANS-DC.AC.com	29-Jun-2020 01:23:42 PM
PROTECT	PROTECT.AC.com	29-Jun-2020 01:23:38 PM
DISCOVERY	DISCOVERY.AC.com	29-Jun-2020 11:15:47 AM

MACHINES WITH PATCHES INSTALLED IN LAST 90 DAYS EXCLUDED 10

Machine Name	DNS Name	Last Patch Assessed On
ISM	ISM.AC.com	29-Jun-2020 01:23:43 PM
EPM-2016	EPM-2016.AC.com	29-Jun-2020 01:23:43 PM
DISCOVERY	DISCOVERY.AC.com	29-Jun-2020 11:15:47 AM
UWM	UWM.AC.com	9-Dec-2019 04:22:55 PM
WIN-10		21-Oct-2019 09:26:23 AM
WIN-06KL03DNQCV	WIN-06KL03DNQCV.AC.com	5-Jul-2019 03:23:14 PM
ADRIANS-WORKHP		3-Jul-2019 04:08:58 PM

Sub Queries are ideal for returning distinct values of objects, this example returns unique machines, however it could quite easily be used to return distinct patches, CVEs or even Domains.

Views and Subqueries in the Security Controls datamodel

View	Report Description	Sub Queries
Machine	All related machine data such Make, Model, OS, Architecture and Agents	None
Patches to Machine	From the Patch perspective, the Bulletin, QNumber, Published Date, one to many relationship with machines, how many machines require the patch and how many have it installed	Patch > Machine
Windows Patching (Current)	From the Windows Machine perspective, what machine, when each detected patch was assessed, its current state as per the last assessment for any individual patch.	Machine > Patch Count Machine > Assessed Machine Machine > Agent Machine > Total Count
Windows Patching (All)	From the Windows Machine perspective. All scans made on that machine and the assessed state of any patch detected.	Machine > Custom Machine > Assessed Machine Machine > Agent Machine > Last Deployment
Windows Patching (Latest)	From the Windows Machine perspective, what machine, when was it last assessed. Returned results for only the last assessment for each machine and only for the patches scanned in the last assessment.	Machine > Patch Machine > Assessed Machine Machine > Agent Machine > Custom
Linux Patching (Current)	From the Linux Machine perspective, what machine, when each detected patch was assessed, its current state as per the last assessment for any individual patch.	Linux Machine > Patch Linux Machine > Assessed Machine Linux Machine > Agent Linux Machine > Custom
Linux Patching (All)	From the Linux Machine perspective. All scans made on that machine and the assessed state of any patch detected.	Linux Machine > Patch Linux Machine > Assessed Machine Linux Machine > Agent Linux Machine > Custom
Linux Patching (Latest)	From the Linux Machine perspective, what machine, when was it last assessed. Returned results for only the last assessment for each machine and only for the patches scanned in the last assessment.	Linux Machine > Patch Linux Machine > Assessed Machine Linux Machine > Agent Linux Machine > Custom
Event	Events Raised by Application Control	None
AC Configuration	Configuration of Application Control	None
Asset	Hardware Asset Management	None
SAM	Software Asset Management	None
Patches	Patches and their Related CVEs and CVSS	None
Patch Scans	From the Patch Scan perspective, one to many relationship with machines and a one to many relationship from machines to detected patches	None
Deployments	From the Deployment perspective, for any deployment when was it scheduled, when did it start and end, what machines were involved and what patches were deployed to which machine. Finally was it completely, partly or not at all successful?	None

Vulnerabilities	CVEs and their Related Patches	None
Top 10 Vulnerable Machines	Top 10 Vulnerable Machines	None

Important note: Current (Linux and Windows Patching) returns the current state of the machine with the results of the last time each patch was scanned for.

All (Linux and Windows Patching) returns the state of each patch every single time that it had been scanned for on each machine.

Latest (Linux and Windows Patching) returns the state of only the patches that were scanned for on the last scan for each machine.

Glossary

Dashboard	Container displaying one or more Components of any type – Dashboards are targeted primarily for onscreen viewing The Dashboard designer determines what to display and how to display it; with the number of Components limited by the need for onscreen display
Document	Container displaying one or more Components of any type – Documents are targeted primarily for export to external applications A document can make use of an attached MS Word document to impose predefined formatting on the output The document designer makes all design decisions based on the target application, which may include Word, PDF, HTML and more
Connector	A data model to a specific database.
Datamodel	The DataModel.dat file that acts as an interpreter to the database(s) it is pointing to. A datamodel can consist of one or more Connectors.
Group Component	Summarises data by one or more fields from the Data Source Group Components may have multiple independent series, each coming from different Data Sources
Time Component	Visually represents data using time slices segregated by hours, days, weeks, months, etc; these can be presented in many formats including area, bar and line charts; or in stacked and 100% stacked formats, which enables the data to be portrayed in comparative context
Tree Component	Like the Group Component it displays a summary of data, but in this case you can add multiple fields and display the summary result as a hierarchy.
Pivot Component	Supports a multi-dimensional pivot by employing a row and column pivot Pivot Components support either group or time pivots
Scorecard Component	Summarises an entire data set providing a single result instead of slicing by time or group as in the above components
List Component	Displays raw data from Data Sources without performing any summarisation
Text Component	A simple component to allow text string to be shown. Can be formatted as a URL to allow the URL to be opened in a new browser window.
Image Component	Displays an image from the server or from a URL
Field	Name of a column in a table in a relational database
Row	A row of related data in a table in a relational database
ResultSet	The data returned from a database after running a query
Sub Query	A query nested inside a SQL query or another subquery to return a specific ResultSet
Datatype	A particular kind of data such as a date, integer or varchar. All fields must have a datatype defined in order to store them in the database.
Query	A script that runs to return a ResultSet