IVANTI XTRACTION - Connector

Endpoint Manager (EPM)

Technical Documentation

10/10/2022

Table of Contents

Requirements

- Ivanti Endpoint Manager (EPM) 2016.1 – 2022.3
  (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.
- Ivanti Xtraction installed – Any version.
- Port 1433 (or Custom if Used) port open between the Xtraction server and the EPM database.
- Read-Only account to the EPM database (May be Domain or SQL Account).

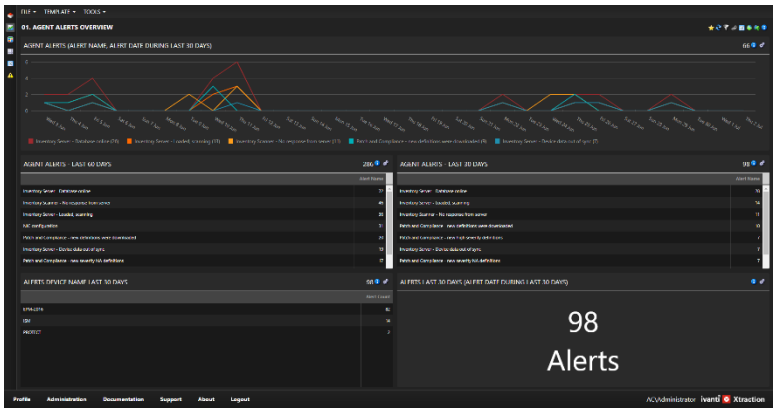
Description

- The EPM Connector allows, through the Xtraction application for data in the EPM 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

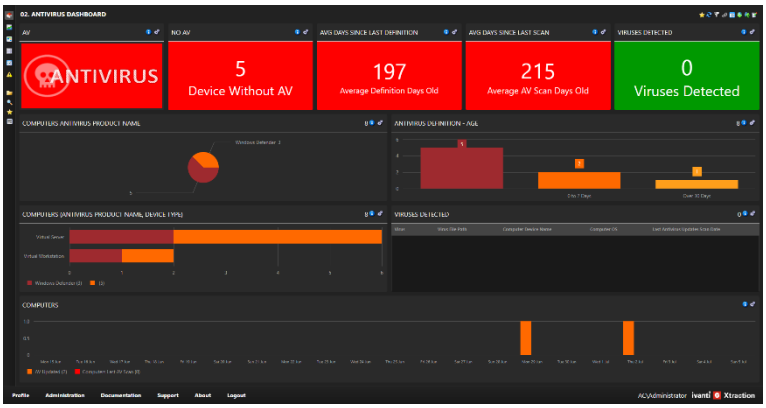
Agent Alerts

- Pivot Table – Alerts / Dates Last 30 Days
- Grouped Count of Alerts Last 60 Days
- Grouped Count of Alerts Last 30 Days
- Grouped Count of Machines with Alerts Last 30 Days
- Total Number of Alerts Last 30 Days



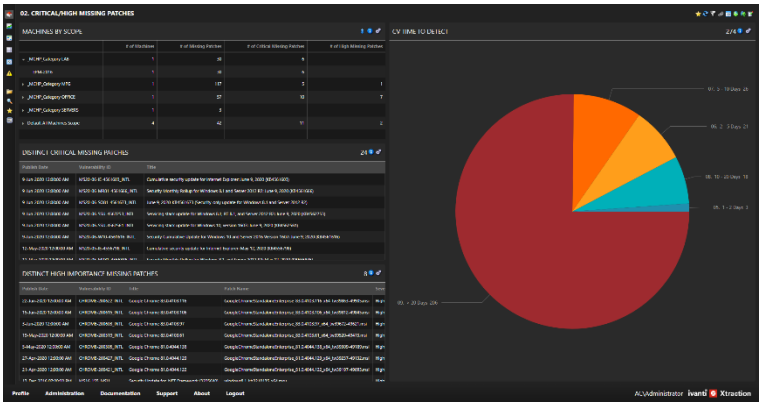
Antivirus Dashboard

- Devices without Antivirus
- Avg Days Since Last Definition
- Avg Days Since Last Scan
- No. of Viruses Detected
- Antivirus Product Installed
- Computers Type and AV Product
- List of Detected Viruses
- Timeline on Last AV Scan



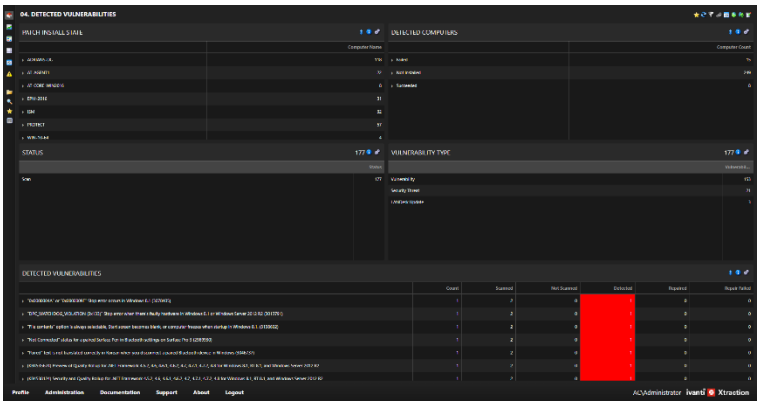
Critical / High Missing Patches

- Scopes / Machines
  Total Missing Patches
  Missing Critical Patches
  Missing High Patches
- Time to Detect CV from Publish Date
- List of Distinct Missing Critical Patches
- List of Distinct Missing High Patches



Detected Vulnerabilities

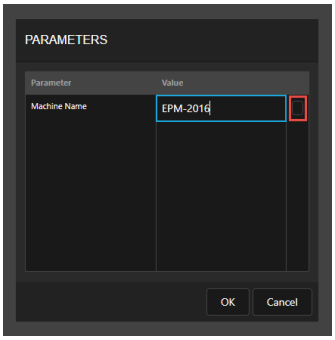
- Path Install State
- Computers with Detected Vulnerabilities Install State
- Status for Detected Vulnerabilities
- Detected Vulnerability Type
- List of Vulnerabilities and their State of Repair

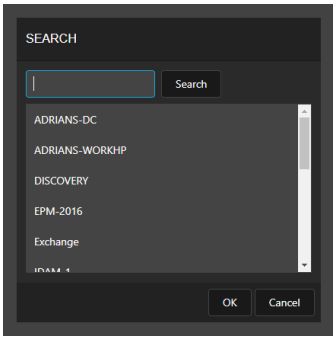


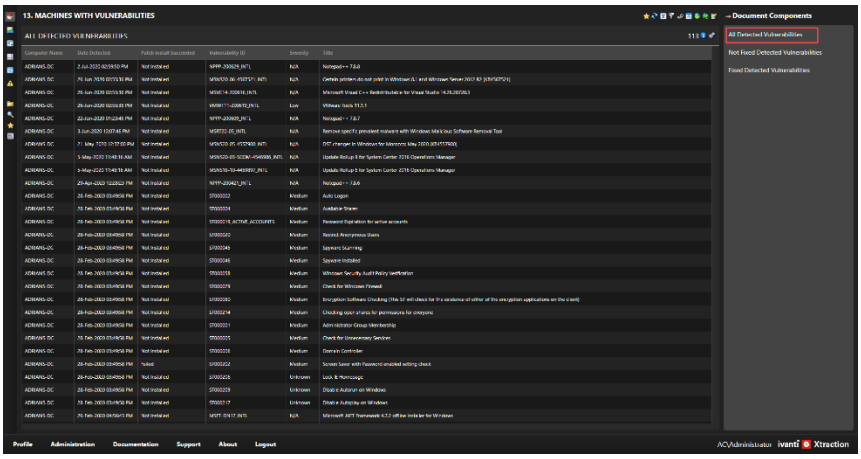
Machines with Vulnerabilities

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







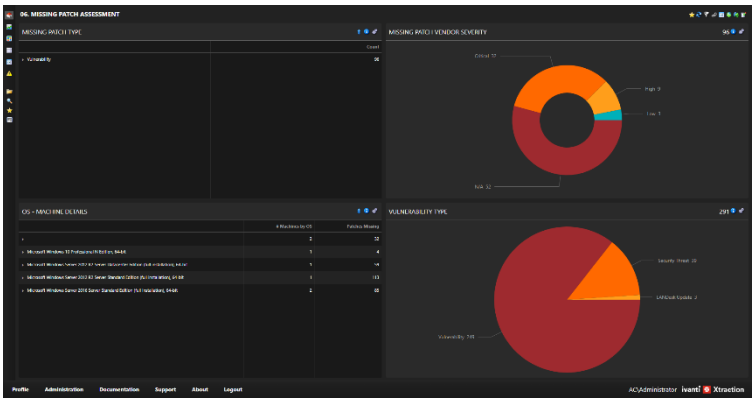
By selecting different components from the Document Components on the right, either

- All detected Vulnerabilities
- Not Fixed Detected Vulnerabilities
- Fixed Detected Vulnerabilities

will be displayed.

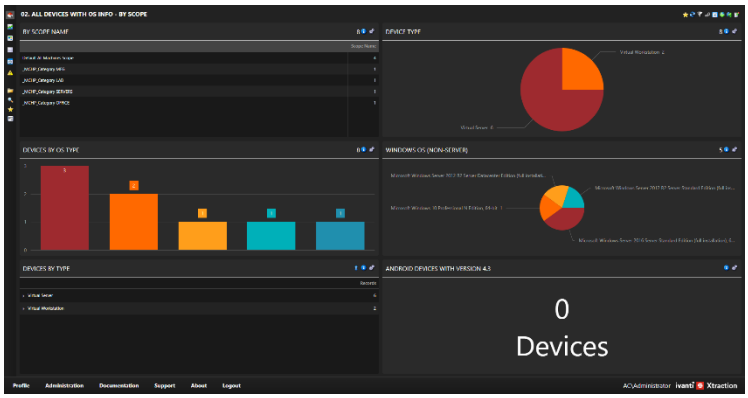
Missing Patch Assessment

- Vulnerability Type, Severity and Count
- Vendor Severity
- Missing Patches by OS
- Vulnerability Type



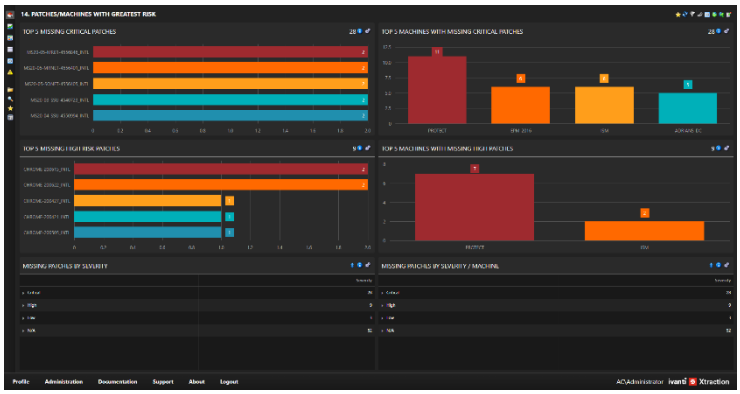
OS Info

- Scope
- Device Type
- Devices by OS Type
- Windows OS Non-Server
- Devices By Type
- Android Devices with Version 4.3



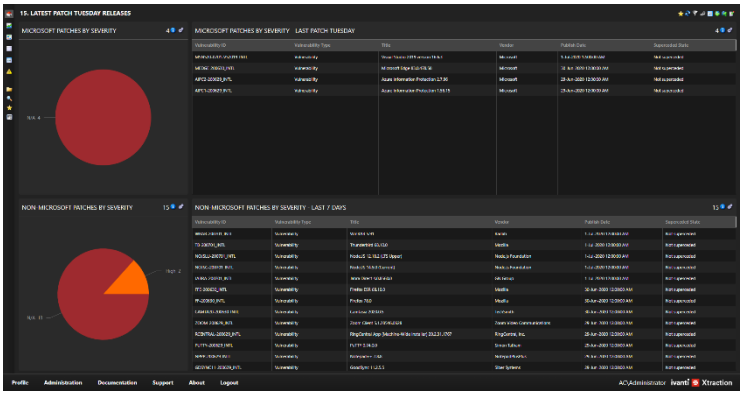
Patches/Machines with Greatest Risk

- Top 5 Missing Critical Patches
- Top 5 Machines with Missing Critical Patches
- Top 5 Missing High-Risk Patches
- Top 5 Machines with Missing High-Risk Patches
- Missing Patches by Severity
  Missing Patches by Severity / Machine



Patch Tuesday – Summary

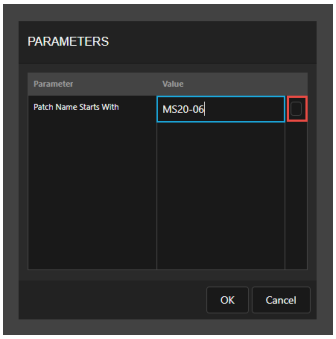
- Microsoft Patches from the Last Release By Severity
- List of Microsoft Patches from the Last Release
- Non-Microsoft Patches from the Last Release By Severity
- List of Non-Microsoft Patches from the Last Release

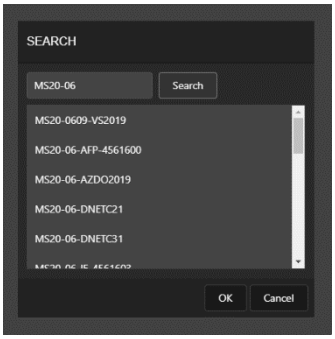


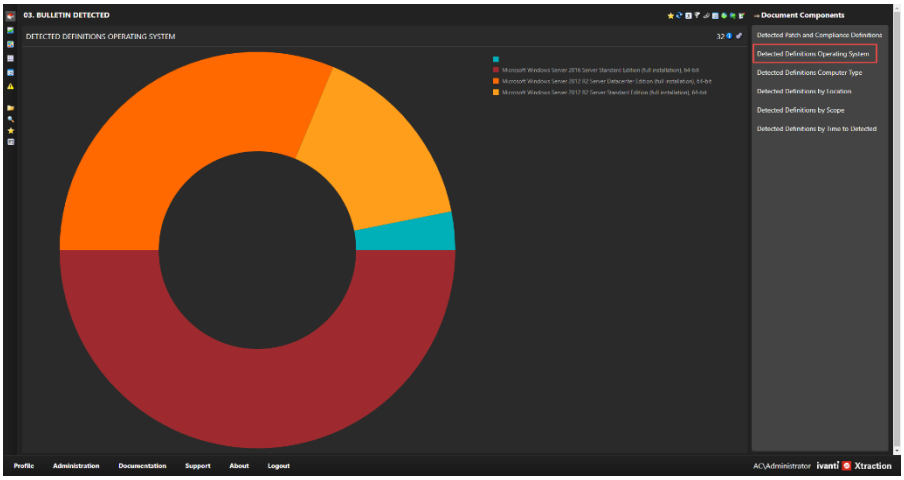
Bulletin Detected

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







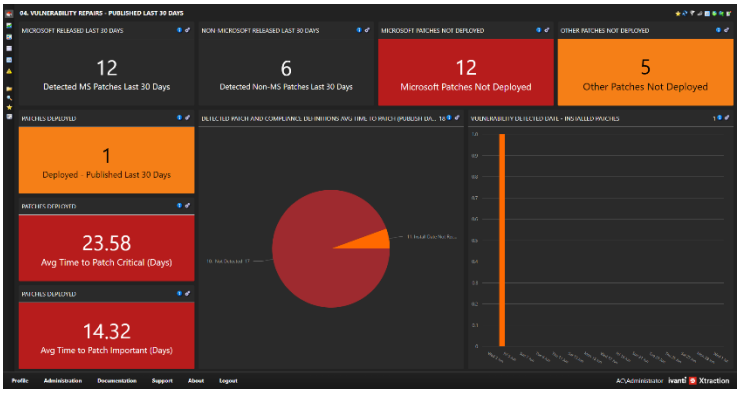
By selecting different components from the Document Components on the right, either

- All Detected Patch and Compliance Definitions
- Detected Definitions OS
- Detected Definitions Device Type
- Detected Definitions by Location
- Detected Definitions by Scope
- Detected Definitions by Time to Detected

will be displayed.

Vulnerability Repairs – Published Last 30 Days

- Detected MS Patches last 30 Days
- Detected Non-MS Patches last 30 Days
- Microsoft Patches Not Deployed
- Other Patches Not Deployed
- Deployed – Published Last 30 Days
- Avg Time To Patch
- Installed Patch Timeline
- Avg Time to Patch Critical
- Avg Time to Patch Important



Software Distribution

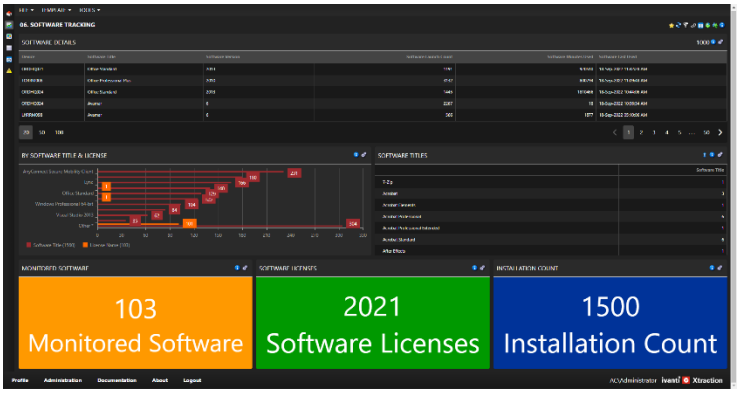
- Overall Success Rate
- Tasks this Year
- Tasks this Quarter
- Tasks this Week
- Push Tasks Success Rate
- Task / Machine Status
- Delivery Type
- Task Success This Month
- Task Success Last 13 Months

Executive Dashboard - Security

- Antivirus Auto Protect
- Missing Service Pack
- Computers without Antivirus
- Avg Antivirus Definition Age
- Total Missing Patches
- Missing Critical and High Patches
- Antivirus Product Names
- Average AV Definition Age
- Top 5 Vulnerable Devices
- Top 5 Detected Vulnerabilities
- AV Computer Type
- Days since Last AV Scan
- Top Vendor Missing Patch

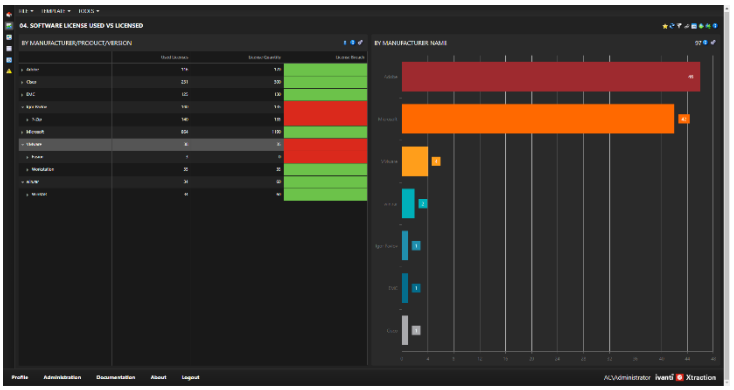
Software Tracking

- Software Name and when it last used
- How many times software is launched
- No. of Minutes Software is used for
- No. Machines software is installed on
- Software and the No. of versions
- Count of Distinct Software installed
- Count of Software Licenses Owned
- Installation Count



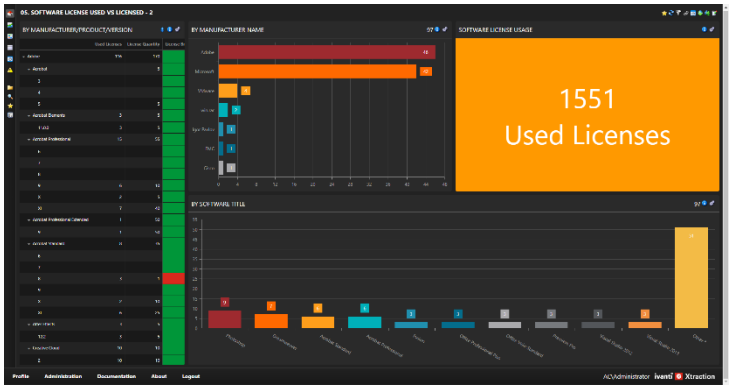
Software Licences

- Used vs Licensed
- Manufacturer / Title / Version
- Product Count by Manufacturer



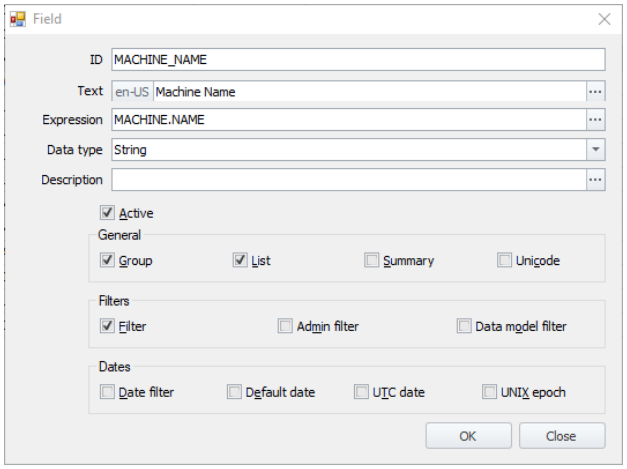
Software Licences Used vs Licensed

- Used vs Licensed
- Manufacturer / Title / Version
- Product Count by Manufacturer
- Count of Software Licenses Used
- Product Version Count



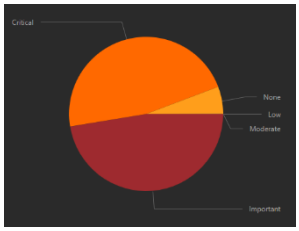
Attribute Definitions and Examples

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



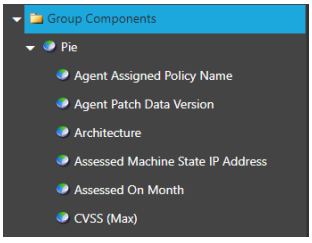
Below is a list, description and sample of each field attribute

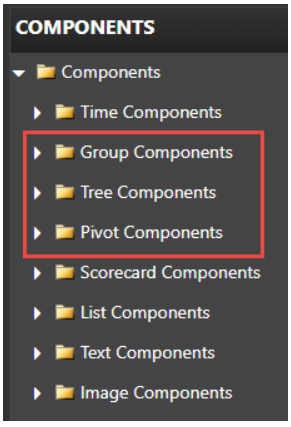
Attribute: **Group**



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

Fields appear in the Group, Tree and Pivot Components





Attribute: **List**

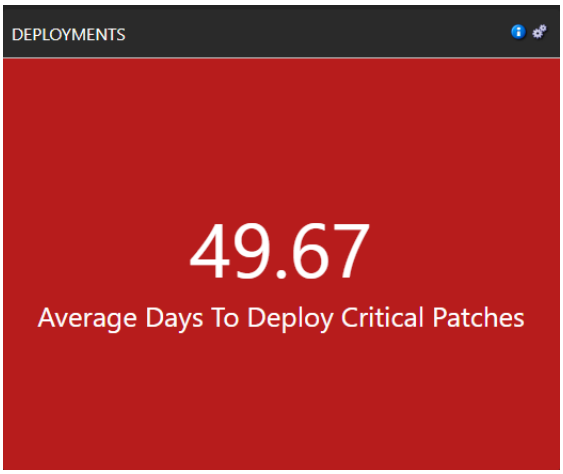
A field that is included in or can be added to a list, this will include almost all fields.

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.**

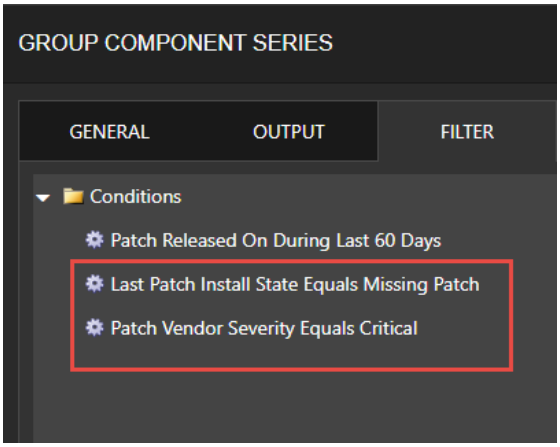


Attribute: **Unicode**

Rarely Used, designed for international characters sets.

Attribute: **Filter**

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



Attribute: **Admin Filter**

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

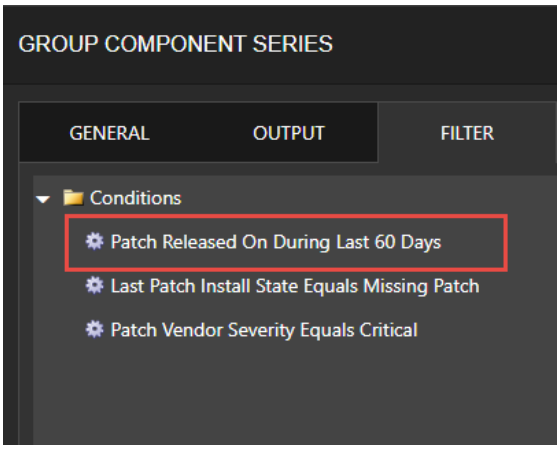
Attribute: **Data Model Filter**

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**

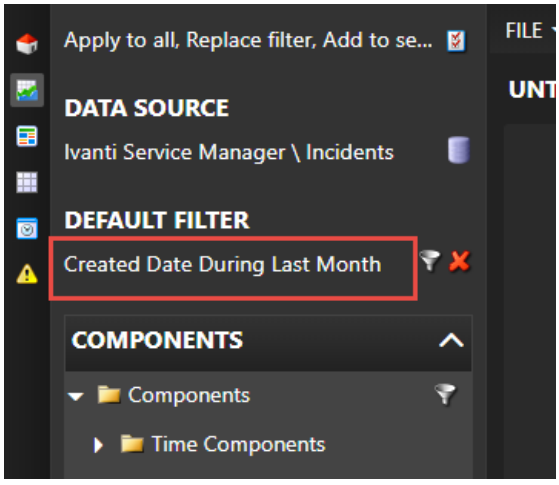
A field that can be used in a date range filter

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



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.



Attribute: **UTC Date**

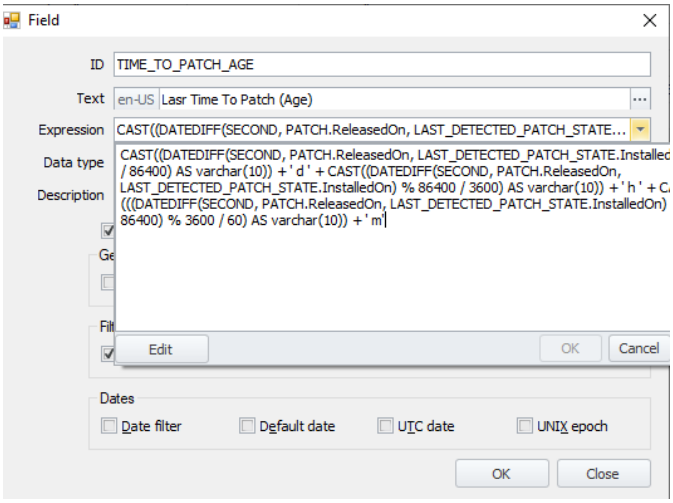
UTC Dates are used in many applications, when selected, Xtraction will presume the date stored is in UTC or GMT+0. Xtraction will then convert the time relative to the location of the person logged on.

Attribute: **Unix Epoch**

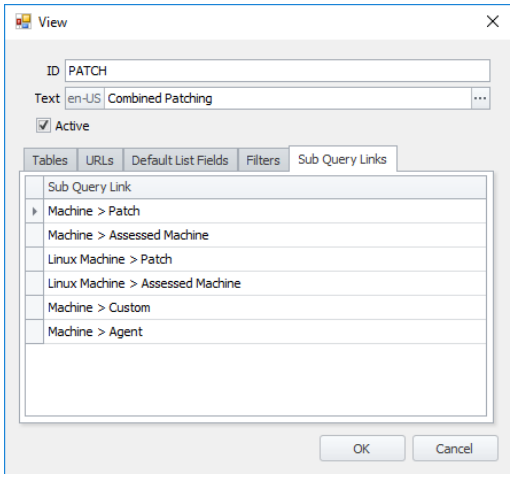
Converts the field from a Unix Epoch format (an integer value that represents the number of seconds between 01/01/1970 00:00:00 and the point in time it was stored) to a readable date format.

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.

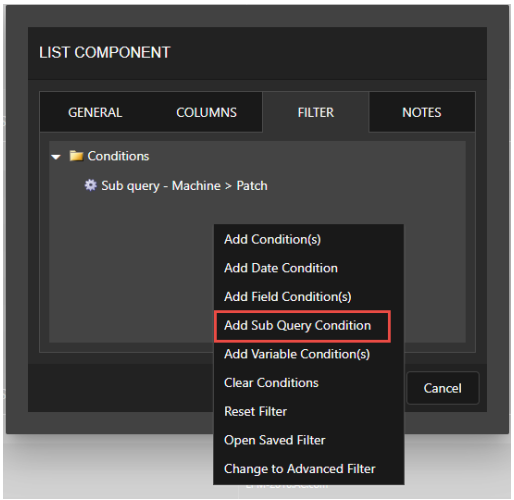


Sub Query Links



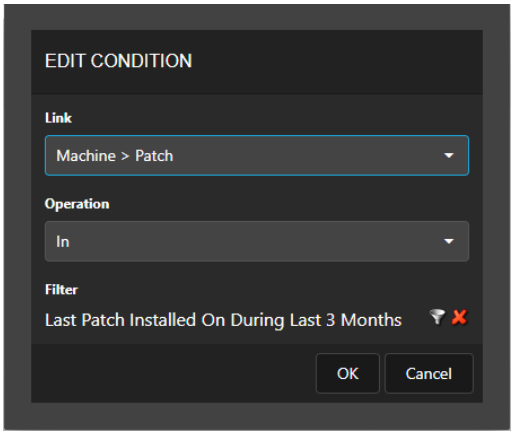
Where are they?

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.



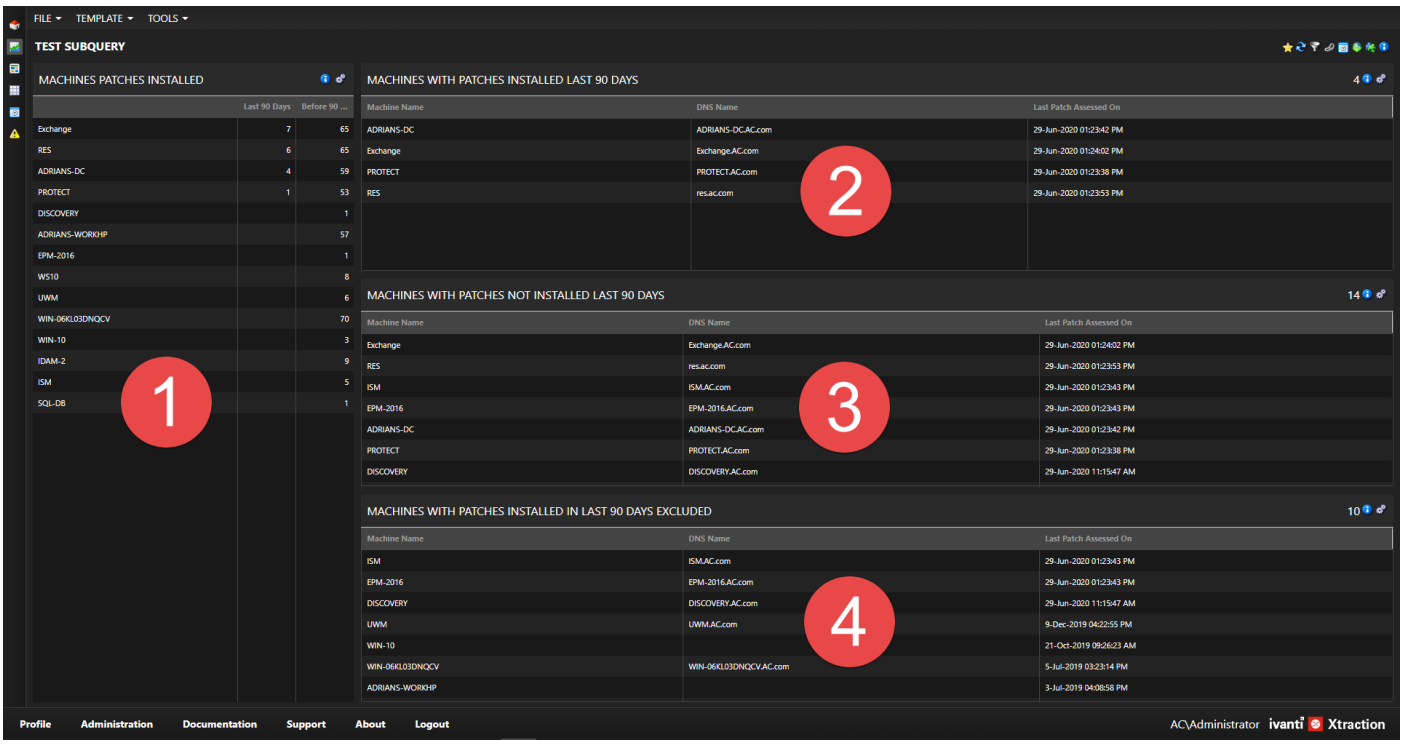
Select the appropriate link, in the **Operation**,

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 4rd 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.



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

View	Report Description	Sub Queries
Computers	All related machine data such Make, Model, OS, Architecture and Agents. In addition things like Installed Software, Group Membership – LDAP and local, Installed Patches, Services and Detected Vulnerabilities can all be reported on.	Computers > Products Computers > Programs Computers > Software Computers > LDAP Machine Groups Computers > Local Users Computers > Patches Computers > LDAP User Groups Computers > Local Groups Computers > Services Computers > Scope Computers > CVDetected
Packages	All information related to packages	None
Tasks	Reports for any task within EPM, Start and Finish of a Task, Name, Type and Current Status are among the reporting fields	None
Detected Patch and Compliance	This view enables reporting on all Detected Vulnerabilities, when, what, how severe and what are the relevant patches or actions required. Have they been successfully repaired and when?	None
Historical Patch and Compliance	History gathering within EPM must be turned on for this to work properly. Reports on remediation of vulnerabilities over a period of time.	None
Software	Software Asset Management from the aspect of the software.	None
Computer Software	Software Asset Management from the aspect of the computer.	None
Licensing	License Management from the aspect of licenses that are owned / used / unused.	None
Asset Control Devices	Hardware Asset Management	None
Remote Control Sessions	Reporting on all Remote Control sessions from EPM	None
Patch History	Reporting on historical patch repairs	None
Task History	Historical Task information	None
Machines Provisioned	Reporting on machine provisioning history	None
Provisioning Templates	Reporting on provisioning template history	None
Viruses Detected	Reporting on viruses, on what machines, primary owner and locations	None
Viruses Quarantined	Reporting on quarantined viruses, on what machines, primary owner and locations	None

Alerts	Full reporting on all alerts generated in EPM	None
Unmanaged Devices	Detailed reporting on any unmanaged	None
Vulnerability Statistics	Statistical reports relating to vulnerabilities, on what machines, scopes and custom groups	Vulnerability > Computer Vulnerability
Computer Vulnerability Details	Detailed reporting on Computers with Vulnerabilities	Computer > Computer Vulnerability Computer Vuln > Vulnerability

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