Compliance Packs (Windows)

The Compliance Packs category encompasses a range of dedicated solutions designed to facilitate and report on compliance with numerous security standards and regulations within the Windows environment. This encompasses monitoring and reporting on aspects such as Microsoft Defender Antivirus status, software compliance, and other vital security configurations crucial for safeguarding organizational assets. By leveraging these compliance packs, organizations can effortlessly conform to industry standards, regulatory mandates, and internal security protocols, thus ensuring a secure and compliant operational landscape.

- Microsoft Defender Compliance Pack (Win)
- BitLocker Management for Windows 10 and 11

Microsoft Defender Compliance Pack (Win)

> Work in progress. Check back tomorrow (Feb 15) and we hope you will attend the Roadshow.

Description

This will be a guide to take FileWave usage one major step further than simply installing an application like Microsoft Defender. In this article you will see how to use Custom Fields, Smart Groups, Filesets, and Grafana to report on the status of your fleet. You can apply these ideas to other software solutions where you need to know if they are working, and to potentially fix them.

Ingredients

- FileWave Central
- Microsoft Defender Recipe (Win)
- Defender Custom Fields.customfields
- Defender Update Defs (Win).fileset.zip
- Defender Run Scan (Win).fileset.zip

The Problem

You are managing hundreds or thousands of macOS or Windows devices, and need to understand if your environment is secure. Today you have been told to deploy Microsoft Defender and to provide reporting to your CISO demonstrating that you have Anti-Malware protection in place, and that it is operating correctly.

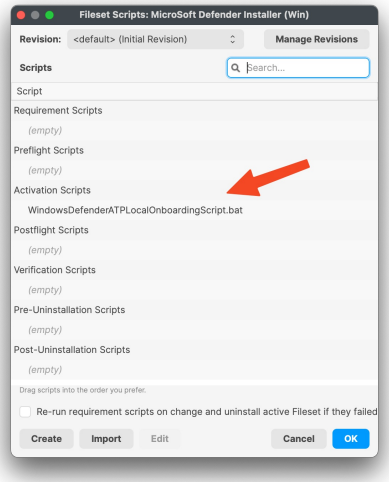
- What kind of installers are used?
- How can the install be performed silently? Fileset Magic needed?
- What is the deadline to have the product deployed?
- Will it replace another product?
- MacOS, Windows or both?

Get started with this like any other deployment project:

- Ask the vendor for installation documentation - but FileWave may also post some examples;
- Create a reverse timeline. Start small.
- Search the Internet for how others have reported on that product because FileWave can do anything scriptable.

Test and Verify:

- Test. Test. Verify and then test again.
- Deploy to 1 machine, then expand in growing waves so that you can stay ahead of issues.
- Do you have an Early Adopters group of users who give feedback and are forgiving?



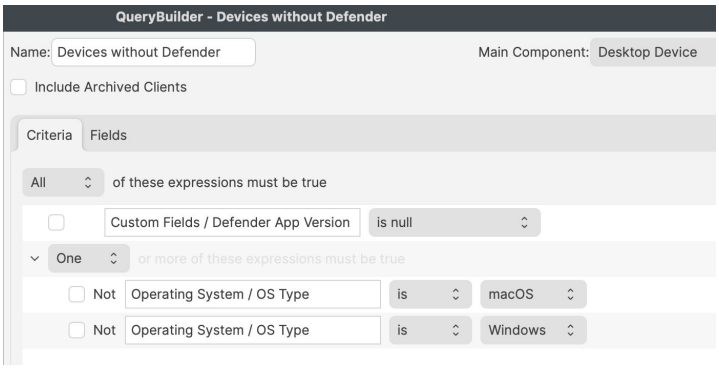
Deployment

Installers on Windows are usually an EXE or an MSI. In this case a BAT file is provided by Microsoft because Defender is part of Windows.

Did you know that you can execute scripts in Filesets, and each kind runs in a specific order and time?

How could the Uninstallation Scripts be helpful? Think about later when you may want to remove the deployed software.

For the Deployment phase see this article on installation: Microsoft Defender Recipe (Win)



Reporting

Queries/Reports are an easy way to keep track of progress and problems. We've made some Custom Fields for Defender, and we can leverage them to show who is missing Defender.

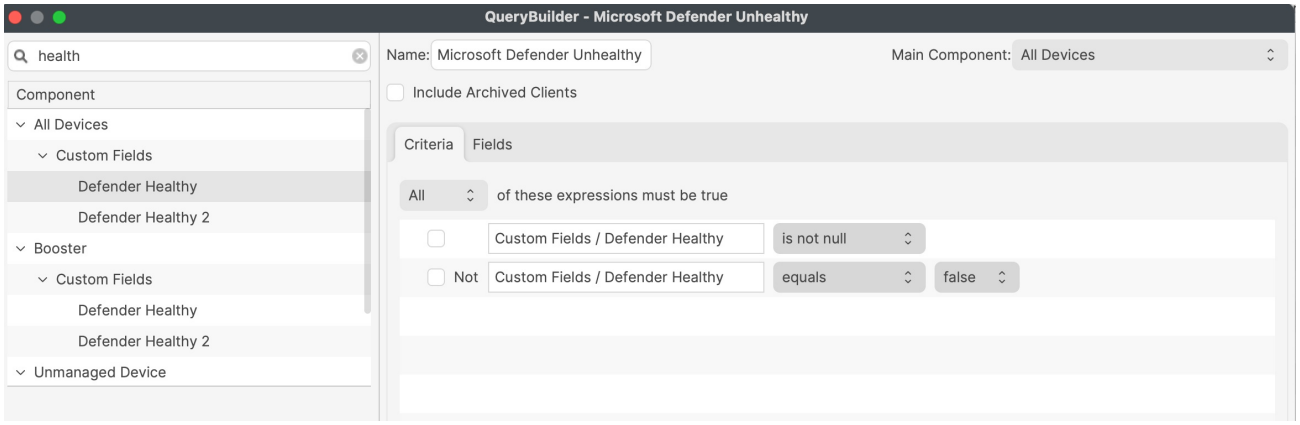
FileWave also has installed application reporting but depending on your needs and how that application reports itself you can consider either method.

To use the custom fields you will want to download Defender Custom Fields.customfields and then add them to your server. Do this in FileWave Central -> Assistants -> Custom Fields -> Edit Custom Field Definitions. Here you will click Import and then pick the file you downloaded. This file has fields that will work for both macOS and Windows. Once added you'll want to enable them for a couple of devices at first. To do that go to FileWave Central -> Clients and right click on a device and pick Edit Custom Field Associations. There you can check the boxes to enable these new fields. When you are happy with these Custom Fields, you'll want to go back to Edit Custom Field Definitions and pick "Assigned to all Devices" for each of the fields.

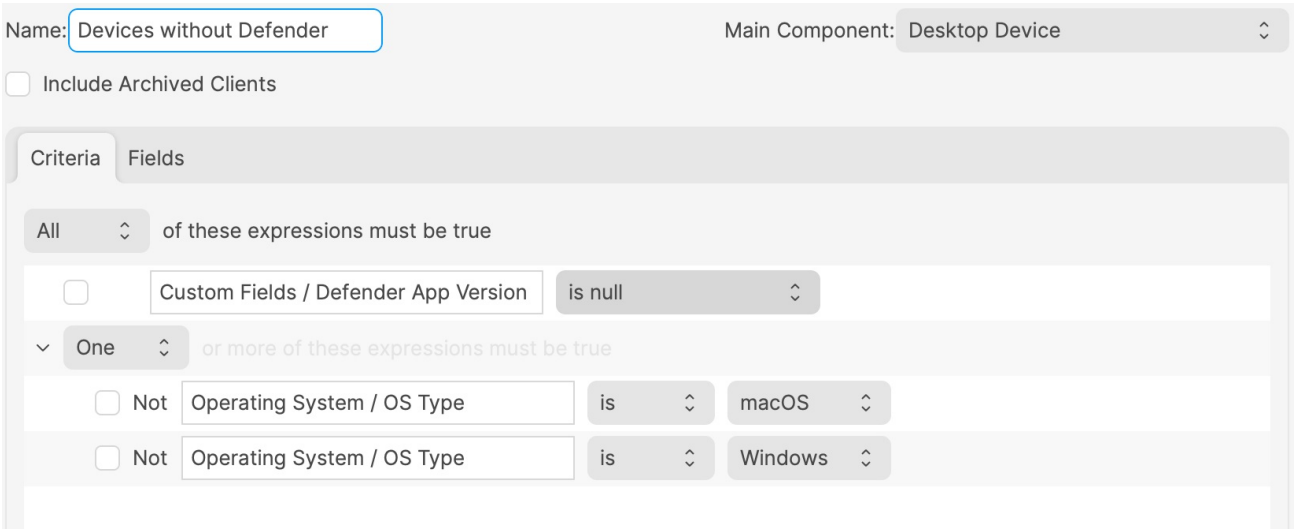
> Custom Fields based on scripts always need to be tested.

Now that you have your Custom Fields in place you should have some results. You can see them by going to Clients -> Customize Columns in the Toolbar, and then adding a couple of the custom fields to just see their values. You could also double click on any device in Clients that has the field active and see the values on the Device Details tab.

Let's move on to making a Query in Central. Click the New Query button in the Toolbar. Ignore the copies of the field below with a "2" as this is my lab. Notice that I used "Defender Healthy" as a Custom Field to test if Defender is healthy. I want to make sure that the field is populated so I check that it's not null, and I want to find unhealthy so I'm going to look for devices where it is false.



To find devices missing Defender notice that the App Version Custom Field can be used. If it is null (empty) then there is no Defender installed.



Remediation

Dashboards

There are two parts to creating a dashboard, getting the data to the dashboard (Prometheus), displaying the data in the way you want (Grafana).

yml_dashboard_files.zip

Create the dashboard:

Copy and Paste the JSON into a New dashboard:

▼ Dashboard JSON


```
{
  "annotations": {
    "list": [
      {
        "builtIn": 1,
        "datasource": {
          "type": "grafana",
          "uid": "-- Grafana --"
        },
        "enable": true,
        "hide": true,
        "iconColor": "rgba(0, 211, 255, 1)",
        "name": "Annotations & Alerts",
        "type": "dashboard"
      }
    ]
  },
  "editable": true,
  "fiscalYearStartMonth": 0,
  "graphTooltip": 0,
  "id": 19,
  "links": [],
  "liveNow": false,
  "panels": [
    {
      "collapsed": false,
      "gridPos": {
        "h": 1,
        "w": 24,
        "x": 0,
        "y": 0
      },
```

```
      "id": 7,
      "panels": [],
      "title": "Overall Status",
      "type": "row"
    },
    {
      "datasource": {
        "type": "prometheus",
        "uid": "filewave_prometheus"
      },
      "description": "",
      "fieldConfig": {
        "defaults": {
          "color": {
            "mode": "palette-classic"
          },
          "custom": {
            "hideFrom": {
              "legend": false,
              "tooltip": false,
              "viz": false
            }
          },
          "mappings": [],
          "unitScale": true
        },
        "overrides": [
          {
            "matcher": {
              "id": "byName",
              "options": "{__name__=\"filewave_inventory_query_55\",
genericclient_ptr__operating_system__type=\"OSX\", instance=\"localhost:20443\", job=\"extra-config-https\",
query_name=\"overall_os_breakdown\"}"
            },
            "properties": [
              {
                "id": "displayName",
                "value": "macOS"
              },
              {
                "id": "color",
                "value": {
                  "fixedColor": "blue",
                  "mode": "fixed"
                }
              }
            ]
          },
          {
            "matcher": {
              "id": "byName",
              "options": "{__name__=\"filewave_inventory_query_55\",
genericclient_ptr__operating_system__type=\"WIN\", instance=\"localhost:20443\", job=\"extra-config-https\",
query_name=\"overall_os_breakdown\"}"
            },
            "properties": [
              {
                "id": "displayName",
                "value": "Windows"
              },
              {
                "id": "color",
                "value": {
                  "fixedColor": "light-purple",
                  "mode": "fixed"
                }
              }
            ]
          }
        ]
```

```
    },
    "gridPos": {
      "h": 10,
      "w": 5,
      "x": 0,
      "y": 1
    },
    "id": 10,
    "links": [
      {
        "targetBlank": true,
        "title": "",
        "url": "https://support2.filewave.net/filewave/reports/55/overview/"
      }
    ],
    "options": {
      "legend": {
        "displayMode": "list",
        "placement": "bottom",
        "showLegend": true
      },
      "pieType": "pie",
      "reduceOptions": {
        "calcs": [
          "lastNotNull"
        ],
        "fields": "",
        "values": false
      },
      "tooltip": {
        "mode": "single",
        "sort": "none"
      }
    },
    "targets": [
      {
        "datasource": {
          "type": "prometheus",
          "uid": "filewave_prometheus"
        },
        "editorMode": "builder",
        "exemplar": false,
        "expr": "filewave_inventory_query_55",
        "instant": true,
        "legendFormat": "{{defender_healthy_fwcomp_pack}}",
        "range": false,
        "refId": "A"
      }
    ],
    "title": "Overall Desktop Device Breakdown",
    "type": "piechart"
  },
  {
    "datasource": {
      "type": "prometheus",
      "uid": "filewave_prometheus"
    },
    "description": "",
    "fieldConfig": {
      "defaults": {
        "color": {
          "mode": "palette-classic"
        },
        "custom": {
          "hideFrom": {
            "legend": false,
            "tooltip": false,
            "viz": false
          }
        },
```

```
          "mappings": [],
          "unitScale": true
        },
        "overrides": [
          {
            "matcher": {
              "id": "byName",
              "options": "{__name__=\"filewave_inventory_query_56\",
genericclient_ptr__operating_system__type=\"OSX\", instance=\"localhost:20443\", job=\"extra-config-https\",
query_name=\"devices_without_defender\"}"
            },
            "properties": [
              {
                "id": "displayName",
                "value": "macOS"
              }
            ]
          },
          {
            "matcher": {
              "id": "byName",
              "options": "{__name__=\"filewave_inventory_query_56\",
genericclient_ptr__operating_system__type=\"WIN\", instance=\"localhost:20443\", job=\"extra-config-https\",
query_name=\"devices_without_defender\"}"
            },
            "properties": [
              {
                "id": "displayName",
                "value": "Windows"
              }
            ]
          }
        ]
      },
      "gridPos": {
        "h": 10,
        "w": 5,
        "x": 5,
        "y": 1
      },
      "id": 11,
      "links": [
        {
          "targetBlank": true,
          "title": "",
          "url": "https://support2.filewave.net/filewave/reports/56/overview/"
        }
      ],
      "options": {
        "legend": {
          "displayMode": "list",
          "placement": "bottom",
          "showLegend": true
        },
        "pieType": "pie",
        "reduceOptions": {
          "calcs": [
            "lastNotNull"
          ],
          "fields": "",
          "values": false
        },
        "tooltip": {
          "mode": "single",
          "sort": "none"
        }
      },
      "targets": [
        {
          "datasource": {
```

```
        "type": "prometheus",
        "uid": "filewave_prometheus"
      },
      "editorMode": "builder",
      "exemplar": false,
      "expr": "filewave_inventory_query_56",
      "instant": true,
      "legendFormat": "{{defender_healthy_fwcomp_pack}}",
      "range": false,
      "refId": "A"
    }
  ],
  "title": "Devices without Defender",
  "type": "piechart"
},
{
  "datasource": {
    "type": "prometheus",
    "uid": "filewave_prometheus"
  },
  "description": "Relative health of Microsoft Defender",
  "fieldConfig": {
    "defaults": {
      "color": {
        "mode": "palette-classic"
      },
      "custom": {
        "hideFrom": {
          "legend": false,
          "tooltip": false,
          "viz": false
        }
      },
      "mappings": [],
      "unitScale": true
    },
    "overrides": [
      {
        "matcher": {
          "id": "byName",
          "options": "True"
        },
        "properties": [
          {
            "id": "color",
            "value": {
              "fixedColor": "green",
              "mode": "fixed"
            }
          }
        ]
      },
      {
        "matcher": {
          "id": "byName",
          "options": "False"
        },
        "properties": [
          {
            "id": "color",
            "value": {
              "fixedColor": "semi-dark-red",
              "mode": "fixed"
            }
          }
        ]
      }
    ]
  },
  "gridPos": {
```

```
      "h": 10,
      "w": 5,
      "x": 10,
      "y": 1
    },
    "id": 1,
    "links": [
      {
        "targetBlank": true,
        "title": "",
        "url": "https://support2.filewave.net/filewave/reports/49/overview/"
      }
    ],
    "options": {
      "legend": {
        "displayMode": "list",
        "placement": "bottom",
        "showLegend": true
      },
      "pieType": "pie",
      "reduceOptions": {
        "calcs": [
          "lastNotNull"
        ],
        "fields": "",
        "values": false
      },
      "tooltip": {
        "mode": "single",
        "sort": "none"
      }
    },
    "targets": [
      {
        "datasource": {
          "type": "prometheus",
          "uid": "filewave_prometheus"
        },
        "editorMode": "builder",
        "exemplar": false,
        "expr": "filewave_inventory_query_49{defender_healthy_fwcomp_pack=\"True\"}",
        "instant": true,
        "legendFormat": "{{defender_healthy_fwcomp_pack}}",
        "range": false,
        "refId": "A"
      },
      {
        "datasource": {
          "type": "prometheus",
          "uid": "filewave_prometheus"
        },
        "editorMode": "builder",
        "expr": "filewave_inventory_query_49{defender_healthy_fwcomp_pack=\"False\"}",
        "hide": false,
        "legendFormat": "{{defender_healthy_fwcomp_pack}}",
        "range": true,
        "refId": "B"
      }
    ],
    "title": "Defender Healthy?",
    "type": "piechart"
  },
  {
    "datasource": {
      "type": "prometheus",
      "uid": "filewave_prometheus"
    },
    "fieldConfig": {
      "defaults": {
        "color": {
```

```
            "mode": "thresholds"
          },
          "custom": {
            "align": "auto",
            "cellOptions": {
              "type": "auto"
            },
            "filterable": false,
            "inspect": false
          },
          "mappings": [],
          "thresholds": {
            "mode": "absolute",
            "steps": [
              {
                "color": "green",
                "value": null
              },
              {
                "color": "red",
                "value": 80
              }
            ]
          },
          "unitScale": true
        },
        "overrides": [
          {
            "matcher": {
              "id": "byName",
              "options": "__name__"
            },
            "properties": [
              {
                "id": "custom.width",
                "value": 290
              },
              {
                "id": "custom.hidden",
                "value": true
              }
            ]
          },
          {
            "matcher": {
              "id": "byName",
              "options": "Time"
            },
            "properties": [
              {
                "id": "custom.hidden",
                "value": true
              }
            ]
          },
          {
            "matcher": {
              "id": "byName",
              "options": "instance"
            },
            "properties": [
              {
                "id": "custom.hidden",
                "value": true
              }
            ]
          },
          {
            "matcher": {
              "id": "byName",
```

```
          "options": "query_name"
        },
        "properties": [
          {
            "id": "custom.hidden",
            "value": true
          }
        ]
      },
      {
        "matcher": {
          "id": "byName",
          "options": "Value"
        },
        "properties": [
          {
            "id": "custom.hidden",
            "value": true
          }
        ]
      },
      {
        "matcher": {
          "id": "byName",
          "options": "job"
        },
        "properties": [
          {
            "id": "custom.hidden",
            "value": true
          }
        ]
      }
    ]
  },
  "gridPos": {
    "h": 10,
    "w": 4,
    "x": 15,
    "y": 1
  },
  "id": 2,
  "links": [
    {
      "targetBlank": true,
      "title": "",
      "url": "https://support2.filewave.net/filewave/reports/50/overview/"
    }
  ],
  "options": {
    "cellHeight": "sm",
    "footer": {
      "countRows": false,
      "fields": "",
      "reducer": [
        "sum"
      ],
      "show": false
    },
    "showHeader": true,
    "sortBy": [
      {
        "desc": false,
        "displayName": "device_name"
      }
    ]
  },
  "pluginVersion": "10.3.1",
  "targets": [
    {
```

```
      "datasource": {
        "type": "prometheus",
        "uid": "filewave_prometheus"
      },
      "editorMode": "builder",
      "exemplar": false,
      "expr": "filewave_inventory_query_50",
      "format": "table",
      "instant": true,
      "legendFormat": "{{device_name}}",
      "range": false,
      "refId": "A"
    }
  ],
  "title": "Unhealthy Defender Clients",
  "transformations": [],
  "type": "table"
},
{
  "collapsed": false,
  "gridPos": {
    "h": 1,
    "w": 24,
    "x": 0,
    "y": 11
  },
  "id": 12,
  "panels": [],
  "title": "Threat Detection and Issues",
  "type": "row"
},
{
  "datasource": {
    "type": "prometheus",
    "uid": "filewave_prometheus"
  },
  "description": "",
  "fieldConfig": {
    "defaults": {
      "color": {
        "mode": "thresholds"
      },
      "custom": {
        "align": "auto",
        "cellOptions": {
          "type": "auto"
        },
        "inspect": false
      },
      "mappings": [],
      "thresholds": {
        "mode": "absolute",
        "steps": [
          {
            "color": "green",
            "value": null
          },
          {
            "color": "red",
            "value": 80
          }
        ]
      },
      "unitScale": true
    },
    "overrides": [
      {
        "matcher": {
          "id": "byName",
          "options": "Time"
```

```
      },
      "properties": [
        {
          "id": "custom.hidden",
          "value": true
        }
      ]
    },
    {
      "matcher": {
        "id": "byName",
        "options": "Value"
      },
      "properties": [
        {
          "id": "custom.hidden",
          "value": true
        }
      ]
    },
    {
      "matcher": {
        "id": "byName",
        "options": "query_name"
      },
      "properties": [
        {
          "id": "custom.hidden",
          "value": true
        }
      ]
    },
    {
      "matcher": {
        "id": "byName",
        "options": "job"
      },
      "properties": [
        {
          "id": "custom.hidden",
          "value": true
        }
      ]
    },
    {
      "matcher": {
        "id": "byName",
        "options": "device_name"
      },
      "properties": [
        {
          "id": "custom.hidden",
          "value": true
        }
      ]
    },
    {
      "matcher": {
        "id": "byName",
        "options": "__name__"
      },
      "properties": [
        {
          "id": "custom.hidden",
          "value": true
        }
      ]
    },
    {
      "matcher": {
```

```
            "id": "byName",
            "options": "instance"
          },
          "properties": [
            {
              "id": "custom.hidden",
              "value": true
            }
          ]
        },
        {
          "matcher": {
            "id": "byName",
            "options": "defender_threats_detected_fwcomp_pack"
          },
          "properties": [
            {
              "id": "displayName",
              "value": "Threat Detected"
            }
          ]
        }
      ]
    },
    "gridPos": {
      "h": 9,
      "w": 19,
      "x": 0,
      "y": 12
    },
    "id": 13,
    "links": [
      {
        "targetBlank": true,
        "title": "Show Details",
        "url": "https://support2.filewave.net/filewave/reports/57/overview/"
      }
    ],
    "options": {
      "cellHeight": "sm",
      "footer": {
        "countRows": false,
        "fields": "",
        "reducer": [
          "sum"
        ],
        "show": false
      },
      "showHeader": true
    },
    "pluginVersion": "10.3.1",
    "targets": [
      {
        "datasource": {
          "type": "prometheus",
          "uid": "filewave_prometheus"
        },
        "editorMode": "builder",
        "exemplar": false,
        "expr": "filewave_inventory_query_57",
        "format": "table",
        "instant": true,
        "legendFormat": "{{label_name}}",
        "range": false,
        "refId": "A"
      }
    ],
    "title": "Detected Threats",
    "type": "table"
  },
```

```
    {
      "collapsed": false,
      "gridPos": {
        "h": 1,
        "w": 24,
        "x": 0,
        "y": 21
      },
      "id": 6,
      "panels": [],
      "title": "Windows",
      "type": "row"
    },
    {
      "datasource": {
        "type": "prometheus",
        "uid": "filewave_prometheus"
      },
      "description": "",
      "fieldConfig": {
        "defaults": {
          "color": {
            "mode": "palette-classic"
          },
          "custom": {
            "axisBorderShow": false,
            "axisCenteredZero": false,
            "axisColorMode": "text",
            "axisLabel": "",
            "axisPlacement": "auto",
            "fillOpacity": 80,
            "gradientMode": "none",
            "hideFrom": {
              "legend": false,
              "tooltip": false,
              "viz": false
            },
            "lineWidth": 1,
            "scaleDistribution": {
              "type": "linear"
            },
            "thresholdsStyle": {
              "mode": "off"
            }
          },
          "mappings": [],
          "thresholds": {
            "mode": "absolute",
            "steps": [
              {
                "color": "green",
                "value": null
              },
              {
                "color": "red",
                "value": 80
              }
            ]
          },
          "unitScale": true
        },
        "overrides": []
      },
      "gridPos": {
        "h": 10,
        "w": 8,
        "x": 0,
        "y": 22
      },
      "id": 4,
```

```
      "links": [
        {
          "targetBlank": true,
          "title": "",
          "url": "https://support2.filewave.net/filewave/reports/52/overview/"
        }
      ],
      "options": {
        "barRadius": 0,
        "barWidth": 0.97,
        "fullHighlight": false,
        "groupWidth": 0.7,
        "legend": {
          "calcs": [],
          "displayMode": "list",
          "placement": "bottom",
          "showLegend": false
        },
        "orientation": "auto",
        "showValue": "auto",
        "stacking": "none",
        "tooltip": {
          "mode": "single",
          "sort": "none"
        },
        "xTickLabelRotation": 0,
        "xTickLabelSpacing": 0
      },
      "targets": [
        {
          "datasource": {
            "type": "prometheus",
            "uid": "filewave_prometheus"
          },
          "editorMode": "builder",
          "exemplar": false,
          "expr": "filewave_inventory_query_52",
          "instant": true,
          "legendFormat": "{{defender_defs_version_fwcomp_pack}}",
          "range": false,
          "refId": "A"
        }
      ],
      "title": "Virus Defs Versions Windows",
      "type": "barchart"
    },
    {
      "datasource": {
        "type": "prometheus",
        "uid": "filewave_prometheus"
      },
      "description": "",
      "fieldConfig": {
        "defaults": {
          "color": {
            "mode": "palette-classic"
          },
          "custom": {
            "axisBorderShow": false,
            "axisCenteredZero": false,
            "axisColorMode": "text",
            "axisLabel": "",
            "axisPlacement": "auto",
            "fillOpacity": 80,
            "gradientMode": "none",
            "hideFrom": {
              "legend": false,
              "tooltip": false,
              "viz": false
            },
```

```
        "lineWidth": 1,
        "scaleDistribution": {
          "type": "linear"
        },
        "thresholdsStyle": {
          "mode": "off"
        }
      },
      "mappings": [],
      "thresholds": {
        "mode": "absolute",
        "steps": [
          {
            "color": "green",
            "value": null
          },
          {
            "color": "red",
            "value": 80
          }
        ]
      },
      "unitScale": true
    },
    "overrides": []
  },
  "gridPos": {
    "h": 10,
    "w": 9,
    "x": 8,
    "y": 22
  },
  "id": 9,
  "links": [
    {
      "targetBlank": true,
      "title": "",
      "url": "https://support2.filewave.net/filewave/reports/54/overview/"
    }
  ],
  "options": {
    "barRadius": 0,
    "barWidth": 0.97,
    "fullHighlight": false,
    "groupWidth": 0.7,
    "legend": {
      "calcs": [],
      "displayMode": "list",
      "placement": "bottom",
      "showLegend": false
    },
    "orientation": "auto",
    "showValue": "auto",
    "stacking": "none",
    "tooltip": {
      "mode": "single",
      "sort": "none"
    },
    "xTickLabelRotation": 0,
    "xTickLabelSpacing": 0
  },
  "targets": [
    {
      "datasource": {
        "type": "prometheus",
        "uid": "filewave_prometheus"
      },
      "editorMode": "builder",
      "exemplar": false,
      "expr": "filewave_inventory_query_54",
```

```
      "instant": true,
      "legendFormat": "{{defender_app_version_fwcomp_pack}}",
      "range": false,
      "refId": "A"
    }
  ],
  "title": "Defender Version Windows",
  "type": "barchart"
},
{
  "collapsed": false,
  "gridPos": {
    "h": 1,
    "w": 24,
    "x": 0,
    "y": 32
  },
  "id": 5,
  "panels": [],
  "title": "macOS",
  "type": "row"
},
{
  "datasource": {
    "type": "prometheus",
    "uid": "filewave_prometheus"
  },
  "description": "",
  "fieldConfig": {
    "defaults": {
      "color": {
        "mode": "palette-classic"
      },
      "custom": {
        "axisBorderShow": false,
        "axisCenteredZero": false,
        "axisColorMode": "text",
        "axisLabel": "",
        "axisPlacement": "auto",
        "fillOpacity": 80,
        "gradientMode": "none",
        "hideFrom": {
          "legend": false,
          "tooltip": false,
          "viz": false
        },
        "lineWidth": 1,
        "scaleDistribution": {
          "type": "linear"
        },
        "thresholdsStyle": {
          "mode": "off"
        }
      },
      "mappings": [],
      "thresholds": {
        "mode": "absolute",
        "steps": [
          {
            "color": "green",
            "value": null
          },
          {
            "color": "red",
            "value": 80
          }
        ]
      },
      "unitScale": true
    },
```

```
      "overrides": []
    },
    "gridPos": {
      "h": 10,
      "w": 8,
      "x": 0,
      "y": 33
    },
    "id": 3,
    "links": [
      {
        "targetBlank": true,
        "title": "",
        "url": "https://support2.filewave.net/filewave/reports/51/overview/"
      }
    ],
    "options": {
      "barRadius": 0,
      "barWidth": 0.97,
      "fullHighlight": false,
      "groupWidth": 0.7,
      "legend": {
        "calcs": [],
        "displayMode": "list",
        "placement": "bottom",
        "showLegend": false
      },
      "orientation": "auto",
      "showValue": "auto",
      "stacking": "none",
      "tooltip": {
        "mode": "single",
        "sort": "none"
      },
      "xTickLabelRotation": 0,
      "xTickLabelSpacing": 0
    },
    "targets": [
      {
        "datasource": {
          "type": "prometheus",
          "uid": "filewave_prometheus"
        },
        "editorMode": "builder",
        "exemplar": false,
        "expr": "filewave_inventory_query_51",
        "instant": true,
        "legendFormat": "{{defender_defs_version_fwcomp_pack}}",
        "range": false,
        "refId": "A"
      }
    ],
    "title": "Virus Defs Versions macOS",
    "type": "barchart"
  },
  {
    "datasource": {
      "type": "prometheus",
      "uid": "filewave_prometheus"
    },
    "description": "",
    "fieldConfig": {
      "defaults": {
        "color": {
          "mode": "palette-classic"
        },
        "custom": {
          "axisBorderShow": false,
          "axisCenteredZero": false,
          "axisColorMode": "text",
```

```
        "axisLabel": "",
        "axisPlacement": "auto",
        "fillOpacity": 80,
        "gradientMode": "none",
        "hideFrom": {
          "legend": false,
          "tooltip": false,
          "viz": false
        },
        "lineWidth": 1,
        "scaleDistribution": {
          "type": "linear"
        },
        "thresholdsStyle": {
          "mode": "off"
        }
      },
      "mappings": [],
      "thresholds": {
        "mode": "absolute",
        "steps": [
          {
            "color": "green",
            "value": null
          },
          {
            "color": "red",
            "value": 80
          }
        ]
      },
      "unitScale": true
    },
    "overrides": []
  },
  "gridPos": {
    "h": 10,
    "w": 9,
    "x": 8,
    "y": 33
  },
  "id": 8,
  "links": [
    {
      "targetBlank": true,
      "title": "",
      "url": "https://support2.filewave.net/filewave/reports/53/overview/"
    }
  ],
  "options": {
    "barRadius": 0,
    "barWidth": 0.97,
    "fullHighlight": false,
    "groupWidth": 0.7,
    "legend": {
      "calcs": [],
      "displayMode": "list",
      "placement": "bottom",
      "showLegend": false
    },
    "orientation": "auto",
    "showValue": "auto",
    "stacking": "none",
    "tooltip": {
      "mode": "single",
      "sort": "none"
    },
    "xTickLabelRotation": 0,
    "xTickLabelSpacing": 0
  },
```

```
      "targets": [
        {
          "datasource": {
            "type": "prometheus",
            "uid": "filewave_prometheus"
          },
          "editorMode": "builder",
          "exemplar": false,
          "expr": "filewave_inventory_query_53",
          "instant": true,
          "legendFormat": "{{defender_app_version_fwcomp_pack}}",
          "range": false,
          "refId": "A"
        }
      ],
      "title": "Defender Version macOS",
      "type": "barchart"
    }
  ],
  "refresh": "",
  "schemaVersion": 39,
  "tags": [],
  "templating": {
    "list": []
  },
  "time": {
    "from": "now-6h",
    "to": "now"
  },
  "timepicker": {},
  "timezone": "",
  "title": "Defender Dashboard",
  "uid": "c26006b5-0295-4ec0-9b54-3efd3d714a9f",
  "version": 1,
  "weekStart": ""
}
```


Related Content

Related Content

- Microsoft Defender Recipe (Win)
- Microsoft Defender Recipe (macOS)
- Microsoft Defender Compliance Pack (macOS)

BitLocker Management for Windows 10 and 11

Description

This article provides a comprehensive overview of the Compliance Pack dedicated to managing and reporting on the BitLocker encryption status for Windows 10 and 11 devices using FileWave. BitLocker is an essential security feature that encrypts the entire disk to protect data from unauthorized access. Organizations need to ensure BitLocker is activated and properly configured to meet security standards and regulatory mandates. This Compliance Pack facilitates monitoring, reporting, and management of BitLocker on Windows 10 and 11 devices, aiding organizations in maintaining a secure operational landscape.

Ingredients

- FileWave Central
- Windows OS systems running a version of Windows that is licensed for BitLocker
- BitLocker Fileset
  - Activation: Associate the Fileset with Windows clients to enable BitLocker.
  - Deactivation: Remove the association to disable BitLocker.
  - Customization: The script within the Fileset includes specific options that can be customized by administrators based on organizational needs.
- Custom Fields
  - BitLocker Key: Displays the recovery keys for encrypted drives. For example, "C:, 219296-176121-018458-479017-019437-305833-463155-542608". After importing the Custom Field, choose to assign it to specific devices or all devices.
  - BitLocker Status: Presents the current encryption state, such as "Conversion Status: Used Space Only Encrypted".

BitLocker Compliance Pack

Directions

Download

1. Download the BitLocker Compliance Pack.
   - Unzip the zip file and you will find a Fileset as well as a Custom Fields file.

BitLocker Custom Fields

The Custom Fields will report information to you and will not encrypt the devices or take any action other than reporting in their current form. The below steps will get you started.

1. In FileWave Central go to Assistants -> Custom Fields -> Edit Custom Field Definitions.
2. Click "Import" and pick the .customfields file from the zip you downloaded.
3. For both BitLocker Key and also BitLocker Status you'll want to select each and check "Assigned to all devices" if you would like to capture the status for all. Otherwise you could pick specific devices in the Clients view and right click there and pick to Edit Custom Field Associations to set specific devices to report.
4. You can now add these 2 new fields to the Clients view or any Query (Report) and see the status. You'll want to do a Model Update and then wait for a device to report in to see the reporting data.

Bitlocker Enforcement Fileset

This Fileset will take action on devices if it is assigned to them. You should test and be sure you understand what it is doing before applying it. If you Associate it with a device you will see that device will encrypt, and the Custom Fields you added will report on that. There is always a delay between action and reporting because an inventory must occur to see it in FileWave so don't worry if it is not immediate, and you can use a Verify to ask the device to inventory sooner when testing.

1. Drag and drop the Bitlocker Enforcement.fileset in to your Filesets area in FileWave Central.
2. Move it to wherever you would like it in the Filesets area.
3. Create an Association or a Deployment to assign it to a device.
4. Watch that device encrypt by looking at properties for the drive on that computer in Explorer or with manage-bde.exe on that computer. The Custom Fields will not update in real time so that is the best way to watch when testing.
5. Notice what happens if you break the Association. The device will decrypt.

You may wonder how this all works. If you pick Scripts from the toolbar when highlighting the Fileset you will see there is a script to encrypt and one to decrypt. If you run in to issues encrypting you will see log information in C:\ProgramData\FileWave\log\fwcld\ in the directory for the Fileset. Every Fileset has an ID number and a directory will be there for that Fileset. Consider if you are running

Windows Home Edition or some other version that doesn't include BitLocker. We can only enable BitLocker when the OS is capable. There are other settings and requirements and you'll see in the encryption script that you could edit it if you would like to set options slightly differently.

Next Steps

We will look to include instructions on setup of a Dashboard in Grafana and to simplify the setup instructions even more.

Related Content

- Compliance Packs (Windows)
- Compliance Packs (macOS)