



This PDF is generated from authoritative online content, and is provided for convenience only. This PDF cannot be used for legal purposes. For authoritative understanding of what is and is not supported, always use the online content. To copy code samples, always use the online content.

# Workbench User's Guide

AD FAQ's

---

## Contents

- **1 AD FAQ's**
  - **1.1 Anomaly Detection Host/Server Operating System Support**
  - **1.2 Anomaly Detection Deployment**
  - **1.3 Workbench Data-Centers**
  - **1.4 AD Infrastructure/Footprint**
  - **1.5 AD Alarms**
  - **1.6 Dashboards and Visualizations**
  - **1.7 AD Data Retention**
  - **1.8 AD Ports**
  - **1.9 GDPR**
  - **1.10 Licenses**

## AD FAQ's

This section provides a useful list of Workbench Anomaly Detection AD Frequently Asked Question's (FAQ's):

### Anomaly Detection Host/Server Operating System Support

- Which Operating Systems are supported by AD?
  - Answer: Windows 2012 and 2016 - RHEL 7 - CentOS 7

### Anomaly Detection Deployment

- Does AD need its own dedicated host infrastructure?
  - Answer: Yes; please review the documentation [Planning](#) section
- Can I install the AD components on the Workbench core component hosts?
  - Answer: No - use separate Hosts for the AD components
- Is the Workbench Agent application required on the AD hosts?
  - Answer: Yes, and is included in the AD Installer.
- What is the maximum number of hosts supported by Anomaly Detection
  - Answer: Please review the [AD Sizing](#) section.
- Does AD support an upgrade capability
  - Answer: No
- Does Workbench AD use the Elastic Machine Learning component's/feature?
  - Answer: No - Workbench AD is a proprietary Genesys Machine Learning model

### Workbench Data-Centers

- Does each Workbench Data-Center need its own AD Node(s)/Host(s)
  - Answer: Yes

## AD Infrastructure/Footprint

- How many dedicated AD Nodes/Hosts are required?
  - Answer: Please review the documentation [Planning](#) section - at a high level:
    - If AD redundancy is required then more than 1 AD Node/Host will need to be deployed at each Workbench Data-Center/Site
    - Also, depending on the number of Hosts sending Metrics to Workbench and the ingestion frequency of those Metrics, additional AD Nodes/Hosts may be required at each Data-Center

## AD Alarms

- What types of alarms are generated by AD?
  - Answer: AD can generate four types of alarms:
    - AD is not able to connect with Workbench Logstash.
    - AD is connected to Workbench Logstash but is not receiving metric data.
    - AD is not receiving data from a particular workbench host.
    - AD is not receiving data from one metric source

## Dashboards and Visualizations

- Does AD ship with example Visualizations/Widgets for Workbench?
  - Answer: Yes.

## AD Data Retention

- How/when is data purged/deleted from AD?
  - Answer: The default AD "Retention Period" is 30 days - this AD Retention Period is not configurable.

## AD Ports

- Which Ports are used by Workbench Anomaly Detection (AD)?
  - Answer:
    - **50000 - 51000**: Nodes and Internal Process Communication
    - **8182**: AD API

- **9091 & 5067**: Workbench Agent and Metricbeat Ports on each AD Host
- **9090**: AD Pipeline Port on the Logstash Application
- Do not use Ports below 1024 for AD as these ports are typically used for system services

## GDPR

- How does AD accommodate the GDPR policy?
  - Answer: Please review the Additional Information/GDPR section of the documentation.

## Licenses

- Does Anomaly Detection need a license?
  - Answer: No - currently it's included with Workbench and needs its own dedicated Node(s)/Host(s).