FORTIFIED WISdom™

WISdom Installation Requirements

Updated: March 25, 2025

WISdom Overview

WISdom offers an agentless data collection service that gathers system, metadata, and runtime data from each system. Utilizing Microsoft Azure, WISdom ensures secure transfer and storage of this data, both in transit and at rest. The data is processed by the WISdom service, which operates locally on virtual machines (VMs) to securely monitor and collect data from managed servers.

The local WISdom application communicates with the Fortified cloud to receive updates and serves as the ingestion point for your environment's database statistics. PowerShell is used to collect and store monitoring information, which is then sent to a dedicated Azure API for processing and storage in the backend Azure Database.

Each client's data collector service has a unique key pair for secure data transfer and processing. All data is encrypted with this dedicated key pair, provided by Fortified, and is automatically updated weekly.

Security Protocols and Features

WISdom Services are designed to ensure optimal performance with minimal impact, while upholding stringent security standards. Below are the essential security protocols and features integrated into WISdom application:

- **Data Collection:** WISdom gathers metadata, runtime, and configuration data using WMI and SQL calls. No sensitive data is transferred to the Fortified environment.
- **Frequency of Collection** – To optimize resource usage, WISdom intelligently collects data based on necessity, ranging from once a minute to once a day, depending on the data type.
- **Upload Process** – All uploaded information is encrypted using TLS and sent to the Azure API for processing. Once processed, the data is sent to each client's individual database, allowing for additional formatting and storage. This ensures the data is ready for display in the WISdom UI.
- **Access to Encrypted Data** – Configuration updates are securely transmitted through an Azure API connection, encrypted using a certificate pair. This pair is stored exclusively on our central server and the client's machine running the WISdom service. Access to the data and encryption keys is strictly limited to the client and Fortified.

WISdom Prerequisites

WISdom Services Host

In preparation for the installation of the WISdom data collection services, it is essential to ensure that the machine hosting the WISdom services is properly configured. This includes installing the correct operating system (OS) and .NET applications. Additionally, the machine must have the capability to establish connections with both the Fortified WISdom API and any target SQL instances assigned to the collector for monitoring.

Windows System Requirements

The WISdom data collection services require the correct operating system (OS) and .NET applications.

Key Requirements

- **OS Requirements:**
  - The OS and patch level of the collector machine must be equivalent to or higher than those of all monitored target machines.
    - Microsoft does not support WMI and performance metric connections from a lower-level OS or patch.
- **Windows Management Framework (WMF) 5.1**
  - Typically included in most Windows OS and Server installations.
- **.NET Desktop Runtime 8.0 or higher**
  - .NET Downloads (Linux, macOS, and Windows)
    - The *.NET Desktop Runtime* will be found in the *All .NET Downloads* page in the right-hand column, second block down.

Firewall Rules

- **Access to Managed Servers on Specific Ports:**
  - SQL Server Port (usually 1433, but may vary)
  - SQL Browser for named instances – Port 1434
  - WMI - Port 135 and 49154
    - If 49154 is already in use, a range of 49152-65535 (RDP range) is required
  - Performance counters – Port 445
- **Outbound firewall rules:**
  - Allow access to https://collectorapi.fortifiedwisdom.com
    - IP Range: 20.85.14.224/29

Antivirus Exclusions

To ensure optimal performance of the WISdom service, exclude the following folders from antivirus scans. Scanning these folders can degrade the performance of the collection service:

- **%Installation Folder%\CollectorResults**
- **%Installation Folder%\UploadReady**
- **%Installation Folder%\ESUploadReady** (If it exists)

**** Note**: The default installation location: C:\Program Files\Fortified\Wisdom*

Service Account Requirements

- **Windows Account**
  - The service account must be a Windows account, preferably a domain account
    - It is recommended to use the service account for all collections, see the collection requirements below
- **Log on as Service Permissions**
  - The account must have the "*Log on as a Service*" permission to run as a Windows service
- **Local Administrator Privileges**
  - The account must be a local administrator on the server hosting the WISdom service
    - These permissions ensure that the WISdom Collection service can function correctly and efficiently.

Collection Server Sizing

Depending on the number of servers or devices managed by WISdom and their locations, you may need to provision a VM to support data collection and upload for each data center or geographic location.

Follow these guidelines for VM sizing:

1-50 Managed servers	50-200 Managed servers	201+ Managed servers
4 Processors	8 Processors*	12 Processors*
8 - 16 GB RAM	16 GB RAM	32 GB RAM
50 GB Storage	75 GB Storage	100 GB Storage

**It is possible to create 2 smaller VMs instead of one larger VM and separate the managed servers between them.*

Collection Requirements

Collection Account Options

- **Monitoring Service Account**
  - The recommended method of collecting Windows and SQL Server Metrics.
- **Secondary Windows Account(s)**
  - Secondary accounts may be used to collect data from other domains and DMZs.
- **SQL Account**
  - Using a SQL Authenticated account will result in the Windows Monitoring metrics (WMI) not being collected.

Windows Monitoring

- **Data Collection Account:** A Windows account is required to collect Windows metrics (WMI), preferably an Active Directory (AD) account.
- **Permissions Required on Targets:**
  - **Local Administrator:** Preferably the account is be a member of the Local Administrators group.
    - **Alternative Permissions:** Instead of Local Administrator, explicitly grant permissions on WMI and DCOM.
  - **Log on as Batch Job:** Necessary for executing scheduled tasks.

- **Group Membership:**
  - Remote Management Users
  - Distributed COM Users

**** Note**: If not using Local Administrator, group policy updates or Windows patching may remove explicitly granted WMI/DCOM permissions, disrupting monitoring until permissions are restored.*

SQL Instance Monitoring

To collect data from a SQL Instance, the collection account must have access to all system tables and specific permissions on certain objects in the master and MSDB databases. The required permissions vary based on the SQL version being monitored.

SQL Server Permissions

SQL 2019 and older SQL versions:

- **Sysadmin** privileges

SQL 2022 and newer SQL versions:

- Member of both Roles:
  - ##MS_ServerStateReader##
  - ##MS_DefinitionReader##

Master Database Permissions

- Grant **View** Any Error Log
- Grant **Execute** on Objects:
  - xp_instance_regenumvalues
  - xp_regread

MSDB Database Permissions

- Grant **Select** on Objects:
  - sysmail_event_log
  - sysmail_allitems
  - log_shipping_monitor_primary
  - log_shipping_primary_secondaries
  - sysalerts
  - suspect_pages
  - sysjobhistory
  - sysjobschedules
  - sysschedules

- sysjobs
- syscategories
- sysjobsteps
- backupset

User Databases Query Store

All User Databases when **Query Store** is enabled

- Grant **Select** on Object:
  - QueryStoreTable
    - Use for a more efficient collection of Query Statistics information

Azure SQL Permissions

The Account used to connect to an Azure connection can be the Monitoring Service Account, a different Windows account, an Azure AD account, or a SQL account. For Managed Instances and Azure SQL Databases, Host metrics may be unavailable or significantly limited.

Azure Managed Instance

Collection Account required permissions

- **Sysadmin** role

Azure SQL Database

The data collection login account must be created in the Master database and each SQL Database being monitored.

Required Account Permissions:

- View Database State permissions

Required account roles:

- ## MS_DatabaseConnector##
- ##MS_ServerStateReader##
- ##MS_DefinitionReader##

Monitoring Amazon Instances

ECS Instances

The requisite account permissions are the same as above in the ***SQL Instance Monitoring*** above.

RDS Instances

To monitor an RDS instance, you need a SQL authentication account designated for data collection. This account must be set up on each database, including the Master, MSDB, and all user databases that are being monitored. Additionally, the account must be

assigned specific roles and permissions within these databases to ensure effective monitoring.

Master Database Requirements

- **Role:**
  - ProcessAdmin

- **Permissions:**
  - View Server State
  - View Any Definition
  - Create and View Any Database
  - Alter Trace

MSDB Requirements:

- **Role:**
  - SQLAgentUserRole

RDS Objects Permissions:

- **Execute** Permissions on:
  - rds_backup_database
  - rds_restore_database
  - rds_task_status
  - rds_cancel_task

- **Select** Permissions on:
  - sysJobs
  - sysJobHistory
  - sysJobActivity

User Database Requirements:

- Permission:
  - Grant ShowPlan