FORTIFIED WISdom™

WISdom Installation Requirements

Updated: June 4, 2026

Overview

WISdom provides an agentless data collection service that gathers system metadata, runtime statistics, and configuration data from each monitored SQL Server environment. Using Microsoft Azure infrastructure, WISdom ensures secure data transfer, processing, and storage within a client-isolated cloud environment.

The WISdom Data Collector runs on a virtual machine (VM) within your network. It connects directly to monitored SQL Server instances using SQL calls, Windows Management Instrumentation (WMI), and Windows Performance Counters. Collected data is organized into flat files, temporarily stored on the collector host, then compressed, encrypted, and transmitted to a dedicated WISdom Azure API for processing and secure storage in a client-specific Azure database.

Each client's data collector is assigned a unique encryption key pair, provided by Fortified, which is automatically rotated weekly.

Security Protocols and Features

WISdom is designed for high performance with minimal system impact while maintaining strong security standards:

- **Data Collection:** Uses WMI and SQL calls to gather metadata, runtime, and configuration data. No sensitive data is transferred.
- **Collection Frequency:** Data is collected as needed — ranging from once per minute to once per week.
- **Upload Process:** Data is encrypted via TLS and sent to the Azure API, then stored in the client's individual, dedicated Azure database for display in the WISdom UI.
- **Encrypted Data Access:** Configuration updates are encrypted and transmitted via Azure API using a certificate pair stored only on the central server and the client's WISdom host.

Prerequisites

WISdom Services Host

The host machine must be properly configured to connect to the Fortified WISdom Azure API, all target SQL instances, and the SQL hosts.

Windows System Requirements

- **Operating System:** Must be equal to or newer than the OS of all monitored machines.
  - Microsoft does not support WMI or performance metric collection from a lower-version OS.

Firewall Rules

Inbound — Access to Managed Servers

Service	Port(s)
SQL Server (default)	1433
Non-standard SQL Server ports	As configured
SQL Browser (named instances)	1434
WMI	135 and 49154
WMI dynamic range (if 49154 unavailable)	49152–65535
Performance Counters	445

Outbound — WISdom Cloud Access

Allow HTTPS traffic to: https://collectorapi.fortifiedwisdom.com

Region	IP Range
US East 2	20.85.14.224/29
US East 2	20.122.252.88/32
US Central	20.236.234.64/29

Antivirus Exclusions

Exclude the following folders and all subdirectories from antivirus scanning:

- %Installation Folder%\CollectorResults
- %Installation Folder%\UploadReady
- % Installation Folder%\ESUploadReady (if present)

> ***Note:*** *Default installation folder is:* ***C:\Fortified\WISdom.*** *If a drive other than C: is present with available space, WISdom will default to that drive. Older WISdom installations may have been placed in C:\Program Files\Fortified\Wisdom. The installation path is user-configured during setup.*

Service Account Requirements

The WISdom service account runs the Watchdog and Collector Windows services on the WISdom host machine.

Account Type

Account Type	Recommendation	Notes
Group Managed Service Account (gMSA)	Recommended — Best Practice	Automatic password management, simplified administration. Ideal for enterprise environments.
Domain Account	Alternative	Centralized control via Active Directory. Requires manual password management.
Local Windows Account	Not Recommended	Requires secondary credentials to be created and assigned to monitored targets in the WISdom UI. Additional service account permissions are required — see note below.

Best Practice: *Use a Group Managed Service Account (gMSA) whenever possible. gMSAs provide automatic password rotation, eliminate manual credential management, and align with Microsoft's security guidance for service accounts.*

Permissions — WISdom Host Machine

The service account requires the following permissions on the WISdom host:

- **Log on as a Service** — Required to run the WISdom Windows service.
- **Local Administrator rights on the WISdom host** — Required to start, stop, and restart the Fortified WISdom Watchdog and Collector services.

Note: *Local Windows Account: If the service account is a local Windows account (not a domain account), Local Administrator rights alone are not sufficient for service control. Explicit permissions must be set on both services using SDDL (Security Descriptor Definition Language) directly on the service objects.*
If adding the account to the Local Administrators group is not permitted, the account must have at minimum Full Control permissions on the WISdom installation directory.

Collection Server Sizing

Provision the WISdom collection VM based on the number of monitored endpoints.

Managed Servers	CPU Cores	RAM	Storage
1–75	4	8–16 GB	25 GB
76–200	8	16 GB	50 GB

Note: *Managed server counts are approximate. The volume of data generated per server, determined by the number of databases hosted and transaction volume, will affect how many targets a single VM can reliably manage. Highly transactional instances and servers hosting many databases may require fewer targets per VM.*

Environments monitoring cloud databases (e.g., Azure SQL Databases): each Azure SQL Database has its own connection and behaves more like an independent instance than a traditional database. Plan capacity accordingly.

Managing more than 200 servers or cloud databases on a single VM may lead to performance bottlenecks. Consider deploying additional VMs and distributing workloads.

Best Practice: *For improved fault tolerance and load distribution, deploy two smaller VMs instead of one large instance. This approach enhances resilience and simplifies maintenance.*

Collection Requirements

Collection Account Options

Account Type	Use Case
Monitoring Service Account (Recommended)	Preferred for collecting both Windows and SQL Server metrics.
Secondary Windows or Entra Accounts	Used when different credentials are needed for specific targets (other domains/DMZs). Supports Active Directory and Microsoft Entra ID accounts.
SQL Account	SQL data collection only. WMI and Performance Counter metrics will not be collected.

Windows Monitoring

A Windows account is required to collect Performance Counter and WMI data. A Windows Active Directory (AD) account is preferred. If a SQL account is used for collection, WMI and Performance metrics will not be collected and costing information cannot be calculated.

Permissions on Target Servers — Least Privilege (Recommended)

Configure the following group membership and permissions on each monitored Windows server:

- Group Membership in these groups:
  - Performance Monitor Users
  - Distributed COM Users
  - Remote Management Users
- Explicit WMI Namespace Security permissions (root\CIMV2) – see steps below

Configuring WMI Namespace Security

See Configuring WMI Namespace Security in the WISdom User Guide, for detailed steps.

> ***Note:*** *In older Windows Server versions, adding the collection account to the Local Administrators group was the standard approach and implicitly granted all required WMI, DCOM, and Performance Counter permissions. Microsoft's current security guidance discourages broad Local Administrator access. The least privilege configuration above is recommended for all new deployments.*

SQL Instance Monitoring Requirements

The collection account must have access to system tables and specific permissions in the master, msdb, and user databases. Required permissions vary by SQL Server version.

SQL Server Permissions by Version

SQL Server 2019 and Earlier

- **Recommended:** sysadmin privileges.
- **Alternative (Least Privilege):** Refer to the Non-SA Collection section in the WISdom User Guide.

SQL Server 2022 and Later

- **Required:** sysadmin privileges, or the least-privilege server roles below.

Required Least Privilege — Server Roles (SQL 2022+)

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

Database-Specific Permissions

Master Database

- GRANT VIEW ANY ERRORLOG
- GRANT ALTER TRACE
- GRANT EXECUTE on:
  - xp_readerrorlog
  - xp_instance_regenumvalues
  - xp_enumerrorlogs
  - xp_regread

MSDB Database

- GRANT SELECT on:
  - 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 with Query Store Enabled (Optional)

When Query Store is enabled, WISdom uses it for more efficient query statistics collection with reduced server impact compared to DMV-based collection.

- GRANT SELECT on:
  - sys.query_store_query
  - sys.query_store_plan
  - sys.query_store_runtime_stats
  - sys.query_store_runtime_stats_interval
  - sys.query_store_wait_stats
  - sys.database_query_store_options
  - sys.query_context_settings
  - sys.query_store_query_text
  - sys.query_store_query_hints
  - sys.database_query_store_internal_state

Azure SQL Monitoring

Azure Managed Instance (MI) Permissions

Master Database

- GRANT VIEW ANY ERRORLOG
- GRANT ALTER TRACE
- GRANT EXECUTE on:
  - xp_readerrorlog
  - xp_enumerrorlogs

MSDB Database Permissions

- GRANT SELECT on:
  - sysmail_event_log
  - sysmail_allitems
  - log_shipping_monitor_primary
  - log_shipping_primary_secondaries

  - sysalerts
  - suspect_pages
  - sysjobhistory
  - sysjobschedules
  - sysschedules
  - sysjobs
  - syscategories
  - sysjobsteps
  - backupset
- EXEC permissions on: agent_datetime

User Databases with Query Store Enabled (Optional)

- GRANT SELECT on:
  - sys.query_store_query
  - sys.query_store_plan
  - sys.query_store_runtime_stats
  - sys.query_store_runtime_stats_interval
  - sys.query_store_wait_stats
  - sys.database_query_store_options
  - sys.query_context_settings
  - sys.query_store_query_text
  - sys.query_store_query_hints
  - sys.database_query_store_internal_state

Azure SQL Database

The collection account must exist in the master database and each monitored user database.

- Required Permission: VIEW DATABASE STATE
- Required Roles:
  - ##MS_DatabaseConnector##
  - ##MS_ServerStateReader##
  - ##MS_DefinitionReader##

Note: *Host-level metrics are unavailable in Azure MI and SQL DB environments.*

Amazon SQL Monitoring

Amazon EC2 Instances

- Use the same permissions as standard SQL Server instance monitoring.
- For WMI collection, configure the least-privilege group memberships and WMI namespace security as described in the Windows Monitoring section above.

Amazon RDS Instances

Use a SQL-authenticated account created in master, msdb, and all monitored user databases.

Master Database

- **Role:** ProcessAdmin
- Permissions:
  - VIEW SERVER STATE
  - VIEW ANY DEFINITION
  - CREATE DATABASE
  - VIEW ANY DATABASE
  - ALTER TRACE

MSDB Database

- **Role:** SQLAgentUserRole

RDS-Specific Object Permissions

- GRANT EXECUTE on:
  - rds_backup_database
  - rds_restore_database
  - rds_task_status
  - rds_cancel_task
- GRANT SELECT on:
  - sysjobs
  - sysjobhistory
  - sysjobactivity

User Databases

- GRANT SHOWPLAN