



# Tungsten Monitor

## Release Notes

Version: 8.3.0

Date: 2024-07-05

**TUNGSTEN**  
**AUTOMATION**

© 2011–2024 Tungsten Automation. All rights reserved.

Tungsten and Tungsten Automation are trademarks of Tungsten Automation Corporation, registered in the U.S. and/or other countries. All other trademarks are the property of their respective owners. No part of this publication may be reproduced, stored, or transmitted in any form without the prior written permission of Tungsten Automation.

Third-party software is copyrighted and licensed from Tungsten Automation suppliers.

Reveille is a trademark of Reveille Software. All other trademarks, registered trademarks, service marks, trade names, or brand names mentioned in this document are the property of their respective owners.

# Table of Contents

Release Notes.....	4
End User License Agreement.....	4
System Requirements.....	4
Permissions Required in Windows Domain Environments.....	4
Tungsten Monitor Multi-Server Installation.....	5
Changing the Tungsten Monitor Database Password.....	6
Tungsten Monitor High Availability (HA) Setup.....	6
Running Tungsten Monitor From a Separate Web Server.....	6
SSL Enablement Information.....	7
New Features.....	7
Upgrading from Earlier Versions.....	8
Tungsten Monitor SNMP Trap Information.....	9
SNMPV1.....	9
SNMPV2c.....	9
SNMPV3.....	9
Starting the Tungsten Monitor Admin Console.....	10
Accessing the Tungsten Monitor Home Page.....	10
Known Issues.....	10
Navigation Icons Incorrectly Displayed.....	10
Installation Error on Windows Server 2016 / 2019 / 2022.....	11
Installation Error on Windows Server 2016 / 2019 / 2022.....	11
Error: 'The requested operation cannot be performed on a file with a user-mapped section open'.....	11
Tungsten Monitor Cannot Report Separate Metrics for KTM Server 2.....	11
Windows Server Event Log Access Errors.....	11
Windows Event Log Access Errors.....	11
Windows Event Log Source Name Filtering.....	12
Oracle ODBC Driver Setup and Configuration.....	12
WinApp Service Account Permission.....	12
Additional Resources.....	12
Related Documentation.....	13
Training.....	13
Getting help with Tungsten Automation products.....	13

# Release Notes

Please read this document carefully, as it contains information that may not be included in other Tungsten Monitor documentation.

 Prior to installing this release, please be sure to run the Tungsten Monitor Prerequisites Server Check Utility, which is available from the Tungsten Automation website and included with Tungsten Monitor software distribution. Review *Using Tungsten Monitor Wizards* for additional Tungsten Monitor configuration and setup details. This document is also included with the Tungsten Monitor software distribution.

## End User License Agreement

The Tungsten Automation End User License Agreement (EULA) contains the terms and conditions for using this software. If you do not accept the EULA, do not install the software; or if installed, uninstall the software and destroy all copies. Usage of the software implies acceptance of the terms and conditions of the EULA.

## System Requirements

This section contains various system requirements for Tungsten Monitor.

The server and client workstations used for Tungsten Monitor must meet the system requirements listed in the *Tungsten Monitor 8.3.0 Technical Specifications* document, which is available from the [Knowledge Base](#) on the Tungsten Automation website.

## Permissions Required in Windows Domain Environments

If using Windows domain accounts, Tungsten Monitor requires the domain user account to be a member of the local Admin Group (the Power Users group does not have sufficient permissions to access the local file system) for Tungsten Monitor to have local file system access and be allowed by UAC.

When setting permissions for a domain user, you must be logged in to the Tungsten Monitor server with a domain user account.

Use the Tungsten Monitor permissions manager to optionally map multiple ADS domains and also specify the ADS container (optional). For example, if the user signs in with the Windows account "abc\Username" (login domain is "abc"), and within ADS the user object "Username" is found under domain "abc.123root.net", the domain mapping entry is:

From: abc To: abc.123root.net Container: <optional>

To reduce the time to enumerate large Windows ADS domain groups during account authentication, use the group mapping option within the Tungsten Monitor permissions manager to specify a specific domain group during access verification.

 The To and Container values are case-sensitive.

If using nested groups, only domain groups nested in the local administrators group of the local Tungsten Monitor server are supported. Nesting domain groups in other local Tungsten Monitor server groups is not supported.

When using a domain account to access the User Console, the identity of the Tungsten Monitor Application Pool must be a Windows domain account for Tungsten Monitor to query the domain controller for validating monitor and Tungsten Monitor permissions.

## Tungsten Monitor Multi-Server Installation

To add a new Tungsten Monitor 8.3.0 server to an existing Tungsten Monitor 8.3.0 database as a worker server:

1. Create the 32-bit ODBC DSNs to the existing Tungsten Monitor 8.3.0 Monitor/ Metric databases on the new worker server.
2. Run the Tungsten Monitor 8.3.0 installer on the new worker server.
3. Select the option indicating that the database already exists at the database installation panel during installation.
4. Select the ODBC DSNs to the existing Tungsten Monitor 8.3.0.
5. The new Tungsten Monitor 8.3.0 server is added as another worker server in a Multi-Server system.

To update an existing Tungsten Monitor 8.3.0 server to use a different Tungsten Monitor 8.3.0 database to form a Multi-Server system:

1. Create the 32-bit ODBC DSNs to the different Tungsten Monitor 8.3.0 database on the existing Tungsten Monitor 8.3.0 server.
2. Stop the Tungsten Monitor monitoring service on the existing Tungsten Monitor 8.3.0 server.
3. In the Admin Console, change the database to use the different Tungsten Monitor 8.3.0 database.
4. Open a Windows Command Prompt window with local administrator rights.
5. Run the Tungsten Monitor command: 'Reveille\Bin\ReveilleUpdateSettings -Init' from the x:\<Tungsten Monitor installation>\reveille\bin Directory.
6. Start the Tungsten Monitor monitoring service on the existing Tungsten Monitor 8.3.0 server.

To completely remove a server from the Multi-Server system, follow the normal Tungsten Monitor uninstallation steps on that server.

To remove a server from a Multi-Server system but *\*not\** uninstall it, then on that server:

1. Stop the Tungsten Monitor monitoring service.

2. Open a Windows Command Prompt window with local administrator rights.
3. Run the Tungsten Monitor command: 'Reveille\Bin\ReveilleUpdateSettings -Delete' from the x:\<Tungsten Monitor installation>\reveille\bin Directory.
4. In the Admin Console, change the database to use the original Tungsten Monitor 8.3.0 server database.
5. Start the Tungsten Monitor monitoring service.

## Changing the Tungsten Monitor Database Password

To change the Tungsten Monitor Database Password:

1. Open a Windows Command Prompt window with local administrator rights.
2. Navigate to the x:<Tungsten Monitor install path>ReveilleSoftware\Reveille\bin directory.
3. Run the ReveilleUpdateDbPasswords.exe program.
4. Update the Monitor and Scorecard Database passwords.

## Tungsten Monitor High Availability (HA) Setup

Tungsten Monitor 8.3.0 supports the use of Failover Clusters with Windows Server 2022 R2 / 2019 / 2016 with the generic service resource to accomplish active/active HA. There are no registry keys to replicate during the setup.

For more information, see [Create a failover cluster](#) on the Microsoft documentation website.

Configure the cluster to start Tungsten Monitor server 2 when Tungsten Monitor server 1 stops, and Tungsten Monitor server 2 will continue monitoring.

 Monitors that were running when Tungsten Monitor server 1 stopped will not have completed. When the same monitors start on Tungsten Monitor server 2, they will start from the beginning, not from where they were testing when Tungsten Monitor server 1 stopped processing.

Tungsten Monitor can be configured to support a 3-tier implementation to further separate Tungsten Monitor subsystems for HA. Both the Tungsten Monitor application server and the Tungsten Monitor web server require an ODBC connection to the Tungsten Monitor database.

## Running Tungsten Monitor From a Separate Web Server

Tungsten Monitor 8.3.0 can be installed on a Tungsten Monitor application server, and use a separate web server.

Assumptions:

- The Tungsten Monitor application server and web server are using the same Tungsten Monitor database.
- The Tungsten Monitor application server and web server can communicate with each other (for example, no communications issues from the web server being in a different domain than the Tungsten Monitor application server).

- They both can use the same Windows user ID for the Reveille services and the Reveille application pool.
- The "same" directory structure / drive is used for the Tungsten Monitor installation on both.
- Tungsten Monitor application server and web server.

#### Setup:

- Install Tungsten Monitor server as a standard installation on Tungsten Monitor application server.
- Install Tungsten Monitor on the web server as a standard installation on the web server pointing to the existing Tungsten Monitor database (before installation, verify the web server has all Tungsten Monitor prerequisites installed, such as NET Framework 4.8, etc.)
- Disable the Reveille monitor service on the web server.
- On the Tungsten Monitor application server, Admin Console> Server> General Tab: set the Web Server address to the web server.
- Restart the Reveille monitor service on the Tungsten Monitor application server.

#### Verification:

- Browse to the Tungsten Monitor User Console on the web server, and the Tungsten Monitor application server name will be shown in the root of the user console tree.

## SSL Enablement Information

To enable SSL (HTTPS), use for the Tungsten Monitor User Console:

- Enable SSL binding for IIS. See <http://learn.iis.net/page.aspx/144/how-to-set-up-ssl-on-iis/>
- Restart IIS.

To enable SSL use by Tungsten Monitor for all monitor tests and proactive actions:

- In the Tungsten Monitor Admin Console, select the server, then the General tab, web server section.
- Select the Web Server SSL option.
- Update the Server Address with the SSL port, such as localhost:443.
- Save the changes.

## New Features

This Tungsten Monitor release provides support for the following Tungsten Automation applications:

- Tungsten Capture (formerly Kofax Capture) 11.0 and higher with all service packs
- Tungsten TotalAgility (formerly Kofax TotalAgility) 7.9 and higher
- Tungsten Analytics for Capture (formerly Kofax Analytics for Capture) 2.0 and higher
- Tungsten Communication Server (formerly Kofax Communication Server) 10.4.0 and higher
- Tungsten Import Connector (formerly Kofax Import Connector) 2.9 and higher
- Tungsten Front Office Server (formerly Kofax Front Office Server) 4.3
- Tungsten VRS (formerly Kofax VRS) 5.2 and higher

- Tungsten Transformation (formerly Kofax Transformation Modules) 6.4 and higher

New capabilities introduced in Tungsten Monitor 8.3.0 include:

- Notification dashboard
- Notification banner
- PostgreSQL database support
- Advanced Test Edit
- Group Dashboards viewer
- Improved Tungsten Monitor application failover
- Expanded set of Tungsten Monitor connectors for Jira, Kaseya Datto, HaloPSA, and Open Telemetry (OTEL)
- Updated the Tungsten License Server and Client levels.

Additional enhancements to Tungsten Monitor include:

- Rebranding to reflect the new product and company names.

Prior to 2024, Tungsten Monitor software was known as *Kofax Monitor*, and Tungsten Automation was known as *Kofax, Inc*. The release notes and other documentation refer to products supported for use with Tungsten Monitor by their newly rebranded names, and their previous names are also referenced. The branding of your Tungsten Automation product may vary, based on the version you use with Tungsten Monitor. For more information, visit the [Tungsten Automation website](#).

- Updates to address Tungsten Monitor Known Issues.

## Upgrading from Earlier Versions

Tungsten Monitor has several new features and enhancements. Tungsten Automation strongly recommends that you contact your Tungsten Automation Account Representative to discuss your current environment and map out a plan to successfully upgrade your existing Tungsten Monitor system to this version.

A mandatory database update is required when upgrading from version 8.x. The database migration utility is located in the Tungsten Monitor software distribution in the X:\Migration directory.

Refer to the *Tungsten Monitor 8.3.0 Migration Guide* for specific requirements and detailed information.

 Any changes to Tungsten Monitor-supplied files (`asp/aspix/config/inc/etc`) should be backed up and saved prior to migrating to the new version.

## Tungsten Monitor SNMP Trap Information

### SNMPV1

For SNMP V1 traps, the Tungsten Monitor trap is a Trap generic type of "6" for enterprise with a Trap specific type of "6". The Trap OIDs within the V1 trap are unique as listed in the following table.

Trap OID	Trap Value
1.3.6.1.4.1.10441.2.10.1.5	Message Date
1.3.6.1.4.1.10441.2.10.1.10	Message Time
1.3.6.1.4.1.10441.2.10.1.15	Monitor Name
1.3.6.1.4.1.10441.2.10.1.20	Resource Name
1.3.6.1.4.1.10441.2.10.1.25	Test Sequence Number
1.3.6.1.4.1.10441.2.10.1.30	Test Description
1.3.6.1.4.1.10441.2.10.1.35	Notification Message
1.3.6.1.4.1.10441.2.10.1.40	Status
1.3.6.1.4.1.10441.2.10.1.45	Escalation

### SNMPV2c

For SNMP V2c traps, the Tungsten Monitor V2c trap is now compliant RFC 2089 and RFC 1089. The Trap OIDs within the V2c trap are unique as listed in the following table.

Trap OID	Trap Value
1.3.6.1.4.1.10441.2.10.1.6	Message Date
1.3.6.1.4.1.10441.2.10.1.10	Message Time
1.3.6.1.4.1.10441.2.10.1.15	Monitor Name
1.3.6.1.4.1.10441.2.10.1.20	Resource Name
1.3.6.1.4.1.10441.2.10.1.25	Test Sequence Number
1.3.6.1.4.1.10441.2.10.1.30	Test Description
1.3.6.1.4.1.10441.2.10.1.35	Notification Message
1.3.6.1.4.1.10441.2.10.1.40	Status
1.3.6.1.4.1.10441.2.10.1.45	Escalation

### SNMPV3

To configure SNMP V3 authentication, go to **Tungsten Monitor > Admin Console > Alerts**, and select **SNMP V3 > Advanced**. Then enter the required information per your installation. The unique Tungsten Monitor Engine ID is 8000010441FFEEDCCBBAA.

For SNMP V3 traps, the Tungsten Monitor V3 trap is compliant with RFC 3414 and RFC 3826. The Trap OID's within the V3 trap are unique as listed in the following table.

Trap OID	Trap Value
1.3.6.1.4.1.10441.2.10.1.6	Message Date
1.3.6.1.4.1.10441.2.10.1.10	Message Time
1.3.6.1.4.1.10441.2.10.1.15	Monitor Name
1.3.6.1.4.1.10441.2.10.1.20	Resource Name
1.3.6.1.4.1.10441.2.10.1.25	Test Sequence Number
1.3.6.1.4.1.10441.2.10.1.30	Test Description
1.3.6.1.4.1.10441.2.10.1.35	Notification Message
1.3.6.1.4.1.10441.2.10.1.40	Status
1.3.6.1.4.1.10441.2.10.1.45	Escalation

## Starting the Tungsten Monitor Admin Console

To start Tungsten Monitor Admin Console, go to: **Start > Tungsten Monitor > Admin Console**.

Alternatively, select the Tungsten Monitor Admin Console desktop icon.

## Accessing the Tungsten Monitor Home Page

The Tungsten Monitor home page can be accessed from the Tungsten Monitor server using a browser with this URL: `http://localhost/reveille`. Replace "localhost" with the "hostname" of the Tungsten Monitor Server for non-local access.

Alternatively, go to **Start > Tungsten Monitor > User Console** (available on the Tungsten Monitor Server), or select the Tungsten Monitor User Console desktop icon.

Refer to the *Tungsten Monitor Online Help* for detailed information.

## Known Issues

This section gives information about issues that you may encounter while using Tungsten Monitor. Workarounds are provided, as applicable.

### Navigation Icons Incorrectly Displayed

Navigation icons are incorrectly displayed on Metrics Dashboards. These icons are standard fonts (not images) and they require a .woff MIME type defined in IIS. This is a standard MIME type for IIS included with the IIS 8.0/10.0 installation. (656375)

**Workaround:** Add the .woff MIME type definition in IIS MIME Types to resolve the problem.

- File name extension: .woff
- MIME type: font/x-woff

## Installation Error on Windows Server 2016 / 2019 / 2022

Operation failed with error code 0x8007000B.

An attempt was made to load a program with an incorrect format.

**Workaround:** Install the ASP.NET 3.5/4.6 role service for the IIS Web Server.

## Installation Error on Windows Server 2016 / 2019 / 2022

Operation failed with error code 0x80070442.

The service cannot be started, either because it is disabled or because it has no enabled device associated with it.

**Resolution:** Verify that the COM+ System Application Windows service is running.

## Error: 'The requested operation cannot be performed on a file with a user-mapped section open'

The Windows Server Microsoft Search indexing can cause issues when rewriting files such as the User Console user profile file. To resolve the issue, turn off indexing on the Reveille folder.

## Tungsten Monitor Cannot Report Separate Metrics for KTM Server 2

Tungsten Monitor cannot report separate metrics for KTM Server 2. This is because Tungsten Capture (formerly Kofax Capture) does not report separate metrics for KTM Server 2. The metrics from KTM Server 2 are merged with the metrics for KTM Server 1. (SPR 00089410)

**Workaround:** Run the KTM modules interactively. This must be done from a Command Prompt window using the /I n switch, where n is the number of the server (1 or 2). For example, "/I 1". Note that a space is required after /I.

## Windows Server Event Log Access Errors

When using WMI or event log tests with Windows Server 2016 / 2019 / 2022, add a Windows account with local administrator rights to the Event Log Readers Group.

## Windows Event Log Access Errors

The following error message appears when using check Windows event log wizard or test:

ERROR: Attempted to perform an unauthorized operation.

A Windows Event log test uses Windows impersonation (as does File Access Wizard), so the same Windows account user ID and password must reside on both the Reveille server and the target Windows server. For more information, see: [http://msdn.microsoft.com/en-us/library/aa376391\(v=VS.85\).aspx](http://msdn.microsoft.com/en-us/library/aa376391(v=VS.85).aspx)

## Windows Event Log Source Name Filtering

When filtering Windows event logs with event source names, use the event provider name available in the event details xml view. Do not use the displayed source name.

Example:

Display Source Name: SharePoint Portal Server

XML View Provider Name: Microsoft-SharePoint Products-SharePoint Portal Server

## Oracle ODBC Driver Setup and Configuration

1. Confirm that the Oracle ODBC drivers have the correct security permissions by explicitly setting read/execute level authority for "authenticated users" to the Oracle Home folder and also propagate to child objects by checking "Allow inheritable permissions".  
Select the "advanced setting" from the Security tab from the Oracle Home folder directory (for example, "x:\oracle\product\<product version>\client\_1") properties to finish.
2. When configuring the Oracle ODBC DSN, check that the Oracle ODBC connection option "Force SQL\_WCHAR Support" is selected on the Workarounds tab (if tab is shown).

## WinApp Service Account Permission

The required permission for the WinApp service account to use RunProgramAsUser from a non-system account without "Interact with Desktop" must include the "Replace a process level token" security permission.

This security setting determines which user accounts can call the CreateProcessAsUser() application programming interface (API) so that one service can start another. An example of a process that uses this user right is Task Scheduler.

Default local accounts with this security:

- Network Service
- Local System

## Additional Resources

This section provides information about additional resources.

## Related Documentation

The release notes are a supplement to the following Tungsten Monitor 8.3.0 documentation:

- *Tungsten Monitor Installation and Setup Guide*
- *Tungsten Monitor Overview Guide*
- *Tungsten Monitor Online Help*
- *Using Tungsten Monitor Wizards*
- *Tungsten Monitor Migration Guide*
- *Tungsten Monitor Technical Specifications*

Your Tungsten Monitor documentation is available in your software package and from the Tungsten Automation website.

## Training

Tungsten Automation offers both classroom and computer-based training that will help you make the most of your Tungsten Automation solution. Visit the [Education Portal](#) on the Tungsten Automation website for complete details about the available training options and schedules.

## Getting help with Tungsten Automation products

The [Tungsten Automation Knowledge Portal](#) repository contains articles that are updated on a regular basis to keep you informed about Tungsten Automation products. We encourage you to use the Knowledge Portal to obtain answers to your product questions.

To access the Tungsten Automation Knowledge Portal, go to <https://knowledge.tungstenautomation.com/>.

 The Tungsten Automation Knowledge Portal is optimized for use with Google Chrome, Mozilla Firefox, or Microsoft Edge.

The Tungsten Automation Knowledge Portal provides:

- Powerful search capabilities to help you quickly locate the information you need.  
Type your search terms or phrase into the **Search** box, and then click the search icon.
- Product information, configuration details and documentation, including release news.  
To locate articles, go to the Knowledge Portal home page and select the applicable Solution Family for your product, or click the View All Products button.

From the Knowledge Portal home page, you can:

- Access the Tungsten Automation Community (for all customers).  
On the Resources menu, click the **Community** link.
- Access the Tungsten Automation Customer Portal (for eligible customers).  
Go to the [Support Portal Information](#) page and click **Log in to the Customer Portal**.
- Access the Tungsten Automation Partner Portal (for eligible partners).  
Go to the [Support Portal Information](#) page and click **Log in to the Partner Portal**.

- Access Tungsten Automation support commitments, lifecycle policies, electronic fulfillment details, and self-service tools.  
Go to the [Support Details](#) page and select the appropriate article.