Kofax Monitor
7.6.0

Release Notes

KOFAX
from Lexmark

2015-10-22

Contents

Release Notes

Please read these notes carefully because they contain information that is not included in the documentation.

Note Prior to installing this update, please be sure to run the Kofax Monitor Prerequisites Server Check Utility, available from the Kofax website.

End User License Agreement

The Kofax 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.

Content Changes

The table below provides information about changes to these release notes that were made since the initial posting to the Kofax Web site.

Revision	Date of Change	What Changed
	November 15, 2011	Initial release
	December 6, 2012	Added revised content for version 6.7.0
Kofax Monitor 6.7.0 R2	January 27, 2013	Added the following items to the Resolved Issues section: SPR00115138 Added version information to Release Notes section Added note about Kofax Monitor Prerequisites Server Check Utility to System Requirements and Introduction
Kofax Monitor 7.0.0	March 10, 2014	Modified System Requirements Updated New Features Section Added traps of SNMPV3
7.0.1	March 5. 2015	Added information on newly supported wizards
7.6.0	October 1, 2015	Various updates for new release.

System Requirements

This section contains various system requirements for Kofax Monitor.

The server and client workstations used for Kofax Monitor must meet the system requirements listed on the Kofax Web site. For information about supported operating systems and other system requirements for Kofax Monitor, visit the Support pages on the Kofax Web site at www.kofax.com.

Note Prior to installing this update, please be sure to run the Kofax Monitor Prerequisites Server Check Utility, available from the Kofax website.

Permissions Required in Windows Domain Environments

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

When setting permissions for a domain user, you must be logged into the Kofax Monitor server with a domain user account.

Use the Kofax Monitor permissions manager to optionally map multiple ADS domains and also specifying 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 Kofax Monitor permission manager to specify a specific domain group during access verification.

Note The To and Container values are case sensitive

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

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

Kofax Monitor Multi-Server Installation

To add a new Kofax Monitor 7.6.0 server to an existing Kofax Monitor 7.6.0 database as a worker server:

1. Create the 32-bit ODBC DSNs to the existing Kofax Monitor 7.6.0 Monitor/ Metric databases on the new worker server.
2. Run the Kofax Monitor 7.6.0 installer on the new worker server.
3. Select the database already exists at the database installation panel during installation.
4. Select the ODBC DSNs to the existing Kofax Monitor 7.6.0 database.

5 The new Kofax Monitor 7.6.0 server will be added as another worker server in a Multi-Server system.

To update an existing Kofax Monitor 7.6.0 server to use a different Kofax Monitor 7.6.0database to form a Multi-Server system:

1 Create the 32-bit ODBC DSNs to the different Kofax Monitor 7.6.0 database on the existing Kofax Monitor 7.6.0 server.
2 Stop the Kofax Monitor monitoring service on the existing Kofax Monitor 7.6.0 server.
3 In the Admin Console, change the database to use the different Kofax Monitor 7.6.0 database.
4 Open a windows command line session with local administrator rights.
5 Run the Kofax Monitor command: 'Reveille\Bin\ReveilleUpdateSettings -Init' from the x:\<Kofax Monitor installation>\reveille\bin Directory.
6 Start the Kofax Monitor monitoring service on the existing Kofax Monitor 7.6.0 server.

To completely remove a server from the Multi-Server system, follow the normal Kofax 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 Kofax Monitor monitoring service.
2 Open a windows command line session with local administrator rights.
3 Run the Kofax Monitor command: 'Reveille\Bin\ReveilleUpdateSettings -Delete' from the x:\<Kofax Monitor installation>\reveille\bin Directory.
4 In the Admin Console, change the database to use the original Kofax Monitor 7.6.0 server database.
5 Start the Kofax Monitor monitoring service.

Changing the Kofax Monitor Database Password

To change the Kofax Monitor Database Password:

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

Kofax Monitor High Availability (HA) Setup

Kofax Monitor 7.6.0.0 supports the use of Failover Cluster Manager in Windows 2008 with the generic service resource to accomplish active/active HA. There are no registry keys to replicate during the setup.

For Windows 2008 Cluster Server Manager setup see: http://blogs.msdn.com/b/clustering/archive/2009/06/09/9712609.aspx

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

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

Kofax Monitor can be configured to support a 3 tier implementation to further separate out Kofax Monitor subsystems for HA.

Running Kofax Monitor From a Separate Web Server

Kofax Monitor 7.6.0 can be installed on a Kofax Monitor application server and use a separate web server.

Assumptions:

- The Kofax Monitor application server and web server are using the same Kofax Monitor database.
- The Kofax Monitor application server and web server can communicate with each other (for example, No communications issues from the web server being in a different dmz than the Kofax 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 Kofax Monitor installation on both
- Kofax Monitor application server and web server

Setup:

- Install Kofax Monitor server as normal installation on Kofax Monitor application server.
- Install Kofax Monitor on the web server as a normal installation on the web server pointing to the existing Kofax Monitor database (before installation, verify the web server has all Kofax Monitor prereqs installed - .NET 3.5 Sp1, etc.
- *Disable* the Reveille monitor service on the web server
- On the Kofax Monitor application server, Admin Console, Server, General Tab - set the Web Server address to the web server
- Restart the Reveille monitor service on the Kofax Monitor application server

Verification:

- Browse the Kofax Monitor User Console on the web server and the Kofax 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 Kofax 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 Kofax Monitor for all monitor tests and proactive actions:

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

Recommended Updates for all Kofax Monitor Servers

KB 981575 - Encryption memory leak, a memory leak occurs in a .NET Framework 2.0-based application that uses the `AesCryptoServiceProvider` class.

`http://support.microsoft.com/kb/981575`

If using Windows Management Instrumentation (WMI) Wizard or tests:

KB 981314 - The "Win32_Service" WMI class leaks memory in Windows Server 2008 R2 and in Windows 7.

`http://support.microsoft.com/kb/981314`

KB 981314 - A memory leak issue occurs in the Windows Management Instrumentation service on a computer that is running Windows Server 2008 R2 or Windows 7.

`http://support.microsoft.com/kb/977357`

Kofax Monitor User Console Browser Configuration Requirements:

1024 x 768 minimum resolution

US English for browser locale

Kofax Communications Server 9.0 Requirements

Install the following patch when using the KCS wizard within a Kofax Monitor: "KCS Monitoring Patch".

This patch is available in the Kofax Communication Server 9.0 download package.

New Features

See the *Kofax Monitor 7.6.0 Overview Guide*, "What's New in Kofax Monitor" section for a complete list of new Kofax Monitor features and enhancements.

Known Issues

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

Navigation Icons Incorrectly Displayed

Navigation icons are incorrectly displayed on ScoreCards and Metrics Dashboards. These icons are standard fonts (not images) and so there needs to be a .woff MIME type defined in IIS. This is a standard MIME type for IIS included with the IIS 7.5/8.0 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

Error During Installation on Windows 2008 R2 or 2012 R2 Server

Operation failed with error code 0x8007000B.

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

Resolution:

Install the ASP.NET 3.5 role service for the IIS Web Server

Error During Installation on Windows 2008 R2 or 2012 R2 Server

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 the COM+ System Application windows service is running.

Error message "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.

Kofax Monitor cannot report separate metrics for KTM Server 2

Kofax Monitor cannot report separate metrics for KTM Server 2. This is because 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 window using the /I n swich, where n is the number of the server (1 or 2). For example "/I 1". Note that a space is required after /I.

Error Sending SMTP Email to Microsoft Exchange Server

When attempting to send email to a MicroSoft Exchange Server, the Kofax Monitor OnCall log contains the error: "Command not implemented. The server response was: Command not Supported."

This problem occurs because the remote SMTP server does not support the SMTP extended Hello (EHLO) command.

The exception occurs when the remote SMTP server returns the 502 reply code and the System.Net.Mail.SmtpClient class expects the 500 reply code. This is a known error with .NET 2.0 System.Net.Mail.SmtpClient class.

A hotfix is available from MicroSoft. Review the following knowledge base article: http://support.microsoft.com/kb/913616.

E-mail notification not working after installing Exchange 2000 SP 3

As Kofax Monitor uses Simple Mail Transfer Protocol (SMTP) mail by using a Collaboration Data Objects for Windows (CDOSYS) application, If Exchange 2000 Server Service Pack 3 (SP3) is installed, you receive the following error message: CDO.Message.1 (0x80040220) The "SendUsing" configuration value is invalid.

NoteSystem.Web.Mail is a managed wrapper to CDOSYS that allows Kofax Monitor to create and send messages by using the CDOSYS message component.

Please review MS KnowledgeBase article http://support.microsoft.com/default.aspx?kbid=816789 workaround section. The virtual directory to check for the anonymous account name is the x:\Program Files\ReveilleSoftware\Reveille\Web\Reveille directory.

HTTP 401.1 Error - Unauthorized: Access is Denied Due to Invalid Credentials

If you receive this error when accessing the Kofax Monitor user console from a non Kofax Monitor Server when running IIS 6.0 or 7.0, apply the workaround section fix in KB article 871179.

See Microsoft KB article 871179 for instructions on applying the workaround: http://support.microsoft.com/kb/871179.

2008 Server Event Log Access Errors

When using WMI or event log tests with Windows 2008 Servers, add a windows account with local administrator rights to the Event Log Readers Group.

Windows Event Log Access Errors

Receive below error message 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 userid and password must reside on both the Reveille server and the target windows server. For more information:

http://msdn.microsoft.com/en-us/library/aa376391(v=VS.85).aspx

Using WMI scripts with a Windows XP OS

For WinXP, the ForceGuest setting is enabled by default when in workgroup mode (not domain) and gives access problems for WMI connections and shares access, other DCOM services and RPC services as well.

Note that for WinXP Home you cannot disable the ForceGuest behavior (only in WinXP Pro).

On a computer running WinXP Pro, try this:

You can change this registry value without using regedit.exe through these steps:

1. Open the Local Security Policy console in the Administrative Tools folder.
2. Browse down to: Security Settings\Local Policies\Security Options.

3. Double-click on the Network Access: Sharing And Security Model For Local Accounts.
4. Change the settings from Guest Only to Classic. This feature is, by default, set to Classic when Windows XP Professional is joined to a domain.

On Windows XP, the ForceGuest registry value is set to 1 by default in the following registry key:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa
```

On a Windows XP computer that is a member of a workgroup:

- If ForceGuest is enabled (set to 1), SSPI will always try to log on using the Guest account.
- If the Guest account is enabled, an SSPI logon will succeed as Guest for any user credentials.
- If the Guest account is disabled, an SSPI logon will fail even for valid credentials.
- If ForceGuest is disabled (set to 0), SSPI will log on as the specified user.

Please review MS KnowledgeBase article http://support.microsoft.com/default.aspx?scid=kb;en-us;290403.

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.....".

   Choose the 'advanced setting' from the security tab from the Oracle Home folder directory (for example, “x:\oracle\product\10.2.0\client_1”) properties to complete this.
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: “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

Launching Internet Explorer (IE) 8.0 from Winapp

Internet Explorer 8.0 by default will perform crash recovery of previous IE sessions.

This can interfere with normal Winapp script processing for IE base applications and the setting should be disabled on Winapp application script machines.

Uncheck the “Enable automatic crash recovery” option within IE: Tools | Internet Options | Advanced Tab.

Migrating From Kofax Monitor (6.X/7.X)

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

There is a mandatory database update when upgrading from Kofax Monitor 6.x. The database migration utility is located on the `KM ISO in X:\Migration` directory.

Refer to the *Kofax Monitor Migration 7.6.0* Guide for specific requirements and detailed information.

Note Any changes to Kofax Monitor supplied files (`asp/aspx/config/inc/etc`) should be backed up and saved prior to migrating to this version.

Kofax Monitor SNMP Trap Information

SNMPV1

For SNMP V1 traps, the Kofax 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 have been made unique and are as follows

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 Kofax Monitor V2c trap is now compliant RFC 2089 and RFC 1089. The Trap OIDs within the V2c trap have been made unique and are as follows

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

Trap OID	Trap Value
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 Kofax Monitor Admin Console > Alerts > select SNMP V3 > Advanced. Then Enter the required information per your installation. The unique Kofax Monitor Engine ID is 8000010441FFEEDDCCBBAA.

For SNMP V3 traps, the Kofax Monitor V3 trap is compliant with RFC 3414 and RFC 3826. The Trap OID's within the V3 trap are unique and are as follows:

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

RSS Support Implementation

To implement Kofax Monitor RSS support, the following configuration updates are required on the Kofax Monitor server:

Enable the background RSS processing by updating the Kofax Monitor `AutoRun.xml file` definition to execute `ReveilleMonitorRSS.exe` on a periodic base (every 5 minutes is default).

Java Applet Information

Kofax Monitor installs the following files to enable the monitoring of SWING (not AWT) based java applets in these locations:

- [JRE]\lib\accessibility.properties
- [JRE]\lib\ext\josit.jar
- [JRE]\lib\ext\jaccess.jar

[JRE] represents the directory where the Sun Microsystems Java Runtime Environment (JRE) is installed. By default for JRE version 5, update 14, this location is "C:\Program Files\Java \jre1.5.0_14\".

Anytime a newer version of the Sun Microsystems JRE is installed, the Kofax Monitor JOSIT files (josit.jar, jaccess.jar, accessibility.properties) must be manually copied to the corresponding directories of the new JRE installation.

Starting the Kofax Monitor Admin Console

To start Kofax Monitor Admin Console, go to: Start Programs > Kofax Monitor > Admin Console.

Alternatively, select the Kofax Monitor Admin Console desktop icon.

Accessing the Kofax Monitor Home Page

Kofax Monitor's home page can be accessed from the Kofax Monitor server using a browser with this URL: `http://localhost/Reveille/homepage/system.aspx`. Replace "localhost" with the "hostname" of the Kofax Monitor Server for non local access.

Alternatively, go to Start Programs > Kofax Monitor > User Console (available on the Kofax Monitor Server), or Select the Kofax Monitor User Console desktop icon.

Refer to the Kofax Monitor - User Console Reference Guide for detailed information.

Changing the Kofax Monitor User Console Theme

To change the new Kofax Monitor User Console theme back to the previous Kofax Monitor 6.7 theme, change the below entry in the `web.config file` located in `<KM installation path>Reveille\Web\Reveille` directory. Backup the existing `web.config` file before making the change.

Change: `<pages theme="ReveilleTheme">`

To: `<pages theme="KofaxClassic">`

Additional Resources

This section provides information about additional resources.

Related Documentation

These release notes are a supplement to the following Kofax Monitor documentation:

- *Kofax Monitor 7.6.0 Installation and Setup Guide*
- ***Kofax Monitor** 7.6.0 Overview Guide*
- *Kofax Monitor 7.6.0 Online Help*
- *Using the Kofax Monitor 7.6.0 Wizards*
- *Kofax Monitor 7.6.0 Migration Guide*
- *Kofax Monitor 7.6.0 Overview Guide*

Your Kofax Monitor documentation is available in your software package and from the Kofax Web site.

Training

Kofax offers both classroom and computer-based training that will help you make the most of your Kofax Capture solution. Visit the Kofax Web site at www.kofax.com for complete details about the available training options and schedules.

Getting Help for Kofax Products

Kofax regularly updates the Kofax Support site with the latest information about Kofax products.

To access some resources, you must have a valid Support Agreement with an authorized Kofax Reseller/Partner or with Kofax directly.

Use the tools that Kofax provides for researching and identifying issues. For example, use the Kofax Support site to search for answers about messages, keywords, and product issues. To access the Kofax Support page, go to www.kofax.com/support.

The Kofax Support page provides:

- Product information and release news

  Click a product family, select a product, and select a version number.
- Downloadable product documentation

  Click a product family, select a product, and click **Documentation**.
- Access to product knowledge bases

  Click **Knowledge Base**.
- Access to the Kofax Customer Portal (for eligible customers)

  Click **Account Management** and log in.

  To optimize your use of the portal, go to the Kofax Customer Portal login page and click the link to open the *Guide to the Kofax Support Portal*. This guide describes how to access the support site, what to do before contacting the support team, how to open a new case or view an open case, and what information to collect before opening a case.
- Access to support tools

  Click **Tools** and select the tool to use.
- Information about the support commitment for Kofax products

  Click **Support Details** and select **Kofax Support Commitment**.

Use these tools to find answers to questions that you have, to learn about new functionality, and to research possible solutions to current issues.