

Sightline Enterprise Data Manager (EDM) Software Release Notes

Contents

Introduction.....	1
Power Agent Compatibility	2
Recommended Configuration	2
EDM 7.2.1 (September 2026).....	3
Installation notes	3
New Features	4
Changes.....	6
Known Issues in EDM 7.2.1	7
EDM 7.2 (July 2026)	7
Installation notes	7
New Features	8
Changes.....	10
Known Issues in EDM 7.2	11
EDM 7.1.1 Installation notes	12
EDM 7.1 Installation notes	12
Installing or upgrading Sightline EDM on Windows Systems	12
Installing or upgrading Sightline EDM on Linux Systems	13
EDM 7.0 Installation notes	13
Upgrade notes	13
Upgrade notes for 1-click upgrades	14
Upgrade notes for manual upgrades.....	14

Introduction

Sightline EDM provides centralized data collection, alerting, archiving and summarization for data provided by Sightline Power Agents and Interface Agents, as well as data collected agent-lessly from other data sources. EDM also provides a web-based interface for data visualization and reporting, root cause analysis, and forecasting.

These release notes describe new features and updates included in version 7.2.1 of Sightline EDM.

Power Agent Compatibility

This release of EDM is compatible with all data sources provided by Sightline Power Agents and Interface Agents.

This release supports web-based Agent Administration for Power Agents running a supported version of the SLAA Listener. For specific versions, contact your Sightline representative.

Recommended Configuration

Operating Systems

- ◆ Windows Server 2016
- ◆ Windows Server 2019
- ◆ Windows Server 2022
- ◆ Windows Server 2025
- ◆ Red Hat Enterprise Linux 9
- ◆ Oracle Linux 9

Minimum System Requirements

- ◆ **Processor:** Intel® Xeon® Processor E5-1620 v4
- ◆ **Memory:** 8-12 GB (up to 96GB if running SightlineDB for performance data repository)
- ◆ **HDD Free space:** 200 GB (varies by number of connections)
- ◆ **Operating System:** Microsoft Windows, Linux
- ◆ **Network Card:** Ethernet 10/100/1000Base
- ◆ **Network capacity:** 1Gbps

Supported Browsers

- ◆ Chrome
- ◆ Firefox
- ◆ Microsoft Edge

Java

EDM version	Java version
7.0, 7.1, 7.1.1, 7.2, 7.2.1	JRE or JDK 21

Wildfly

EDM version	JBoss/Wildfly version
7.0, 7.1, 7.1.1	Wildfly-37.0.1.Final
7.2, 7.2.1	Wildfly-39.0.1.Final

Admin Database

EDM version	Database type and version
7.0, 7.1, 7.1.1	◆ Microsoft SQL Server 2016, 2019, 2022 ◆ MySQL 5.6.20, 5.7.x, 8 ◆ PostgreSQL 15.10, 18.1
7.2, 7.2.1	◆ Microsoft SQL Server 2016, 2019, 2022 ◆ MySQL 5.6.20, 5.7.x, 8 ◆ PostgreSQL 18.3, 18.4

Database for Live Performance Data Repository

EDM version	Database type and version
7.0, 7.1, 7.1.1	◆ SightlineDB 1.7.1
7.2, 7.2.1	◆ SightlineDB 2.8

EDM 7.2.1 (September 2026)

Sightline EDM 7.2.1 includes an enhanced trace file-to-SightlineDB data migration utility, which lets sites that store performance data in trace files move that history into SightlineDB from the EDM web interface, one connection at a time. This release also hardens the SightlineDB 1.7 to 2.8 upgrade introduced in EDM 7.2, corrects the published free-space requirement for that upgrade, and resolves defects reported from the field.

Installation notes

Before upgrading to EDM 7.2.1, confirm that your current version is EDM 7.0 or higher. Upgrades from versions prior to EDM 7.0 are not supported. See the *EDM 7.1 Installation notes* for details about installer commands on Windows and Linux.

Sites upgrading from EDM 7.1.1 should also review the *EDM 7.2 Installation notes* below, which apply to this upgrade: the one-time SSL state repair via **System Settings**, the cleared **URL in alert email** field, and the replacement of `sightlinedb.conf` by `sightlinedb2.toml` (any tuning applied to the 1.7 file must be re-applied manually in the new file).

Installation and upgrade enhancements

- ◆ **Corrected free-space requirement for the SightlineDB 1.7 to 2.8 upgrade**
This applies to customers upgrading from EDM 7.1.1 or lower using SightlineDB 1.7. The EDM 7.2 release notes stated that the target drive must have at least two times the current SightlineDB 1.7 data size free. The correct requirement is the size of the existing SightlineDB 1.7 data plus 1 GB — for example, 50 GB of SightlineDB 1.7 data requires roughly 51 GB free. The earlier figure double-counted the 1.7 data already present on the drive. The installer checks this before starting the upgrade; where free space cannot be determined it now proceeds rather than refusing to run.

-
- ◆ **SightlineDB 1.7 data in a non-default location now detected correctly**

Detecting the SightlineDB 1.7 data directory in a non-default location has been corrected for installs on a drive other than C: and for configurations whose `sightlinedb.conf` specifies a data path with no drive letter (for example `\var\lib\sightlinedb`). Previously such an install could be treated as a fresh setup instead of an upgrade. Fully qualified paths (for example `J:\`) and UNC paths are unaffected. The upgrade and uninstall plans now report the actual data drive. An installation whose SightlineDB service is stopped at upgrade time is now also correctly identified as 1.7 rather than being left unmigrated.
 - ◆ **Adding SightlineDB to a trace-file-only installation**

Sites trace files can now add SightlineDB through the upgrade, which is the prerequisite for the trace file-to-SightlineDB migration described under **New Features**. SightlineDB remains an optional component and is not enabled automatically.
 - ◆ **Fresh install onto an existing admin database**

When a fresh install is pointed at an admin database that already contains EDM data, the installer now detects this and asks whether to keep the existing tables (the default) or reset them. Upgrades always keep existing tables. If the admin database cannot be reached, the installer keeps the existing data.
 - ◆ **Configuration settings are merged on upgrade**

New and updated settings in `config.properties`, `quartz.properties`, and `eventExcludeList.properties` are now added to your existing files during an upgrade; the file will not be overwritten. Settings you do not already have are appended, together with their comment blocks, so newly shipped optional settings are visible for you to enable. Your file's line endings and Windows paths are preserved.

New Features

- ◆ **Trace File to SightlineDB data migration**

Sites that store performance data in trace files can now migrate that data into SightlineDB from the EDM web interface, one connection at a time. The migration is performed from the **Migration Status** tab under **Connections**, and includes live metrics, events, and each configured summary tier.

 - **Migration plan before you commit**

Show Migration Plan lists each tier (live and event data, and each summary level) with its source size, time span, retention policy, and SightlineDB availability.
 - **Migrate only what is missing**

Each phase compares the trace file's time span against what SightlineDB already holds and migrates the data absent at either end — history older than SightlineDB's earliest point and data newer than its latest.
 - **Verification with a downloadable report**

Every migration is checked for completeness. The migration report leads with a verdict, lists any gap alongside the action to take for it, and can be downloaded from the EDM UI for review or for sending to Sightline Technical Support. The verdict is also shown on the connection's migration status line.

-
- **Verify before you switch reads**
The read source is selectable per connection — trace file, SightlineDB, or the Data Collector default — so you can migrate a connection, read data from SightlineDB in a Quick Chart while trace files are still being written, confirm the data matches, and only then switch that connection over. Migration never changes the read source on its own.
 - **Reclaim the disk afterward**
Once a connection's migration is complete and verified, a **Delete source tracefile** action removes the original trace files for that connection. This is always initiated by the user; EDM never deletes source trace files automatically.
 - **Clear outcomes**
A migration ends either **Completed** or **Failed per connection**. A write that EDM cannot confirm reached SightlineDB fails the run, and the message names what failed and why. A completed run whose verification found gaps stays **Completed**, with the findings and the recommended action in the verification report and an alert raised so the run stays visible. Migrations are not retried automatically — re-run the connection once the cause is resolved.

For the full procedure, see *Migrating Trace File Data to SightlineDB* in the *Sightline EDM User's Guide*. We recommend that you contact Sightline Systems or your local Sightline representative before a large migration.

- ◆ **Migration Status view for all connections**
A **Migration Status** view has been added to the **Connections** tab, showing migration state across every connection in one place. Columns include the proportion of data already in SightlineDB, how much remains, current lag, retention policy, read source, and throughput, with elapsed and remaining times. The view supports filtering and sorting, hiding completed connections, selecting connections with checkboxes, clicking through to a connection, and an explicit **Refresh**. The migration indicator on a connection links directly to this view.
- ◆ **Collector repository mode can now be set in the EDM interface**
The Data Collector Service write and read repository modes can be set from **Settings > Data Collectors** by an EDM Administrator, replacing hand-editing of `config.properties` to set up a migration and to cut over afterward. **Write** offers Trace File, SightlineDB, or Trace File and SightlineDB; **Read** is constrained to a repository used by DCS. The dropdowns are unavailable if SightlineDB is not active.
- ◆ **Renaming retention policies**
Retention policies can now be renamed. The rename is applied in SightlineDB and access under the previous name is preserved, so existing queries and reports continue to work.
- ◆ **Old summary files must be migrated individually**
When a connection has older (closed) trace files, they will not be automatically migrated. Present each file to the collector in turn and migrate again; each run accumulates into the same SightlineDB bucket.

Changes

- ◆ **EDM now listens on all network interfaces (ticket #27585)**
After upgrading EDM, the URL to access EDM by IP address no longer resolved because EDM server had multiple network adapters. The EDM service now binds to all interfaces.
- ◆ **Vulnerabilities in libcurl resolved (ticket #27578)**
A site's security scan flagged a set of vulnerabilities in the installed EDM instance, which were tracked to libcurl 8.21.0 used by PostgreSQL. Unused components (StackBuilder and libcurl) are now removed from the bundled PostgreSQL installation on Windows, as they are not used by Sightline EDM. Installations on Linux were not affected, because they did not include libcurl.
- ◆ **WildFly working files no longer deleted when standalone.bat is invoked (ticket #27568)**
After upgrading EDM, users found that EDM was accessible but then started displaying the message "<EDM Server> redirected too many times" and EDM was no longer available. Investigation shows that a legacy line in `standalone.conf.bat` deleted EDM's extracted WildFly working files under `standalone\tmp` every time `standalone.bat` was run, including a read-only version check issued by an external monitoring service. This has been corrected and the deletion will no longer occur.
- ◆ **EDM service start and stop hardening**
Stopping the Sightline EDM service now performs a more graceful shutdown, and the shutdown timeout has been increased. This also resolves the "Address already in use" upgrade failure listed as a known issue in EDM 7.2.
- ◆ **Services that were running before a custom install are restarted afterward**
After a custom install, services that were running before the upgrade will be returned to their previous running state.
- ◆ **Unattended installation to a pre-created directory failed**
A 1-click installation failed when the PostgreSQL installation directory already existed, reporting "The chosen installation directory exists and is non-empty" and exited without installing. The installer no longer pre-creates that directory, so installations to a prepared path now complete normally.
- ◆ **Retention policy changes are applied to SightlineDB when saved**
Editing a retention policy in EDM now applies the change in SightlineDB immediately on save. Previously, a retention policy change could be left unapplied in the performance data repository.
- ◆ **Installing SightlineDB no longer enables dual write automatically**
Installing SightlineDB previously turned on dual write without being asked to. Dual write is now left as configured by the user. Additionally, a newly installed SightlineDB uses the DCS drive.
- ◆ **SightlineDB retention and shard configuration no longer depends on creation order**
Bucket retention periods and shard geometry in SightlineDB are now set consistently regardless of the order in which buckets were created.
- ◆ **Deleting performance data from SightlineDB**
Deleting performance data for a connection now works correctly with SightlineDB 2.x.

-
- ◆ **Connection start time shows the actual start of data**
The connection start time displayed in EDM showed the current timestamp instead of the timestamp of the earliest available data. This has been corrected.
 - ◆ **Metric list remains available when a trace file has been removed**
For a connection whose data has been migrated to SightlineDB and whose trace file is no longer present, the metric list shown in a Quick Chart is now correctly retrieved from the SightlineDB symbol table.
 - ◆ **Security and dependency updates**
This release updates BouncyCastle to 1.84, Jackson to 2.18.8, and OmniFaces to 4.7.5, and removes an unused Velocity component, clearing a number of reported CVEs. EDM now sends the X-Frame-Options: SAMEORIGIN response header to prevent the application being framed by another site. Additional findings from internal code analysis have been addressed.

Known Issues in EDM 7.2.1

- ◆ **DCS connection fails over HTTPS when the certificate name does not match the server's host name (Linux)**
On Linux servers where EDM web HTTPS (SSL) is enabled with a certificate whose Subject Alternative Name (SAN) lists only the FQDN (for example, `host.example.local`) while the operating system reports the machine by its short name (for example, `host`), DCS cannot connect to EDM. Connections stay in "Connecting" with 0 data blocks, alert delivery fails, and the DCS log shows a certificate name-mismatch error. Windows servers are not affected. To work around this, reissue the HTTPS server certificate with both the FQDN and the short host name as DNS entries in its SAN (in **Settings > Certificates**, use the **Add** button to enter both names), enable HTTPS with the new certificate in **Settings > SSL Configuration**, and restart DCS. Because both names are on the certificate, the update will survive future SSL configuration changes and the post-upgrade sync. This will be fixed in a future release.
- ◆ **Cannot change trace file retention policy**
When writing to trace files, changing the retention policy causes DCS to stop writing to the live trace file. No data will be displayed for the connection, although the connection status is **Active** ("Receiving Data Blocks"). The End time will be advancing but the data block count will stop incrementing.

EDM 7.2 (July 2026)

EDM 7.2 is a major release that includes new features, platform upgrades, and targeted bug fixes

Installation notes

Before upgrading to EDM 7.2, confirm that your current version is EDM 7.1 or 7.1.1. Upgrades from versions prior to EDM 7.1 are not supported. See the *EDM 7.1 Installation notes* for details about installer commands on Windows and Linux.

Customers running SSL on 7.1.1 must log in and navigate to the System Settings page after upgrading to 7.2 to trigger an automatic SSL state repair.

On upgrade to 7.2, the **URL in alert email** field in **System Settings** is cleared so that the alert-email URL stays in sync with the active SSL configuration. Customers using a customized URL (e.g., a reverse-proxy front-end) should re-enter it after upgrading.

New Features

- ◆ **TLS / mTLS for Power Agent ↔ DCS communication**
End-to-end encryption between Windows and Linux Power Agents and the Data Collector Service, with TLS-mode defaults and clear mismatch error messages. Requires Windows Power Agent version 7.1 or Linux Power Agent version 7.2. See the Power Agent release notes for configuration details.
- ◆ **OpenTelemetry (OTLP)**
OTLP is a new protocol type including an Admin UI configuration wizard. OTLP provides endpoint and Event Data values, dynamic symbol-table / attribute-to-subscript mapping, and Protobuf (application/x-protobuf) content-type support.
- ◆ **In-product User Guide & Training Material**
A Help link and integrated User Guide are now accessible directly from the EDM UI.
- ◆ **Kafka monitoring via JMX connection**
EDM now includes a JMX connection subtype for Kafka data collection. Kafka JMX connections collect the standard JVM metrics **plus** ~17 curated Kafka-specific MBeans (broker throughput, replica state, controller state, consumer-group coordinator state).
- ◆ **Enhanced EDM Correlation**
EDM's correlation engine has been significantly expanded, giving you more ways to discover and validate relationships between metrics:
 - **Multiple correlation methods:** Choose Pearson, Spearman, or Kendall, or use **Compare All Methods** to evaluate all three side by side with the strongest method highlighted per metric.
 - **Time-lag analysis:** Set a maximum lag to detect leading indicators, metrics whose changes precede another metric's by one or more periods.
 - **Granger causality testing:** Optionally test for causal relationships, with a configurable lag order and significance level, and view F-statistic and p-value details.
 - **Causal network visualization:** See metrics as an interactive network, with edge strength reflecting correlation and directional arrows for causal relationships.
 - **Insights tab:** Automatic summaries including the strongest correlations, category and strength breakdowns, method agreement, leading indicators, and recommendations. You can add an alert for a correlated metric directly from an insight.
 - **Smart data mode selection:** EDM recommends live data or a summary level (for example 10-minute or 30-minute summaries) based on the selected time range, and warns when a finer resolution than recommended is chosen.
- ◆ **Metric Definitions now stored in the AdminDB**
Metric definitions referenced by the Explain Metric feature are now stored in the AdminDB. A future release will allow users to enter site-specific metric and expression definitions.

- ◆ **New web monitoring default report templates for Windows systems**

EDM will now be installed with new default charts, templates, and expressions for Windows IIS throughput monitoring.

- ◆ **Expanded Generate CSR screen for enterprise certificate requests (ticket #27521)**

The **Generate CSR** screen has been expanded to capture the full set of fields required by enterprise and government certificate authorities. You can now produce a CSR directly in EDM that meets stricter issuing-authority requirements, instead of falling back to external tools such as the Windows MMC Certificates snap-in or keytool. The screen now supports:

- **Subject fields:** Common Name, Organization, Organizational Unit, Locality, State, Country, and Email
- **Subject Alternative Name (SAN):** multiple DNS entries plus one or more IP entries, enabling certificate-based access by hostname or IP
- **Key Usage:** Digital Signature and Key Encipherment
- **Extended Key Usage:** Server Authentication and Client Authentication
- **Private key options:** selectable key size (2048 supported), selectable hash algorithm (SHA-256 supported), and a "Make private key exportable" option
- **Output:** user-specified CSR filename in Base64 format.

The generated keypair works with EDM's existing certificate import and SSL configuration flow.

- ◆ **Support for outbound SNMP v2C / v3 traps (tickets #27499)**

EDM can now send SNMP traps using SNMP v3, in addition to the existing v1 and v2c support. This lets you forward EDM alerts to receivers that require SNMP v3 security, such as Moogsoft and other monitoring or ticketing platforms. When configuring a trap destination, you can now choose the SNMP version (v1, v2c, or v3). For v3, you set the security level (noAuthNoPriv, authNoPriv, or authPriv) and the associated credentials in one place per destination:

- **Authentication protocol:** SHA-512, SHA-384, SHA-256, SHA-224, SHA-1, or MD5
- **Privacy protocol:** AES-256, AES-192, AES-128, 3DES, or DES
- **Security name and passphrases** for authentication and privacy
- **Engine ID** can be entered manually or left blank for automatic discovery at send time

v3 credentials are defined per trap destination, so alert definitions that use that destination automatically send with the correct security settings. SNMP v3 traps are sent for both manual test traps and live alert events, including alert-cleared notifications.

SNMPv1 trap destinations now send the configured community string; previously v1 traps were sent with an empty community and were silently dropped by receivers that enforce community authorization. The Test Trap action now reports a result for every SNMP version.

- ◆ **SNMPv3 multi-device reliability**

`snmp_v3.properties` now accepts an optional 6th column with the device's authoritative engine ID. Adds polling USM isolation and per-device trap engine ID handling.

- ◆ **Consistent SNMP metric set across v1/v2c/v3**

The SNMP collector now recognizes and categorizes error responses, so v1, v2c, and v3 connections report the same metric set. Connections with bad credentials now fail instead of falsely showing as connected.

-
- ◆ **Sightline MIB and SNMP_v1.properties configuration corrected (ticket #27516)**
The enterprise OID in the Sightline MIB configuration has been updated. In addition, the `snmp_v1.properties` file was being overwritten on each DCS startup; this has been corrected.

Changes

- ◆ **WildFly upgraded to 39.0.1**
Wildfly has been upgraded from 37.0.1 to 39.0.1. EDM upgrade scripts will handle migration to the new version in existing installs.
- ◆ **PostgreSQL upgrade to 18.4**
PostgreSQL has been upgraded to address reported CVEs.
- ◆ **SightlineDB upgrade to InfluxDB 1.7.x to 2.8**
SightlineDB is being upgraded from InfluxDB 1.7 to version 2.8. The EDM upgrade scripts will handle migration to the new version in existing installs. This upgrade includes data-integrity validation, rollback testing, and performance benchmarking.
- ◆ **Log4j upgraded to 2.25.4**
EDM 7.2 includes an upgrade of log4j from 2.25.3 to 2.25.4 to address CVE-2026-34478 and CVE-2026-34480.
- ◆ **Installer script is now digitally signed**
The EDM installer script is now code-signed for improved security and trust verification.
- ◆ **Auto-rescue SSL state on 7.0 / 7.1 → 7.2 upgrade**
SSL configuration is automatically repaired after upgrading. Customers running SSL on 7.1.1 must log in and navigate to **System Settings** once after upgrading to trigger the fix.
- ◆ **Alert-email URL stays in sync with SSL config on upgrade**
On upgrade to 7.2, the **URL in alert email** field in **System Settings** is cleared so the alert-email URL stays in sync with the active SSL configuration. Customers using a customized URL should re-enter it after upgrading.
- ◆ **General SSL / HTTPS hardening based on internal testing**
Multiple updates have been made to enhance and harden general SSL configuration, including certificate import, UI feedback, DCS path handling, CSR workflow, full-chain certificate storage, country-code validation, and upgrade migration.
- ◆ **AutoDiscoverTLC DNS resolution options**
Optional DCS `config.properties` settings for host discovery have been added. `discover.dns.suffixes` is a comma-separated list of DNS suffixes appended to short names (for example, `sightline.local`); this list is empty by default, so it must be set to the site's DNS domain to take effect. `discover.dns.required` defaults to true (strict DNS-only resolution); set it to false to fall back to the OS resolver for names DNS cannot resolve. The fallback is opt-in because the OS resolver may use NetBIOS or LLMNR.
- ◆ **Scheduled-report PDF timeout is now configurable**
Scheduled and on-demand reports failed intermittently with a Playwrite error, and logs indicated that Playwrite was exceeding its default 30-second timeout while waiting for the report to

render. This has been corrected by extending the default timeout to 5 minutes and adding the `headless.browser.timeout.ms` configuration entry to EDM's `config.properties` file.

- ◆ **Access URL in SSL Configuration corrected (tickets #27518, 27519)**
After manually configuring SSL and then upgrading to EDM 7.1.1, the URL displayed in **Settings > System Settings > SSL Configuration** was incorrect. In addition, the Disable HTTPS button produced an error. These have been corrected.
- ◆ **SSL Management Port socket-binding issue resolved (ticket #27500)**
After manually configuring SSL and then upgrading to EDM 7.1.1, the Sightline EDM service would start then stop after a few seconds, because the upgrade introduced duplicate socket bindings in the `standalone-full.xml` configuration file. This has been corrected.
- ◆ **Connections “start, collect, then stop” issue resolved (ticket #27517)**
After upgrading to EDM 7.1.1, connections to some systems did not stay active. Investigation revealed that DCS's data parser did not catch all malformed numeric value patterns in some ClearPath OS 2200 connections. This has been corrected.
- ◆ **Artifacts from Assure can now be deleted from EDM (ticket #27347)**
After deleting alert groups and other artifacts, they reappeared when EDM was restarted. This has been corrected.
- ◆ **DCS service now stays running after upgrade**
After upgrading to EDM 7.1.1 the DCS service did not stay active, due to an incorrect file path in NSSM. This has been corrected.

Known Issues in EDM 7.2

- ◆ **Wildfly error “Address already in use” when upgrading with management port disabled**
Before upgrading EDM on a system with the management port disabled, do not rely on the Services console to stop the EDM service (this triggers the same failed shutdown). Stop EDM in a way releases the ports - a graceful CLI shutdown against the management port that IS open, or stop the service and then confirm that ports 443/3528 are free (end any lingering EDM Java process). Then start the upgrade.
- ◆ **Upgrade boot-safety guard for HTTPS-only configurations**
On servers where the standard HTTP listener's socket binding had been removed or commented out (for example, HTTPS-only or locked-down deployments) but was still referenced elsewhere in the configuration, upgrading to 7.2 could leave the server unable to start, with a WFLYCTL0362 "required capabilities are not available" error in `server.log`. The installer now detects this during the upgrade and automatically restores the missing socket binding, so these servers start normally. No customer action is required. The restored binding does not open any additional port - if the HTTP listener was disabled, it stays disabled - so it does not weaken an HTTPS-only setup.
- ◆ **Alert-email URL stays in sync with SSL config on upgrade**
On upgrade to 7.2, the **URL in alert email** field in **System Settings** is cleared so the alert-email URL stays in sync with the active SSL configuration. Customers using a customized URL should re-enter it after upgrading.

EDM 7.1.1 Installation notes

Before upgrading to EDM 7.1.1, confirm that your current version is EDM 7.0 or EDM 7.1. Upgrades from versions prior to EDM 7.0 are not supported. See *EDM 7.1 Installation notes* below for more details about installing EDM 7.1.x.

EDM 7.1 Installation notes

Before upgrading to EDM 7.1, confirm that your current version is EDM 7.0. Upgrades from versions prior to EDM 7.0 are not supported.

Sightline EDM 7.1 features only two installation kits, one for Windows systems and one for Linux systems. The install/upgrade script provides choices to either install the defaults or customize, and to upgrade both default and custom installations. Begin the installation and respond to the prompts; the scripts will proceed with the install or upgrade as indicated.

The Sightline EDM installer script supports:

- **Custom or default install mode** (`edm install` or `edm install custom`) – select which components to install, change ports, paths, use an external DB instead of bundled PostgreSQL
- **EDM upgrade** (`edm upgrade`) – detects current versions, upgrades components as needed, and preserves data and configuration
- **Detection** (`edm detect`) – scans the system and reports what's installed with health status, works regardless of how components were originally installed
- **Rollback on failure** – if a step fails mid-install, completed steps are undone automatically
- **Manifest tracking** (`sightline-manifest.json` in the install base directory) — records what was installed and where, verified against real system state on every run
- **Per-component upgrade** — detects each component's version independently, only upgrades what's needed
- **Force re-deploy** (`edm upgrade --force`) — re-deploy EDM and DCS JARs even when version hasn't changed
- **Safe password handling** — special characters (' , \$, ! , etc.) work correctly
- **Modular architecture** — each component is its own module (Java, PostgreSQL, WildFly, EDM, DCS, Power Agent, SightlineDB, Chrome, OPC, Firewall)

Installing or upgrading Sightline EDM on Windows Systems

The following commands can be used with the EDM install script on Windows systems:

```
edm.bat install
edm.bat install custom
edm.bat install opc
edm.bat upgrade
edm.bat upgrade --force
```

```
edm.bat uninstall
edm.bat detect
edm.bat help
```

The install/upgrade log is located at:

```
%TEMP%\sightline-installer\
```

Installing or upgrading Sightline EDM on Linux Systems

The following commands can be used with the EDM install script on Linux systems:

```
sh edm.sh install
sh edm.sh install custom
sh edm.sh install opc
sh edm.sh upgrade
sh edm.sh upgrade --force
sh edm.sh uninstall
sh edm.sh detect
sh edm.sh help
```

The install/upgrade log is located at:

```
/tmp/sightline-installer/
```

EDM 7.0 Installation notes

We recommend using the 1-click installation option for fresh installs of EDM 7.0. This will install Java 21, Wildfly 37.0.1.Final, Chromium, PostgreSQL 18.1, EDM and DCS. If a manual installation is required at your site, please contact Sightline Technical Support for assistance.

Upgrade notes

Before upgrading to EDM 7.0, confirm that your current version is EDM 6.0.x. Upgrades from version prior to EDM 6.0.0 are not supported.

Site-specific configuration settings for SSL, blocking ports (8080 and/or 9990), or updated Java memory settings will not be preserved when upgrading to EDM 7.0. These settings will need to be reconfigured after the upgrade is complete. See the *Sightline Enterprise Data Manager User's Guide* for configuration details.

Upgrade notes for 1-click upgrades

During the 1-click upgrade process a password for the Admin Database will be requested. Enter the current password or select a new password. Alternately, you can ask the installer to generate a random password. Passwords will be encrypted and then saved to EDM's configuration files.

Upgrade notes for manual upgrades

Sightline EDM 7.0 requires Java 21. For sites that perform manual upgrades, Java 21 *must* be installed before the upgrade, and the JAVA_HOME environment variable updated to point to the new Java version. Not installing Java 21 will cause the EDM upgrade to fail.

Sightline EDM 7.0 requires Wildfly 37.0.1.Final. For sites that perform manual upgrades, Wildfly 37.0.1.Final *must* be installed before the upgrade, and the JBOSS_HOME environment variable updated to point to the new Wildfly version. During the installation process, the locations of the old and new Wildfly directories will be requested. Not using Wildfly 37.0.1.Final will cause the EDM upgrade to fail.

Sightline EDM 7.0 requires Chromium to support scheduled reports and dashboards. When installing Wildfly 37.0.1.Final, you must also unzip `chrome-win.zip` into the `\wildfly-37.0.1.Final\bin\chrome-win\` directory.