

## **Entire Connection**

### **Release Notes**

Version 9.1.3

October 2021

This document applies to Entire Connection Version 9.1.3 and all subsequent releases.

Specifications contained herein are subject to change and these changes will be reported in subsequent release notes or new editions.

Copyright © 1984-2021 Software AG, Darmstadt, Germany and/or Software AG USA, Inc., Reston, VA, USA, and/or its subsidiaries and/or its affiliates and/or their licensors.

The name Software AG and all Software AG product names are either trademarks or registered trademarks of Software AG and/or Software AG USA, Inc. and/or its subsidiaries and/or its affiliates and/or their licensors. Other company and product names mentioned herein may be trademarks of their respective owners.

Detailed information on trademarks and patents owned by Software AG and/or its subsidiaries is located at <http://softwareag.com/licenses>.

Use of this software is subject to adherence to Software AG's licensing conditions and terms. These terms are part of the product documentation, located at <http://softwareag.com/licenses/> and/or in the root installation directory of the licensed product(s).

This software may include portions of third-party products. For third-party copyright notices, license terms, additional rights or restrictions, please refer to "License Texts, Copyright Notices and Disclaimers of Third-Party Products". For certain specific third-party license restrictions, please refer to section E of the Legal Notices available under "License Terms and Conditions for Use of Software AG Products / Copyright and Trademark Notices of Software AG Products". These documents are part of the product documentation, located at <http://softwareag.com/licenses> and/or in the root installation directory of the licensed product(s).

Use, reproduction, transfer, publication or disclosure is prohibited except as specifically provided for in your License Agreement with Software AG.

**Document ID: PCC-RELNOTES-913-20210929**

## Table of Contents

|  |   |
|--|---|
| 1 About this Documentation .....               | 1 |
| Document Conventions .....                     | 2 |
| Online Information and Support .....           | 2 |
| Data Protection .....                          | 3 |
| 2 Release Notes .....                          | 5 |
| Supported Operating Systems .....              | 6 |
| Compiler Used to Build Entire Connection ..... | 6 |
| Important Notes .....                          | 6 |



# 1 About this Documentation

---

- Document Conventions ..... 2
- Online Information and Support ..... 2
- Data Protection ..... 3

## Document Conventions

---

| Convention     | Description  |
|----------------|--|
| <b>Bold</b>    | Identifies elements on a screen.   |
| Monospace font | Identifies service names and locations in the format <i>folder.subfolder.service</i> , APIs, Java classes, methods, properties.  |
| <i>Italic</i>  | Identifies:<br><br>Variables for which you must supply values specific to your own situation or environment.<br>New terms the first time they occur in the text.<br>References to other documentation sources. |
| Monospace font | Identifies:<br><br>Text you must type in.<br>Messages displayed by the system.<br>Program code.  |
| { }            | Indicates a set of choices from which you must choose one. Type only the information inside the curly braces. Do not type the { } symbols.   |
|                | Separates two mutually exclusive choices in a syntax line. Type one of these choices. Do not type the   symbol.  |
| [ ]            | Indicates one or more options. Type only the information inside the square brackets. Do not type the [ ] symbols.  |
| ...            | Indicates that you can type multiple options of the same type. Type only the information. Do not type the ellipsis (...).  |

## Online Information and Support

---

### Software AG Documentation Website

You can find documentation on the Software AG Documentation website at <https://documentation.softwareag.com>.

### Software AG Empower Product Support Website

If you do not yet have an account for Empower, send an email to [empower@softwareag.com](mailto:empower@softwareag.com) with your name, company, and company email address and request an account.

Once you have an account, you can open Support Incidents online via the eService section of Empower at <https://empower.softwareag.com/>.

You can find product information on the Software AG Empower Product Support website at <https://empower.softwareag.com>.

To submit feature/enhancement requests, get information about product availability, and download products, go to [Products](#).

To get information about fixes and to read early warnings, technical papers, and knowledge base articles, go to the [Knowledge Center](#).

If you have any questions, you can find a local or toll-free number for your country in our Global Support Contact Directory at [https://empower.softwareag.com/public\\_directory.aspx](https://empower.softwareag.com/public_directory.aspx) and give us a call.

### **Software AG Tech Community**

You can find documentation and other technical information on the Software AG Tech Community website at <https://techcommunity.softwareag.com>. You can:

- Access product documentation, if you have Tech Community credentials. If you do not, you will need to register and specify "Documentation" as an area of interest.
- Access articles, code samples, demos, and tutorials.
- Use the online discussion forums, moderated by Software AG professionals, to ask questions, discuss best practices, and learn how other customers are using Software AG technology.
- Link to external websites that discuss open standards and web technology.

## **Data Protection**

---

Software AG products provide functionality with respect to processing of personal data according to the EU General Data Protection Regulation (GDPR). Where applicable, appropriate steps are documented in the respective administration documentation.

---

# 2 Release Notes

---

- Supported Operating Systems ..... 6
- Compiler Used to Build Entire Connection ..... 6
- Important Notes ..... 6

This document describes the new features, changes and enhancements for Entire Connection Version 9.1.3. This is the successor of Entire Connection Version 9.1.2.

## Supported Operating Systems

---

Entire Connection supports the following 64-bit operating system platforms:

- Microsoft Windows 8
- Microsoft Windows 10
- Microsoft Windows Server 2012
- Microsoft Windows Server 2016
- Microsoft Windows Server 2019

Make sure the machine on which you are going to run the installer contains the latest Windows updates before you start the installation. On Windows server 2012 R2, the installation will fail if the Microsoft update KB2919355 is missing.

Home editions of Microsoft Windows are not supported.

The runtime components of Entire Connection are always 32-bit applications, even on 64-bit platforms.

For further information, see *Prerequisites* in the *Installation* section.

## Compiler Used to Build Entire Connection

---

Entire Connection was built and tested with the following compiler:

- Microsoft Visual Studio 2017

## Important Notes

---

- To address vulnerabilities of previous OpenSSL/TLS versions this release of Entire Connection includes OpenSSL/TLS 1.1.1g.
- To address vulnerabilities of previous SSH2 versions this release of Entire Connection includes libssh2 1.8.2.

This vulnerability has been rated as having a security impact of Moderate. After evaluation and in accordance with the criteria noted in the product support life cycle, there are no plans to address this issue in an upcoming release.

- CVE-2019-13115: A vulnerability was discovered in libssh2 versions before 1.9.0.

In libssh2 before 1.9.0, `kex_method_diffie_hellman_group_exchange_sha256_key_exchange` in `kex.c` has an integer overflow that could lead to an out-of-bounds read in the way packets are read from the server. A remote attacker who compromises a SSH server may be able to disclose sensitive information or cause a denial of service condition on the client system when a user connects to the server. This is related to a `_libssh2_check_length` mistake, and is different from the various issues fixed in 1.8.1, such as CVE-2019-3855.

For more details see <https://nvd.nist.gov/vuln/detail/CVE-2019-13115#vulnCurrentDescription-Title>

This vulnerability has been rated as having a security impact of Moderate and will not be addressed in the current version of Entire Connection.

- To address vulnerabilities of previous ICU versions this release of Entire Connection includes ICU 63.2.0.0.

