



Micro Focus Visual COBOL 10.0 for Visual Studio

Release Notes

Micro Focus
The Lawn
22-30 Old Bath Road
Newbury, Berkshire RG14 1QN
UK
<http://www.microfocus.com>

© Copyright 2024 Micro Focus or one of its affiliates.

MICRO FOCUS, the Micro Focus logo and Visual COBOL are trademarks or registered trademarks of Micro Focus or one of its affiliates.

All other marks are the property of their respective owners.

2024-06-26

Contents

Visual COBOL 10.0 for Visual Studio Release Notes	4
What's New	5
Rocket COBOL and Enterprise Extensions for Visual Studio Code	5
.NET Support	6
COBOL Language	6
Code Analysis and a Natural Language Analysis Assistant	6
Compiler Directives	7
Customer Experience Improvement Program	7
Database Connectors	7
Enterprise Server	7
Enterprise Server Common Web Administration (ESCWA)	7
Enterprise Server Security	8
Interface Mapping Toolkit	9
Licensing Changes	9
Micro Focus Unit Testing Framework	9
Visual Studio Integration	9
Significant Changes in Behavior or Usage	10
Known Issues	15
Resolved Issues	16
Other Issues Resolved in This Release	40
Unsupported or Deprecated Functionality	41
Additional Software Requirements	42
Installation	43
Before Installing	43
Downloading the Product	43
On Windows	43
Basic Installation	46
Installing	46
Advanced Installation Tasks	47
On Windows	47
After Installing	50
On Windows	50
Licensing Information	57
To activate Visual COBOL Personal Edition	57
To buy and activate a full unlimited license	57
To start Micro Focus License Administration	57
Installing licenses	58
Applying your license file	58
If you have an authorization code	59
To obtain more licenses	60
Updates and OpenText Support for Micro Focus Products	61
Further Information and OpenText Support for Micro Focus Products	61
Information We Need	62
Creating Debug Files	62
Copyright and Disclaimer	63

Visual COBOL 10.0 for Visual Studio Release Notes

These release notes contain information that might not appear in the Help. Read them in their entirety before you install the product.



Note:

- This document contains a number of links to external Web sites. Micro Focus cannot be responsible for the contents of the Web site or for the contents of any site to which it might link. Web sites by their nature can change very rapidly and although we try to keep our links up-to-date, we cannot guarantee that they will always work as expected.
- Check the *Product Documentation* section of the [OpenText Support and Services Documentation Web site for Micro Focus products](#) for any documentation updates.

Product Overview

Visual COBOL enables you to develop COBOL applications within Microsoft Visual Studio. You use the Visual Studio integrated development environment (IDE) to edit, compile and debug COBOL applications. The IDE provides all the functionality to manage projects and build applications.

The product is available in the following variants - Visual COBOL for Visual Studio 2022. The execution environment for applications created with any of these product variants is COBOL Server.

Upgrading from earlier Micro Focus products

This version of your product is dependent on a later version of the Microsoft C run-time system than earlier Micro Focus products. This means that COBOL executables (.exe) built with a version earlier than 4.0 might not be compatible with the current version of the run-time products. If the behavior of your application changes with the current version, we strongly recommend that you relink the main executable with the current version. This will ensure that the COBOL run-time system fully handles any run-time error conditions that might occur.

A new executable that is fully compatible with the current version can be produced without recompiling the application, as long as the original object code is available and it is relinked with the current version.

To allow your executables to benefit from the product's latest programming and performance enhancements, we recommend a full recompilation of your source code.

If you are using Visual Studio, you can configure the IDE to automatically check whether applications created with older releases must be relinked. If the application uses an older version of the C run-time system, Visual COBOL can automatically relink the existing executable or .dll to the new version of the C run-time system without the need to recompile the application first. If a project needs relinking, Visual Studio displays a message in the status bar providing an option for you to choose and relink the project.

What's New

Enhancements are available in the following areas:

- [Rocket COBOL Extensions for Visual Studio Code](#)
- [.NET Support](#)
- [COBOL Language](#)
- [Code Analysis and a Natural Language Assistant](#)
- [Compiler Directives](#)
- [Customer Experience Improvement Program](#)
- [Database Connectors](#)
- [Enterprise Server](#)
- [Enterprise Server Common Web Administration \(ESCWA\)](#)
- [Enterprise Server Security](#)
- [Interface Mapping Toolkit](#)
- [Licensing Changes](#)
- [Micro Focus Unit Testing Framework](#)
- [Visual Studio Integration](#)

Rocket COBOL and Enterprise Extensions for Visual Studio Code

[Back to Top](#)

The Micro Focus COBOL and Enterprise extensions for Visual Studio Code have been repackaged by Rocket Software on the Microsoft Visual Studio Marketplace.

- The Rocket COBOL extension for Visual Studio Code (formerly Micro Focus COBOL Extension for Visual Studio Code) provides COBOL edit, compile and debug support for Visual COBOL and Enterprise Developer users in Visual Studio Code.
- The Rocket Enterprise extension for Visual Studio Code (formerly Micro Focus Enterprise extension for Visual Studio Code) provides PL/I edit, compile and debug support for Enterprise Developer users in Visual Studio Code. This extension installs the Rocket COBOL extension.
- The Rocket JVM COBOL extension for Visual Studio Code (formerly Micro Focus JVM COBOL extension for Visual Studio Code) provides support for debugging JVM COBOL code in Visual Studio Code.
- The Learn COBOL extension for Visual Studio Code provides all training materials for the Micro Focus COBOL Fundamentals Training course.

New enhancements in this release are:

- Support for accepting command-line arguments in COBOL notebooks.
- New debug launch options - console and integrated Terminal support for platform specific values in the `launch.json` file.
- Support is available for fine-tuning the colors of different parts of the code in the editor via Visual Studio Code's `settings.json` file. This requires a minimum release 10.0 of Visual COBOL.



Note: These extensions are not included with the Visual COBOL installer. They are available from the Microsoft Visual Studio Marketplace website. All of the extensions are available on Windows and Linux.

.NET Support

[Back to Top](#)

This release provides the following enhancements to .NET support:

- .NET COBOL projects now target .NET 8. Earlier versions of .NET are not supported. Support for building .NET Framework 4.x COBOL projects using Visual Studio remains unchanged.

COBOL Language

[Back to Top](#)

This release includes the following enhancements:

- The **FREE** statement - under the MF dialect, you can now free memory, allocated via the ALLOCATE statement, directly by using `FREE ADDRESS OF data-name`. This negates the need to specify a returning pointer during allocation (i.e. `ALLOCATE data-name RETURNING my-pointer`) and then freeing the pointer.
- **COBOL/Java interoperability** - the following features have been added to the COBOL and Java interoperability for native COBOL code:
 - Support for the use of dynamic length COBOL items when running under an MF dialect. See *Mapping COBOL Items and Java Types*.
 - User-defined exception handling when calling Java static methods. See *Example 5 - Exception Reporting When Calling Java Static Methods*.
- The **entry_point_mapper_disable_auto_aliasing** run-time tunable - this new tunable has been introduced to determine whether the Entry Point Mapping facility should *not* emulate the alias function of an IBM mainframe linkage editor, and instead generate a COBRT173 Called program file not found in drive/directory run-time system error.
- **Enterprise COBOL support** - the following enhancements provide greater compatibility with IBM Enterprise COBOL version 6.4:
 - The STRING and UNSTRING statements now support USAGE UTF-8 data items.
 - The ENCODING phrase of the JSON-GENERATE and JSON-PARSE statements is now supported.
 - The ENTRY-NAME and ENTRY-INTERFACE clauses of the Function-ID paragraph are now supported; however, these clauses are strictly documentary.
- **New MF Level** - this release includes a new default level (MF"23") of reserved words. See *Reserved Words Table* for words associated with this level.
- **Pointer dereferencing** - improvements have been made in the ability to dereference pointers using both the DATA...AT and :: (colon-colon) syntax. See *Pointer Dereferencing*.

Code Analysis and a Natural Language Analysis Assistant

[Back to Top](#)

This release includes the following enhancements related to integration with COBOL Analyzer and Enterprise Analyzer:

- Natural Language Analysis Assistant in the IDE - integration with COBOL Analyzer and Enterprise Analyzer now provides a natural language **Analysis Assistant** chat window in the IDE. You can type queries about a COBOL workspace in a COBOL Analyzer or an Enterprise Analyzer repository. From the Analysis Assistant window results you can open Program Flow Graphs, view Complexity Reports, and open COBOL source files.



Note: This functionality requires a licensed copy of either COBOL Analyzer 10.0 or Enterprise Analyzer 10.0.

Compiler Directives

[Back to Top](#)

The following Compiler directive is new in this release:

- **ILPOINTER-REFERENCE** - Determines how a pointer used as a method parameter is passed if BY VALUE or BY REFERENCE is not specified as part of the parameter.

Customer Experience Improvement Program

[Back to Top](#)

Starting this release, the Customer Experience Improvement Program collects high-level, anonymous information on how Micro Focus products are used. The information collected includes product name and version, OS in use, and features used with the purpose to improve the products and, consequently, the customer experience.

Customer Experience Improvement Program participation is enabled by default. You can opt out with the help of the `mfceipconfig` command-line utility.

Database Connectors

[Back to Top](#)

- The CARRIAGE-CONTROL-FILTER XFD directive - enables carriage control characters to be retained when AcuXDBC reads a LINE SEQUENTIAL data file.

Enterprise Server

[Back to Top](#)

This release provides the following enhancements:

- Remote File Access - it is now possible to remotely access files using a configured Remote File Access (RFA) MFCS Connector. You can access ordinary files, cataloged datasets, and spool output. This also enables remote editing of COBOL data files using the new Data Tools utility. This enables you to download and upload files, datasets, and spool output locally or remotely using the existing Enterprise Server Security configuration. Various security features make this solution a more secure alternative to more generic solutions such as FTP and SSH.

Enterprise Server Common Web Administration (ESCWA)

[Back to Top](#)

This release includes the following enhancements:

- Catalog view has improved filtering options and now includes paging. A new **Load on navigation** check box enables you to filter based on the previously selected conditions. See *Catalog List* in the product Help.

- A new Configuration Report page enables you to visualize potential security vulnerabilities in the ESCWA and MFDS configurations. Each domain and configuration attribute combination has its own help dialog. See *Configuration Report* in the product Help.
- Role-based security configuration. You can now configure a users view of ESCWA. If a user does not require specific roles then you can hide corresponding pages and API. You can configure the role-based access from the **Role Options** page. Click **Security** , expand **ESCWA Configuration** followed by the ESM, and then click **Roles**. See *Role Options* in the product Help.



Note: Role-based security is an ESCWA only feature that works on top of existing product security.

- It is now possible to remove Locks, if necessary, to fix applications that are broken due to a lock that has not been removed. You can enable this feature from the **Locks** page. Click **Native > Monitor > Locks**, and then click **Remove Locks**. This functionality is controlled by the casstop resource entity in the OPERCMDS resource class. See *Locks* in the product Help.



Caution: Incorrectly removing locks can result in system instability and corruption or loss of data.

- Region verification - ESCWA can now verify the configuration of selected components for an enterprise server region. You can use this feature to identify potential start up or configuration issues for the selected region. The verification process uses the casverify utility to perform the verification action. See *Verify* in the product Help.
- Improved CICS resource navigation. Active resources can now be filtered by group and large sets of filtered data can be paged.
- The API return codes have been improved. Previously, when the region monitor and control APIs were called, they would return a HTTP 200 code, with the error specified in the JSON output. The return codes have been improved to give more information. You can configure the API to use the new or old behavior.
- The ESCWA user interface is now more responsive and can be used with a greater variety of smaller Web browsers.

Enterprise Server Security

[Back to Top](#)

This release includes the following enhancements:

- Enterprise Server security features provided by the VSAM External Security Manager (ESM) module are enabled by default. You will need to supply valid credentials when you interact with ESCWA, the Micro Focus Directory Server and regions in the browser based UI or in the IDE, use certain utilities from the command line, use TN3270 emulator to access regions, log into or with FileShare. See *After Installing > Enterprise Server Security Features* for details on how to configure this product.
- TLS Certificate Checking Utility - a new executable in the product that can be used to help diagnose problems with TLS certificates. It can check the validity of certificates, verify certificate chains, check that certificates and private keys match and check that a certificate contains a SAN that matches a provided hostname/address. Improves TLS usability by diagnosing TLS certificate problems. See *CertChecker Utility* for more information.
- The VSAM ESM Module, which provides file-based security for Enterprise Server is now a GA quality.
 - User authentication and resource authorization control can be enabled through a simple file-based security mechanism.
 - Security data can be imported from YAML or LDIF and exported to YAML for portability and ease of editing / scripting.
- Additional optional security features are available for HTTP and MFBINP conversations, for the Web Services and J2EE, Web, and Remote File Access conversation types. Listeners can be configured to require user authentication and/or to restrict access to specific types of requests. See *Enhanced Security for HTTP and MFBINP* for more information.

Interface Mapping Toolkit

[Back to Top](#)


This release provides the following enhancement:

- The `imtkmake -defmap` command now support the following new parameters that enhance the default mapping support for service interfaces - endpoint, method, and path.

Licensing Changes

[Back to Top](#)

- The SafeNet Sentinel licensing system that was available with previous releases of this product has been deprecated and is no longer available in release 10.0. This product also uses the Micro Focus AutoPass licensing technology which was introduced in release 8.0. Starting with release 10.0, AutoPass is the only licensing technology available in this product.
- The SafeNet Sentinel licenses are no longer supported, and you need to use AutoPass licenses starting with release 10.0. Contact your account manager to replace your existing SafeNet Sentinel with AutoPass licenses.

 **Note:** Installing 10.0 on a machine where there are other Micro Focus products or versions installed that use SafeNet Sentinel licensing might result in some compatibility issues. While the 10.0 installation process has been designed to address such issues, you should be aware of the following scenarios and if any action might be required to ensure licensing works as expected. See *Advanced Installation Tasks > Licensing Coexistence when Upgrading to Release 10.0* in the *Installation* section.

Micro Focus Unit Testing Framework

[Back to Top](#)

This release includes the following enhancement:

- A new configuration file format has been introduced that enables you to use environment variables in your unit test code for tests that are compiled for more than one scenario. A portable environment file can provide environment variables for a test case that has been compiled in multiple ways (for Windows/UNIX, 32-bit/64-bit, etc...). See *Configuring the Run-Time System Environment* in your product Help.

Visual Studio Integration

[Back to Top](#)

This release provides the following enhancements:

- Colorization of items in the editor - there are now more COBOL items that you can configure the editor colors for from **Tools > Options > Environment > Fonts and Colors**.
- Server Explorer enhancements - you can now connect to a remote ESCWA, and add remote Directory Servers to the ESCWA opened in Server Explorer.

Significant Changes in Behavior or Usage

This section describes significant changes in behavior or usage. These changes could potentially affect the behavior of existing applications or impact the way the tools are used.

- [Licensing Changes](#)
- [Significant Changes in Behavior or Usage - Enhancements](#)
- [Significant Changes in Behavior or Usage - Fixes](#)

Licensing Changes

[Back to the list](#)

- With release 10.0, the SafeNet Sentinel licensing technology has been deprecated. This can result in some compatibility issues if you install 10.0 on a machine where there are other Micro Focus products or versions installed that use SafeNet Sentinel licensing. While the 10.0 installation process has been designed to address such issues, you should be aware of the following scenarios and if any action might be required to ensure licensing works as expected. See *Advanced Installation Tasks > Licensing Coexistence when Upgrading to Release 10.0* in the *Installation* section.

Significant Changes in Behavior or Usage - Enhancements

[Back to the list](#)

The numbers that follow each issue are the Support Case Numbers followed by the Issue number (in parentheses).

- [Data Tools](#)
- [Enterprise Server](#)

Enterprise Server

[Back to the list](#)

- Enterprise Server's PAM ESM Module now has a group-filter option that can be used to ignore all user groups that do not matching a specified pattern. See *PAM ESM Module Custom Configuration Information* in your product Help for more information.
3176983 (12500)
 - In ESCWA, the **Enable Single Sign-On for Unsecured Resources** has been renamed to **Single Sign-On Behavior** which has three options:
 - **Disabled** - This disables all single sign-on including live enterprise server regions.
 - **Only Secure and Loopback** - This is the old 'default' behavior, single sign-on will be enabled for secured and localhost resources.
 - **Allow Insecure (All)** - Single sign-on will be enabled for everything. This list controls two boolean configuration attributes specified in the `commonwebadmin.json` file:
 - **InsecureAutoSignOn** - this is an existing attribute.
 - **DisableAutoSignOn** - this is a new attribute, if this is set to true then **InsecureAutoSignOn** will have no effect and all single sign-on will be disabled. If set to false then **InsecureAutoSignOn** will operate as before.
- 02663941 (658042)
- In ESCWA, you can now set table column defaults for users. This can be configured from the column filtering option of the table in ESCWA. If an administrator has not set table defaults then the table columns displayed will match the ESCWA defaults. You can specify which users are able to configure

default columns. This can be performed by modifying the **Table Column Configuration** security resource entity. See *Security Resources to Control ESCWA* and *API Access* in your product Help for more information.



Note: If **Table Column Configuration** is not specified then ESCWA will use the configuration specified for the **Common Web Administration** resource class.

02618280 (532051)

- The `casverify` utility has been improved with new functionality and additional verification stages. See *casverify* in your product Help for more information.



Note: The changes to its text and JSON output formats are incompatible with earlier versions.

(527008)

Significant Changes in Behavior or Usage - Fixes

[Back to the list](#)

The numbers that follow each issue are the Support Case Numbers followed by the Issue number (in parentheses).

- [Compiler](#)
- [Enterprise Server](#)
- [File Handling](#)
- [Interface Mapping Toolkit](#)
- [Micro Focus Directory Server](#)
- [Run-Time System](#)

Compiler

[Back to the list](#)

- The intrinsic function LENGTH and special register LENGTH OF were not always returning the correct result for PIC N NATIONAL fields. These have been updated to the correct behavior, namely returning the number of characters for the former and number of bytes for the latter. If your legacy code has been relying on the previously incorrect behavior, results might now differ.

(613039)

- Generated code only (excluding Intel x86 32-bit platforms): an error when moving from a COMP-6 item to another COMP-6 item when the SIGNFIXUP Compiler directive is specified has been fixed.

(665005)

Enterprise Server

[Back to the list](#)

- When running with TRANCLASS active, TD Queue transaction triggering was not working.

02737664 (629076)

- ASSIGN INVOKINGPROG did not behave correctly when a CALL was involved.

02662244 (543070)

- A DPL over a SYNCLEVEL2 connection could result in an XA start being driven out of sequence resulting in a protocol error.

02583717 (477027)

- In a TRANCLASS enabled enterprise server region with a high volume of XA transactions, the logging overhead could cause performance degradation. This has been improved.

02560536 (468059)

- The PAC compatibility checks that run at startup have now been relaxed. Consistent platform and bitism are still checked, but product version checks are no longer carried out. The ES_PAC_MIN_COMP_CHECK environment flag has now been deprecated.



Note: Enterprise Server will still carry out record compatibility checks during start up.

(19756)

- The statusCodes flag has been added to some ESCWA API endpoints which can be used to enable ESMAC to return appropriate HTTP error status codes instead of embedding failure messages in successful responses. In a future product release, the new behavior will be enabled by default in the version 2 of the API and the flag will be removed. The version 1 of the API will maintain the current behavior.

02601489 (506061)

- ESCWA now limits the session timeout to 20 days. If an existing configuration is greater than that it will be limited to that value.

(665130)

- In ESCWA, the **Listener Properties** page now limits user inputs when the **smem** protocol is selected. Multiple host names are not permitted, and port selection is also not permitted.



Note: API functionality remains the same.

(665044)

- Runaway timeout was intermittently incorrectly calculated.

02529887 (468050)

- The JSON output format for the `casverify` utility has changed. Messages specific to `casverify` itself are no longer identified by "msgout" but under a "messages" array.

(570009)

- For Enterprise Server application failure reports and storage dumps generated by runtime errors, the RTS error code is now taken into account during `es-dump-limit` (ES_DUMP_LIMIT) processing. Runtime errors with differing error codes will now be treated as distinct.

02660093 (561067)

- The **Allow no-password signon for default users** property has been added to the ESCWA **Advanced Region Properties** page. If this property is set to `false`, an explicit signon request with no password matching an enterprise server default user account will no longer be treated as a no-password verify, and will instead result in a not authenticated failure.

02728103 (625033)

- When no connection string is supplied through ESCWA/MFDS/esfadmin the `vsam_esm` module will default to `C:\ProgramData\Micro Focus\Enterprise Developer\es_esm_file_directory`. This directory will have been configured through running `mfseconv init`, which is called by the product installer in 10.0 and later.

(545065)

- The `es_default_security.yaml` file is now supplied with the product and is located at `%ProgramFiles(x86)%\Micro Focus\Enterprise Developer\etc` (Windows) or `$COBDIR/etc/vsam_esm` (UNIX). You can use this file as a template to configure the VSAM ESM Module. See the *VSAM ESM Module* topic in your product Help for more information.

(613052)

- Client connection to Micro Focus Directory Server (MFDS) would sometimes convert a fully qualified host name to just the simple host name. This could result in TLS connection issues if this did not exactly match the host names specified in the certificate.

02587914 (486048)

File Handling

[Back to the list](#)

- The Micro Focus file handler now passes correct information to the third-party file handlers for the implementation of the FS_RENAME_FILE routine.

02794472 (559042)

Interface Mapping Toolkit

[Back to the list](#)

- The base path is no longer part of the **Service name** field in the **Properties** dialog box of **REST Web service Deployment Server** tab. (It is only visible in the **Advanced Settings** of the service name.)

02795415 (651091)

Micro Focus Directory Server

[Back to the list](#)

- When starting or stopping an enterprise server region using MFDS or the ESCWA user interface, the `casstart` and `casstop /m` parameter would use the MFDS IP address rather than the host name, which could result in an issue if TLS certificates were used that required a particular host name.

02603383 (505074)

- An issue introduced Patch Update 1 resulted in ESCWA not listing all enterprise server regions for legacy import if they contained script data and the MF Directory Server was not sufficiently authorized to import script data.

(636060)

- The Micro Focus Directory Server (MFDS) **Start on System Start** enterprise server region option on the ESCWA General Properties page was not working because the **Automated Execution Control Enterprise Server Credentials** were not being applied correctly.

02795649 (652065)

- When exporting enterprise server regions registered in the MF Directory Server using XML format, regions for which the user did not have read/write access could also be exported.

(526005)

- Issues existed with importing enterprise server regions saved in JSON, XML, and Legacy format into a MF Directory Server, which resulted in incorrect listener states and counts.

(559058)

- You can now control the execution and update permission for an enterprise server region's start and stop, and on unrespondent scripts, by using a new LDAP Enterprise Server Administration security resource class **Scripts** entity. If this security resource entity has been specified with appropriate access control entries, the MFDS session will require Update permission in order for the authorized user to modify a region s script or to enable or disable it. In addition, for a script to execute, then you must specify Execute permission. See *Class - Enterprise Server Administration* in your product Help for more information.



Note: This is not a region restriction, but applies to the MFDS instance where the region is specified. If no security or MFDS Internal Security is configured for use then region scripts will not be executed nor will they be able to be modified. The Scripts resource is not a security resource created by default. It can be created by the ESCWA interface or other LDAP administration configuration tools.



Important: In future product versions, the access control that uses the Scripts security resource will be a requirement in order for any region s scripts to be executed or modified.

02822038 (499063)

- The default **UI Session Timeout** value for MF Directory Servers has changed from -1 (no timeout) to 600 seconds (10 minutes). The default value for the MF Directory Server **API Session Timeout** has been reduced from 3600 seconds (an hour) to 1200 seconds (20 minutes).
(628068)

Run-Time System

[Back to the list](#)

- The Java/COBOL application launcher - `cobjrun` - now supports Java command-line argument files. See <https://docs.oracle.com/en/java/javase/17/docs/specs/man/java.html#java-command-line-argument-files> for details on how these files should be constructed.
02744842 (636023)

Known Issues

Refer to the *Known Issues and Restrictions* topic in the *Product Information* section of your product Help.

In addition, note the following:

- .NET COBOL projects only support Windows and Linux OS. The **Create a new project** dialog box in Visual Studio, however, shows other platforms as supported.
- If, after installing the product for Visual Studio 2022, you cannot access the Micro Focus functionality, execute the following command from a Visual Studio command prompt:

```
devenv /updateconfiguration
```
- In Visual COBOL 4.0 and 5.0 in an extremely small and limited set of cases, an issue could occur with running .NET executables and .dll files, or JVM .class files, created with an earlier version of the product. This issue only occurred if:
 1. The application performs an IS NUMERIC condition test on a variable declared with USAGE NATIONAL.
 2. The application has been created with Visual COBOL 3.0 or earlier, then executed in Visual COBOL 4.0 or 5.0.

In these rare cases, the IS NUMERIC test could provide the wrong answer.

In order to resolve this issue, in Visual COBOL 6.0 and later, the .NET COBOL and JVM COBOL run-times reject any program using IS NUMERIC on a NATIONAL item which was compiled with a version 5.0 or earlier of the product. You receive a "missing method" exception. To resolve the issue, you need to recompile any programs that use this construct in the newer versions of Visual COBOL.

Programs that do not use NATIONAL data, or those that have been recompiled in Visual COBOL 6.0 or later are not affected.

Resolved Issues

This section describes resolved issues in this release that resulted in product enhancements, and those that resulted in product fixes.

- [Resolved Issues - Enhancements](#)
- [Resolved Issues - Fixes](#)

Resolved Issues - Enhancements

[Back to the list](#)

The numbers that follow each issue are the Support Incident Numbers followed by the Defect number (in parentheses).

- [Compiler](#)
- [Database Connectors](#)
- [Enterprise Server](#)
- [Interface Mapping Toolkit](#)
- [Micro Focus Common Client](#)
- [Micro Focus Cryptographic Library](#)

Compiler

[Back to the list](#)

- For the processing of XML GENERATE, JSON GENERATE, and JSON PARSE statements, data names with a leading # character are now treated as though the character was not present. This ensures valid XML and JSON documents are maintained.
(529106)
- Under the MF dialect, you can now use the FREE statement to directly free memory allocated via the ALLOCATE statement, by using FREE ADDRESS OF data-name. This negates the need to specify a returning pointer during allocation (i.e. ALLOCATE data-name RETURNING my-pointer) and then freeing the pointer.
(528109)

Database Connectors

[Back to the list](#)

- The new CARRIAGE-CONTROL-FILTER XFD directive provides the same functionality as the CARRIAGE_CONTROL_FILTER runtime configuration variable, allowing carriage control characters to be retained when AcuXDBC reads a LINE SEQUENTIAL data file. See *CARRIAGE-CONTROL-FILTER directive* in your product Help for details.
02669873 (557005)

Enterprise Server

[Back to the list](#)

- You can now archive the auxiliary trace file by setting the `archive_auxiliary_trace` property to true. You can set this property in the **Enterprise Server Common Web Administration (ESCWA)** interface on the **Advanced Region Properties** page. See *Auxiliary Trace* in your product Help for more information.

(425091)

- In ESCWA, validation has been added to file path inputs to ensure they do not contain leading or trailing white space characters.

02513150 (446067)

- Exporting an enterprise server region as a JSON file will now be formatted.

02818032 (510031)

- Two new audit event codes have been added, 5 10 and 2 21. See *Audit Event Codes* in your product Help for more information.

02809915 (658081)

- In ESCWA, the **Password Change Enabled** check box has been added to the **Security Settings** page. Checking this enables you to change a users password when they log on.

02589857 (498029)

- In ESCWA, a new **Active XA Resources** widget has been added to the dashboard. See *Dashboard* in your product Help for more information.

02621260 (517076)

- In ESCWA, you can now remove locks for enterprise server regions that are part of a Performance and Availability Cluster (PAC). You need to be able to stop an enterprise server region in order to remove locks. The OPERCMDS(CASSTOP) resource will be checked.



Caution: Incorrectly removing locks can result in system instability and corruption or loss of data. You can contact Micro Focus Customer Support for more information and guidance on removing locks.

02659029 02869605 (545043)

- The `casverify` utility has been improved with a new verification stage to check connectivity to Scale Out Repositories (SOR) and key records for Performance and Availability Clusters (PAC) enabled enterprise server regions.

(549010)

- The `casverify` utility has been improved with new external security manager checks against configured default users and provided user credentials. Also, step names have become more concise, which might affect scripts consuming `casverify` output.

(609033)

- If the Micro Focus Common Client (MFCC) attempts to bind to an MFDS directory using configured credentials, and the credentials are rejected, it will retry the bind anonymously. This emulates the behavior of older product releases and is not a security weakness since it will only succeed against non-secured directories.

(673053)

- The password-expiration heuristic mechanism (**expiration-check** configuration setting) of the MLDAP ESM Module has been enhanced to improve accuracy under a number of conditions with various LDAP servers. Micro Focus recommends that customers using LDAP-based security for Enterprise Server with bind-mode user verification enable this setting as it results in more precise and accurate return codes from ESF Verify (user authentication) operations. See *MLDAP ESM Module Bind Rejection Heuristics* in your product Help for more information.

02547852 (472036)

- The **expiration-check** option of the MLDAP ESM Module now supports checking for the commonly-used LDAP user attributes `passwordExpirationTime` and `pwdChangedAt`, when attempting to determine whether a user bind was rejected due to an expired password. This improves the accuracy of the error codes returned when using LDAP-based security with bind-mode user verification.

02520274 (411002)

Interface Mapping Toolkit

[Back to the list](#)

- COBOL clients now correctly format an `x-www-form-urlencoded` JSON request body.
02495086 (402050)
- The generated COBOL Web service client proxy program now keeps the communication session open for the duration of potentially multiple service-invocation calls.
02441897 (385004)

Micro Focus Common Client

[Back to the list](#)

- When the Micro Focus Common Client (MFCC) needs to use MFDS to find the location of a service, it now by default tries to use the `readonly` account configured as part of the default Enterprise Server security to bind to MFDS. This is enabled through the `mf-client.dat` configuration file, and can be changed after installation. The effect of this change is that functions such as listing deployment listeners with the `imtkmake` command will typically work in a fresh product installation with no further configuration changes required.
(656131)

Micro Focus Cryptographic Library

[Back to the list](#)

- The TLS Certificate Checking Utility is a new executable that can be used to help diagnose problems with TLS certificates. It can check the validity of certificates, verify certificate chains, check that certificates and private keys match and check that a certificate contains a SAN that matches a provided hostname/address. It improves TLS usability by diagnosing TLS certificate problems.
(666106)

Resolved Issues - Fixes

[Back to the list](#)

The numbers that follow each issue are the Support Case Numbers followed by the Issue number (in parentheses).

- [Common Communications Interface](#)
- [Compiler](#)
- [Data Tools](#)
- [Debugger](#)
- [Documentation](#)
- [Enterprise Server](#)
- [Enterprise Server Auditing](#)
- [File Handling](#)
- [Interface Mapping Toolkit](#)
- [MFUnit Testing Framework](#)
- [Micro Focus Directory Server](#)
- [Micro Focus License Administration](#)
- [Run-Time System](#)
- [SQL: COBSQL](#)
- [SQL: DB2 ECM](#)
- [SQL: OpenESQL](#)

- [Visual Studio Code](#)
- [Visual Studio IDE](#)
- [XML Support](#)

Common Communications Interface

[Back to the list](#)

- MRPI clients no longer experience high CPU usage when trying to contact a TLS enabled Micro Focus Directory Server (MFDS).
(474026)
- The CreateDemoCA script will now error with an informational message if the target directory does not exist.
(679011)
- Memory leaks occurred on outbound connections.
(632064)

Compiler

[Back to the list](#)

- When a program was compiled with PERFORM-TYPE(RM) and TESTCOVER an error could occur.
02810218 (656001)
- 64-bit Windows only. Native code only. When a program used parameterized performs, and passed a two-byte comp-x item by value in a call statement, the NCG sometimes failed to generate the code and give an error.
(549015)
- Windows 64-bit generated code only: an issue where a program uses nested programs and parameterized sections has been fixed.
(587005)
- An error in generated code when the size of perform-frame local variables is large - typically > 32K - has been fixed.
(529009)
- All platforms except Intel x86 32-bit. For generated code only, an error accessing perform-frame local variables has been fixed.
(614046)
- An issue in generated code, which was applicable to all platforms except Intel x86 32-bit, regarding perform frame local variables used as actual parameters to an invocation of a parameterized perform, has been fixed.
(640145)
- Compiling COPY REPLACING syntax with the CP preprocessor, where more than one replacing text string is a match, is now processed with correct precedence (that is, the earliest specified).
02615125 (515001)
- Compiling a program with the CP preprocessor, that includes DIRECTIVES-IN-COMMENTS, now has that option fully respected.
02625721 (522038)
- Optimization work has been completed on internal structures for certain sizes of COMP-5 FILLER items to mitigate against internal limits being broken when there are a large number of these items.
02622866 (522008)

- The CP preprocessor (and hence the COBSQL preprocessor) now correctly processes lines which, after COPY REPLACING has taken effect, are longer than the specified SOURCEFORMAT setting allows.
02694883 (569001)
- A COMPUTE statement with an index name operand now compiles and executes as expected.
02616505 (516028)
- Non-unique paragraphs in non-unique sections now compile and execute as expected.
02673302 02709104 (550010)
- Issues with SBCS Kana characters when used in the sequence area have been fixed.
02805785 (653168)
- A source file with a large number of external programs can now be edited normally, without background syntax checks slowing down and eventually being disabled.
02802818 (657005)
- Very large programs that exceeded a Compiler system limit and received error message COBCH1674S Internal dictionary overflow now compile without error.
02744922 (640020)
- A COMP-3 field without decimal places can now be generated by `IS2WS` as a type-decimal SOAP field rather than type-integer by adding a nominal trailing `V` to the PICTURE clause, for example `S9(5)V`. This has no effect on the compiled code, but provides a way to emulate the IBM behavior of always generating type-decimal fields for all COMP-3 items.
02684426 (564011)
- A COBCH808S Maximum number of data items exceeded error no longer occurs for a program with a very large number of data items, most of which are unreferenced.
02711056 (615041)
- Previously, `COBPROF` was truncating output to 79 columns when `+wide` was specified, and was not truncating when `+wide` was omitted. This is the opposite of the correct behavior, and so has been fixed.
00367108 (13279)
- Programs with a very large number of predominantly unreferenced data items, can now compile without breaking system limits.
02622364 (519033)
- The INITIALIZE of a reference-modified numeric item now executes as expected.
02757198 (640076)
- The external names of functions and function prototypes are now checked for consistency.
(666084)
- The syntax `LENGTH OF variable-length-group` used as a reference modification offset now executes as expected in all scenarios.
02757096 (637070)
- Illegal MOVE statements involving level-88 condition names now correctly receive a syntax error rather than generating illegal intermediate code.
02787014 (643131)
- Processing of the BASIS control file now correctly differentiates between a BASIS DELETE statement and a DELETE token that is part of an EXEC SQL statement.
02629601 (526116)
- The INITIALIZE .. TO VALUE statement now works as expected for table value syntax.
02613611 (510045)
- An INITIALIZE ..TO VALUE statement, which refers to multi-value table syntax, now compiles and executes as expected.

(9332)

- Within an EVALUATE statement, you now correctly receive a COBCH0334 Cannot follow WHEN OTHER error if a WHEN clause follows a WHEN OTHER clause.

(516009)

- MOVE statements involving condition names now execute correctly when valid, and are rejected when invalid.

(652137)

- A program with an incorrect non-unique data name specified as a PROCEDURE DIVISION USING parameter now has normal IDE functionality available.

02598892 (498059)

- Defining DYNAMIC LENGTH items in the LINKAGE SECTION, to be used as BY REFERENCE parameters or RETURNING items, is now supported.

(414197)

- The STATIC keyword is now a context-sensitive word under the ENTCOBOL dialect. (STATIC remains a reserved word under .NET and JVM COBOL.)

(661032)

- In an overlapping perform range, none of the overlapping sections must contain locally declared variables, nor must they be parameterized. Such scenarios generate a COBCH2024 error during compilation.

(675020)

- If a program containing a SORT statement with an input or output procedure was compiled to .NET or JVM with a perform type other than MF, bad code could be generated, resulting in an invalid program exception at run time.

02619192 (515065)

- A SEARCH ALL statement on a variable length group within a class (as opposed to a procedural COBOL program) could sometimes work incorrectly, as it used the maximum length of the group instead of the current length. This has now been resolved.

02640706 (526104)

- A READ statement of the form :read type a::bwhere b is a static property in type a exposing a dictionary or list, was producing an error. This is now fixed.

02669838 (550012)

Data Tools

[Back to the list](#)

- UNC paths were not properly resolved when loading data or structure files.

02819143 (673075)

- There was an issue with deleting multiple records of Line Sequential files simultaneously.

02542533 (425037)

- Previously, records located via the **Go To** action were not selected in the editor. This is now fixed.

02542696 (427048)

- The **Data File Tools Structure** view displayed incorrect values for binary data items that were explicitly defined with a number of storage bytes different to the default.

02649377 (536037)

- When inserting new records, the caret was always positioned at the end of the new record. This is now fixed.

02542581 (427045)

- In overwrite mode (toggled by Insert key) it was impossible to extend the length of text in fields. This also applied to functions like Find/Replace. This is now fixed.

02596359 (501005)

Debugger

[Back to the list](#)

- An issue has been fixed within the **Character Animator**, where data item names containing DBCS characters sometimes could not be queried.

02811986 (658028)

Documentation

[Back to the list](#)


- Searching the help for `special registers` now returns the main topic on special register usage.
(612069)
- Details of the CP pre-processors COPYINEXEC directive have been added to the documentation. Use this directive to determine whether CP treats COPY tokens in an EXEC statement as a COBOL COPY statement or part of the embedded language syntax.
02729687 (623036)
- The documentation for the READ statement has been corrected for rule 26 in the General Rules for Formats 1, 3, 4 and 5 (Sequential, Relative, and Indexed Files) section.
(489027)
- Dynamic length items are no longer restricted items to enclose in a JAVA-SHAREABLE block.
(666196)
- A formatting issue in the Usage Clause syntax diagram has been corrected - the THREAD-POINTER and typedef-name-1 elements are now showing correctly.
(505117)
- The parameters for library routine CBL_SUBSYSTEM have been updated in the product Help.
(386097)
- The documented restriction for the F run-time switch usage within .NET COBOL and JVM COBOL has been removed.
02720237 (613087)
- The Z run-time switch has been removed from the documentation.
(520009)
- The documentation now includes an additional rule for the DECLARE statement to point out that, unless explicitly initialized to a value, a DECLARED item is initially undefined.
(667190)
- A number of reserved and context-sensitive words have been added to the product in support of the latest ENTCOBOL enhancements; see the *Reserved Words Table* and *Context-sensitive Words Table* topics in the product help for full details.
(666134)
- A typo has been corrected in the parameter definitions of the documented CBL_GET_PROGRAM_INFO routine.
(517025)
- The documentation has been updated to clarify some potentially undefined behavior when the `cobtidy()` function is invoked; see the *cobtidy()* help topic.
(637112)

- The documented Byte-stream library routines have now moved to a sub-section under the *Files and Filename Routines* section.
(610007)
- The documentation for the CALL statement has been corrected with respect to the LENGTH OF clause, which can now take a literal value when under the MF dialect.
02182932 (218025)
- The *File Handling Performance* documentation has been updated to reference the DATACOMPRESS and KEYCOMPRESS options, which can significantly improve performance.
02737405 (639069)
- The SORT documentation has been updated to include the BUILD synonym that is supported within the OUTFIL and OUTREC control statements.
02707437 (613023)
- The documented definition of MFFTP_PROCESS_TRAILS_ONGET control variable has been corrected to state it works in conjunction with LOCSITE (and not LOCSTAT).
02772554 (644097)
- Additional optional security features are available for HTTP and MFBINP conversations, for the Web Services and J2EE, Web, and Remote File Access conversation types. Listeners can be configured to require user authentication and/or to restrict access to specific types of requests. See *Enhanced Security for HTTP and MFBINP* in your produce Help for more information.
(635054)
- The option to associate an enterprise server region with a project has been removed from the Visual COBOL documentation.
00372693 (11386)
- The documentation covering the syntax options required for building the container demonstrations has been updated to include the hotfix option, when building demonstrations built from a patch update product.
02590001 (488005)
- The product documentation was missing a product name in the instructions for running a native COBOL application on a network server.
(550040)
- The documentation now includes information on how to create a Certificate Authority (CA) trust store and how to set a password.
02767272 (643023)
- The JSON Processing tutorial in the documentation has had a few cosmetic updates.
(666207)
- The documentation has been updated to reference the level 78 item, MFU-GET-FILE, available in `mfunit.cpy`, that can be used to call the MFUGETF routine.
(9316)
- The documentation for the PROPERTY clause has been updated to explain how a property is exposed based on the setting of the ILARRAYPROPERTY directive.
00373023 (13206)


Enterprise Server

[Back to the list](#)

- The Mfsecrets AES provider now uses umask when creating directories.
(469050)

- Mfsecrets AES provider will now follow the umask when creating files
(464065)
 - The Privacy Enhanced Mail file `CARootCerts.pem` has been updated.
(244065)
 - ESCWA interactive API library request body documentation has been corrected for pipeline related endpoints.
(485045)
 - Success message from CAS is now checked to return a success. Any message different to the successful cancel will now be interpreted as an error and ESCWA will notify as such.
(567043)
 - ESCWA would crash when deleting a package or handler along with its associated service.
02594214 (489082)
 - ESCWA now accepts fully qualified domain names for its bind address.
02493351 (450067)
 - ESCWA will now return a unique message if the user if user has been revoked.
02808236 02862909 (651201)
 - In ESCWA, on the **Services** page you can now delete parent services and associated packages in a single action.
02591547 (489045)
 - In ESCWA and version 2 of its API, the DCT recoverable fields did perform correctly.
(561042)
 - In ESCWA, an error would occur if non-ASCII characters were sent to ESMAC.
02729629 (625030)
 - In ESCWA, the PO/PDS datasets were not loading.
02819576 (658003)
 - In ESCWA, the SEPs logs were not displaying.
(652129)
 - ESCWA interactive API V2 endpoints failed to operate correctly, including tracing and `tn3270Screen`. These have been fixed.
(485029)
 - The ESCWA **XA Resource** page no longer has a notice that it is a technology preview feature.
02534474 (415107)
 - ESCWA now allows Catalog Entries with DS Org set to GDG to have empty string to be submitted for Record Format through the API and it has been hidden by the API
(653208)
 - In ESCWA, the documentation for the Web API contained errors that prevented client generation using OpenAPI. In addition, fields that were missing have been added and security and resource keys have been removed from version 2 of the API.
-  **Attention:** Micro Focus strongly recommends that you no longer use security and resource keys.
- (453029)
 - In ESCWA, the comparison of PAC strings were treated as case sensitive.
02761061 (638085)

- A problem that caused memory for `escwa.exe` processes to grow without falling back to normal levels has been fixed.
02735194 (629100)
- In ESCWA, validation has been added to multi-line file path inputs to ensure they do not contain leading or trailing white space characters.
02513150 (515022)
- In ESCWA, user token fields were treated as invalid if the stored value contained inconsistent capitalization.
02634935 (545054)
- In ESCWA, you can now remove locks if necessary. Contact Micro Focus Customer Support for more information and guidance on removing locks. See *Locks* in your product Help for more information. The `casstop` resource entity is checked as part of the OPERCMDS resource class. A user must have **Alter** permissions to do this, which are the same permissions required to stop a region.
(651022)
- User authorization is no longer logged by default and can be enabled in the ESCWA interface.
(682002)
- You can now configure ESCWA to audit request bodies. To enable this auditing, check **Audit Request Bodies** in **Tracing and Logging Settings**. This information is recorded in audit event code 5 10. See *Tracing and Logging Settings* and *Audit Event Codes* in your product Help for more information.
02605389 (525006)
- In earlier releases, the sample LDIF security definitions had incorrect definitions for the DOC*, TCP*, and URI* resources in the MFESMAC class. This resulted in access failures when attempting to view or modify those resource types in ESCWA for some administrative users when LDAP-based security was used and security rules were specified using one of the sample configurations.
(651189)
- The `mldap_esm` security manager will now load the appropriate threaded/non-threaded version of `libldap` which will result in the correct threaded/non-threaded LDAP library to be loaded.
(273023)
- When using `mfseconv` to export users, the **Audit** property was not exported correctly. In addition, when using `mfseconv` to convert LDIF to YAML the case of the **Mto** property for a user was not correct. These have been fixed.
(665201)
- The `esfadmin` command-line utility will now accept an ESM server URL of up to 256 characters in length. Previously this was limited to 80 characters.
(484061)
- The `mfseconv` utility now sets a non-zero exit code if it encounters any serious errors, messages of error or severe error level are reported. If the new `--exit-codes` command-line option is specified, it sets exit code 3 if any severe errors are reported, 2 if any errors are reported, 1 if warnings are reported, and 0 if only informational messages are generated. This feature will assist in determining success or failure when running the utility in a script.
(653180)
- The `mfseconv` export was creating incorrect YAML.
(652164)
- A number of modifications have been made to diagnostic messages to improve accuracy and relevance when users attempted to change their passwords under Enterprise Server, when the MLDAP ESM Module was used with bind-mode authentication.
02547852 (505042)

- An issue existed with the map CN configuration option for the DCAS conversation type.
02528628 (414079)
- If the configuration for a Security Manager using the MLDAP ESM Module explicitly disables Version 1 Authentication (the default behavior), this no longer incorrectly forces DSS wildcard processing to compatible mode.
02637403 (529091)
- Performing an `mfsecconv` import of a YAML file containing users with non-literal password verifiers will no longer cause those users to have an incorrect password.
(666125)
- Enterprise Servers MLDAP ESM Module can now detect the failure to contact an LDAP server for more types of network failures. Configure the connect timeout setting to permit the module to abandon hanging connection attempts after a specified time. If the redundant option is enabled for an enterprise server region (or ESCWA or MFDS) security, a connection timeout will let ESF fail over to another Security Manager; otherwise, it will let ESF fail the security request after the timeout expires, rather than hanging indefinitely.
 **Note:** With this change, if a timeout is not configured the module will timeout a connection attempt after 2147483 seconds, a bit less than 25 days.
02004184 (193042)
- Under certain configurations the MLDAP ESM Module could fail to authenticate user credentials correctly, allowing users to sign onto Enterprise Server with incorrect passwords.
02652865 (537022)
- For security and SYSLOG AUDIT enabled enterprise server region, `mfdatatools2` no longer leaves File Descriptors with Syslog AUDIT permanently opened.
02792367 02806218 02882401 (652220)
- If a Distributed Program Link (DPL) targeting TXSeries resulted in a backout, this was not being signaled through EIBRESP.
02639307 (628005)
- When attempting to emit the message `CASKC0001E Transaction trn abend abcode. Backout Successful.` the CASSI process could trap with an RTS114 error.
02625044 (576015)
- When a distributed program link (DPL) originator executed a SYNCPOINT ROLLBACK the end of task processing would report an AEXJ abend.
02725418 (633017)
- The matching string was incorrectly built.
(297001)
- When `casgate` processed large volumes of concurrent work, the TCA control block could be left in an invalid state, resulting in the TCA being disconnected.
02609989 02612420 02618756 (509036)
- CASOUT requests can hang in server when SEPs are too busy.
02620485 (522007)
- When a 403 Forbidden was issued, the Web error program DFHWBEP was not called. This has been fixed
02833723 (665237)
- On a busy system, when multiple ITRs were created the KEY could sometimes be a duplicate, resulting in loss of an ITR. A unique key is now always created.
02615912 (517014)

- When using DISPLAY upon console, the buffer was truncated on the first x00 value.
02793186 (653054)
- Concurrent SET FILE requests were resulting in SEP and enterprise server region crashes.
02629317 (528008)
- After a distributed program link had been executed a subsequent TS queue operation could result in a SYSIDERR.
02826408 (663078)
- When an enterprise server region was starting in a PAC, it could sometimes rollback an inflight transaction executing in another region.
02809622 02856124 (657012)
- Whenever trace flags are modified via ESCWA or casutl, a console message is now written to indicate the trace flags that are currently active.
(499017)
- If a pool thread in the casras process failed to access a record in the PSOR due to an error scenario that required the thread to reconnect, the thread did not retry to connect. The thread now retries the connection 10 times. This can be modified by setting ES_SOR_RETRIES to the required number of attempts. If the thread still fails to connect then a CASRS2107E console message will be generated.
02815996 02819419 02791959 02870114 (665003)
- The casrdo modules were initializing or handling the cascookie browser cookie incorrectly.
02713518 (589017)
- The FLENGTH operand is now initialized to 0 if the container no longer exists.
02794254 (652175)
- Files with more than 8 indexes were not being displayed in ESMAC.
(484021)
- The Historical Statistical Facility (HSF) CASA_ECI_Function now records the program name when a PGMIDERR abend occurs.
02406172 (362003)
- New ESMAC sessions did not redirect to the **System Sign On** page when the default user sign on was disabled on a secure enterprise server region.
02518847 (415043)
- A trap could occur in casmgr depending on the memory layout, because the memory type was not checked when processing a chain. This has been fixed
02835014 (665257)
- When a process died before responding to the process that issued an RPC wait, the recovery failed to dispatch the waiting process, resulting in a process hanging.
02671714 (561035)
- Invocation of a Tuxedo -hosted program using DPL and specifying a transaction ID was not working.
02538521 02644110 (419027)
- The terminator for custom field entries has been changed from # to x00. This is to prevent field entries from being truncated at #.
02737028 (629069)
- The CASSI1452E console message now correctly reports runtime errors that caused casmfdbfh initialization to fail.
02703834 (614008)
- The Internal Reader queue will now be installed in all enterprise server regions in a PAC, and not only on the first region starting the PAC.

02669519 02678257 (545089)

- Every time `casmgr` hard killed a process that was stuck after the threshold issued a kill, a dump was taken. If someone was formatting the dump at the same time, `casmgr` would be blocked trying to access the dump file for up to 10 seconds. A kill is now issued for all the stuck processes and only perform a single dump at the end.

02814032 (666034)

- If a `USERIDERR` occurred then the partner did not receive the error message.

02744133 (628170)

- When a `USERIDERR` occurred on a start transaction the socket failed to close. This has been fixed

02739278 (629094)

- When the `ENOMEM` error was reached after the maximum number of sockets were in use, the listener would not issue the `ACCEPT` call, resulting in a blocked listener.

02667973 (613088)

- When creating a resource the name was not being trimmed.

02667449 (542093)

- Using the `SET TRANSACTION` API did not publish changes to other enterprise server regions in the PAC.

02634669 02674657 02712535 (528029)

- A shared memory leak could occur during `castrc` recovery processing.

02568907 (474022)

- When a shared memory lock produces a dump, the lock is released before opening the dump file, and the lock is acquired afterwards.

02867469 (683131)

- An enterprise server region would fail to start if `FUTEX` was enabled.

02782113 (643047)

- The `casclsec` utility failed to receive the `userid`.

02636579 (526099)

- When a distributed program link passed a large channel, the receiving enterprise server regions buffer could overflow causing unpredictable behavior.

02600111 (517086)

- HTTP requests exceeding 32 headers to a Web Services and J2EE listener can cause a runtime error in `MFRHCGI`. This has been fixed. HTTP requests exceeding 64 headers to a Web Services and J2EE listener might be rejected with a 400 HTTP response status code with Too many request headers. in the response body.

02789436 (651069)

- A delay in transaction routing and DPL introduced by the fix for defect 401124 has been fixed.

02656673 02656960 (543009)

- DPL interactions with a Tuxedo CRM server would trap during SL2 exchanges.

02667227 (543087)

- Issuing a program cancel with the no wait option in a PAC, left an orphaned record in the PSOR. This record is now cleaned up at the end of the command.

02674657 (615074)

- The `FILE` API response codes were not being propagated back to the remote system.

02785730 (648026)

- Incorrect auth calls were being made while using the `DFED`.

02628702 (529011)

- Alter or update privileges for a user are only checked when a user is performing an update action.
02619324 (515072)
- The code that matches TS queue instances with TSMODEL prefixes did not always return the closest matching prefix.
(540013)
- An RTS 114 could occur in `cascd` or `casmgr` when the connection to the database used by MFDBFH was lost.
02575775 (486054)
- The copybook `dfhcbtct.cpy` has been updated to the latest version.
02821444 (667228)
- The 64-bit Dump Formatter incorrectly formatting trace point 4084 from `dfheserv`.
02599370 (506047)
- Improvements have been made to the checks for jobs waiting to be dispatched in an enterprise server region.
02596825 (503030)
- The console message `CASSI9051I` was not displayed correctly.
(472003)
- Support for multiple system procedure libraries has been added.
02762877 (639081)
- LRECL was truncated when displaying the catalog dataset properties.
02632597 (528027)
- A delay in transaction routing and DPL introduced by the fix for defect 401124 has been fixed.
02645065 (526115)
- In ESCWA, an error caused uninitialized data to be entered into the file size in some cases where 0 should have been displayed.
02527126 02616594 (509029)
- The number of connected SEPs was truncated when the value was higher than 255.
02640448 (528100)
- When using the provided TCPIP SERVICE(HTTPNSSL) from GROUP(DFHWEB), CWBXN would try to link to a program name only containing spaces as the TCPIP SERVICE had no URM defined.
(645127)
- New traces have been added to differentiate between GLM, PAC, or LOCKDB locks.
(651046)
- An RTS 173 could occur in the `casverify` command-line utility during verification for the ESMQXA XA switch module.
(662068)
- If a network error occurred in one of the CASRAS threads but not in the PING thread, then the threads that contained the error would stop processing work.
02653594 02792419 (649048)
- Viewing the system trace table from ESCWA (by selecting **Trace X**) displayed invalid timestamps in all trace entries.
(566040)
- The find option in CEBR did not work correctly. This has been fixed
02803455 (657011)

- If an application performed a READ FILE ... UPDATE and then invoked a DELETE with RIDFLD() where the RIDFLD was different from that used in the READ, this would fail with an INVREQ.
02806458 (663049)
- If the buffer to display contained an x 00 then the text was truncated.
02861717 (683119)
- When a user not accessible in the OS user database attempted to start an enterprise server region, a runtime error would occur in `cascfg`.
02659924 02782387 (543066)
- Previously, if a Configuration Manager property fails validation, the enterprise server region initialization would fail with a corresponding `CASCF0070E` console log error message. Now, in some situations the property value will be limited and identified by a `CASCF0071W` console log warning message.
02662199 (622019)
- DPL requests that interacted with Tuxedo CRM would result in a trap in the target during SyncPoint processing.
02690834 (600001)
- During an INVOKE SERVICE command, the name of the current channel might be incorrectly modified that is a GET CONTAINER with the CHANNEL option would return CHANNELERR.
02837778 (674022)
- ENDDATA was incorrectly sent when a client using http was disconnected.
02526457 (473050)
- On a busy system with active TRANCLASS, SEPs could hang if they did not receive a response to a request if some SEPs had died.
02646979 02671418 02751632 02680443 02894969 (547001)
- In ESMAC, user access to the **Server Information** page can be restricted using the **TABLE*** resource under **MFESMAC** in LDAP.
00368580 (13547)
- When running in a PAC, a RETRIEVE could incorrectly return an IOERR. This would occur if the transaction was initiated via a START using the TERMID and FROM options and the terminal was connected to an enterprise server region different to the one processing the transaction executing the START.
(477002)
- A PACs internal reader jobs were not dispatched when using disposition MOD.
02669519 (561052)
- The EIBRESP from the remote enterprise server region was not being propagated to the requester region.
(567053)
- When a SEP is killed before it can pick up work, the terminal was not notified resulting in a hung state.
02552505 (464090)
- The SET-TERMINAL performance has been improved. Shared memory is now used for an ENQ from a LOCKDB enterprise server region instead of using MFDBFH.
02797529 (651059)
- Authentication checks would fail when the ES_ESM_SECPRFX environment variable was enabled.
02628811 (527015)
- Viewing active Interval Control Elements (ICE) from ESCWA or ESMAC for a TRANCLASS enabled enterprise server region could unexpectedly fail, or result in a memory access violation in `cast.sc` if the Temporary Storage, Channels and Containers Control (TSC) trace flag was set.
02569568 (508026)

- If a SEP was terminated in the middle of writing to a TS queue, then an infinite loop could be encountered on all subsequent writes to that queue. This is a result of the queue control record not being updated. If this does occur then the first write will retry for a period before returning TIMEDOUT. All subsequent writes will function as normal.
02625902 (521033)
- Stage descriptions and step names in the `casverify` command-line utility have been updated to be more consistent and informative.
(662031)
- Paths containing spaces were not correctly handled in enterprise server region configuration when using the `casverify` utility.
(550021)
- The token creation for the BROWSE CONTAINER commands (STARTBROWSE, GETNEXT, and ENDBROWSE) did not operate correctly.
(685021)
- A CFLE transaction incorrectly set the file to DISABLED when CLOSING.
02852107 (681023)
- Attempting to perform a DPL from TXSeries would fail due to unexpected PIP data included with the ATTACH.
02622825 02703317 (577002)
- An issue preventing Japanese localization from being displayed on the ESCWA **Advanced Region Properties** page has been fixed.
(389049)
- An error is now returned if a `castran /v` is attempted on a program that has a PPT specified.
(517043)
- When using the EXEC CICS INQUIRE TERMINAL API, the `userarea` and `userarea len` were not being returned correctly.
02767317 (644145)
- Displaying fixed record length files with deleted records on ESCWA and legacy ESMAC interface could have issues with paging and report an incorrect total record count.
(685076)
- The import and export of TST resources now supports Process Local and Exclusive queue types.
02757840 (640174)
- The incorrect length was used on query security when RESTYPE was used.
02852945 (679030)
- Starting a `cobesdebug` session with `type=J2EE` would result in a communications timeout error.
02594045 (504155)
- Attempting to dynamically update an XA Resource without a close string could result in an RTS114 within the `CASA_Update_XRM` service.
(653074)
- In a PAC environment, if a transaction had performed an XA prepare and not performed an XA commit or XA rollback while a new enterprise server region was starting, the recovery transaction started at the region start could result in an incorrect recovery of an inflight transaction. The process now checks that it is a true indoubt transaction rather than an inflight transaction.
02575529 (477030)
- Any nameless steps in preflight modules have now been titled appropriately.
(674050)

- The ESCWA v2 dynamic-config API produced a JSON error when a HTTP PUT request succeeds with further messages.
(653051)
- SYSIDNT was not retrieved correctly when added to the configuration manager.
02635287 (683088)
- Added option for regular JSON output to the `casverify` command line utility. See `casverify` in the product Help for more information.
(658063)
- The embedded template command `#INCLUDE` is now supported in DOCUMENT APIs.
02728038 (651024)
- When XAID is specified, ISOLEVEL is now set for the dynamic Oracle and DB2 switches.
(472008)
- If the ESXAEXTCFG exit module fails to load when ESLOGGING is enabled in the XA open string, then a `CASKC0025I` message will be displayed in the console log.
02725011 (623009)
- The PostgreSQL XA switch module now uses a valid SQL statement to test the current connection.
02721671 (618025)
- The XA recovery transaction failed when using `ES_XA_RECONNECT` and the connection to the Resource Module (RM) was lost, the transaction was started too many times which flooded the system.
02532560 (415184)
- XA resource without customization in the XA open string continues to open connection as-is when Micro Focus Vault support is enabled for other XA resources.
02671497 02675636 02819649 (547042)
- If a container that should have been created by the application was not found, then the error in `DFHJSON-ERROR` and `DFHJSON-ERRORMSG` failed to be returned. This is now fixed.
02801082 (652110)
- `mfsecrets` no longer displays unhelpful warning about config items not being found in ESCWA logs.
02543385 (425051)
- If `mfsecrets` fails to load the config file it now displays a more explicit error.
(662041)
- After performing a successful migrate, `mfsecretsadmin` will no longer produce an error message indicating it failed.
(661078)
- In ESCWA, previously the transaction count on the **Live Properties** page and API was incorrectly tied to the task number, which would reset when reaching 99999.
(683114)

Enterprise Server Auditing

[Back to the list](#)

- An issue occurred at shutdown when using TLS, this could result in socket closure before the peer had time to complete receiving.
(272016)

File Handling

[Back to the list](#)

- A new index has been added to the RecordLocks tables, to improve performance when accessing busy files.
02501734 (467002)
- When submitting JCL jobs to a spooler hosted in MFDBFH, a problem where two jobs could be issued the same job number when the system was under heavy load, has been fixed.
02570363 02599513 (469065)
- When searching on wildcards in a catalog hosted in MFDBFH, sometimes not all matching records would be returned. This has now been resolved.
02647090 (534024)
- A segmentation fault has been fixed when uploading indexed and sequential files to an SQL Server via MFDBFH.
02399653 02593176 (364088)
- Handling of stranded locks on region recovery has been improved.
02520632 (409110)
- A number of performance improvements have been made relating to Oracle DBs use of applocks.
02709174 (613045)
- An issue where the MFDBFH cross-region installation scripts would fail to run due to incorrectly generated statements has been resolved
(645036)
- An issue with deadlocks in MFDBFH has been resolved where we would mistakenly cause a full table scan, which resulted in TABLOCKS being taken. Indexes have been added to the Filename and Folder columns of the \$DataStore\$ table to help prevent this.
02618882 (518002)
- There was an issue where warnings from SQL code execution were reporting a bad file status incorrectly. This is now fixed.
(526092)
- The fileID has been added as part of an index name, to keep it unique, as previously duplicate index names were being generated.
(528097)
- The dbfhview utility will now convert ASCII numeric data (that is not of type COMP), that is stored in Postgres or SQL Server, to human readable values.
02488484 (399076)
- When using MFDBFH with Oracle databases, all required Oracle functions are now installed, if not already detected.
02687277 (549030)
- When opening a file hosted in MFDBFH that didnt exist but was marked as optional, it was possible for a deadlock to occur within the Oracle Openfile procedure. This procedure has now been modified to remove that possibility.
02684956 (567017)
- If a stored procedure for MSSQL was missing, it would be dynamically installed, but would sometimes still report an error that it was missing. This error no longer appears.
(559039)
- During a READ operation, the read closest op code now finds the next complete record from the relative byte address provided.
(387018)
- An error displayed in the IDE stating that a project Could not load assembly MicroFocus.COBOL.FHRedir.dll has been fixed.

(515058)

- An issue, where programs that included the following copybooks failed to compile when using the `sourceformat(free)` directive, has been fixed:
`fsdatab.cpyfsdatabv2.cpyfsviewop.cpyfsviewopv2.cpyxfhcd3.cpy`

(403045)

- An issue has been fixed when initializing File Handling tracing when the `mfdas32` command is run.

(675076)

Interface Mapping Toolkit

[Back to the list](#)

- Web services using very large SOAP messages no longer throw a 153 (subscript out of range) runtime error.

02778746 (645015)

- COBOL client generation no longer fails due to the presence of escaped XML characters.

02730776 (629048)

- CICS Web Service requestor SOAP messages no longer contain extraneous namespace declarations.

02771747 (644034)

- Top-down generated CICS Web services now correctly handle mixed-content SOAP elements.

02809925 (651214)

- The `occurs` attribute is now unbounded on service interface fields for COBOL items that have an ODO clause and that are mapped using default mapping.

02614317 (519020)

- The presence of escaped XML characters sometimes caused COBOL client generation to fail.

02662184 (544055)

MFUnit Testing Framework

[Back to the list](#)

- An issue with COBOL Language Server failing to locate `MFUPD_` and `MFUWS_` prefixed files when compiling with the MFUnit Pre-Processor (`mfupp`) has been fixed.

(530030)

Micro Focus Directory Server

[Back to the list](#)

- Creating a new Communications Process could result in a duplication of an existing Communications Process instance value. This has been fixed. In addition, improvements have been made to enterprise server region **Validate** feature which now checks for and fixes duplicate instance values and Communications Process names that do not match the parent Enterprise Server name.

02627797 (528031)

- The Micro Focus Directory Server (MFDS) could sometimes crash when adding an External Security Manager (ESM) if no password was supplied.

(446038)

- A TLS-enabled Micro Focus Directory Server (MFDS) would become unresponsive when receiving requests from MRPI clients.

02552647 (465007)

- Setting Default Process UserID value as a UID rather than `userid` value caused the MFDS process to abend when using ESCWA to view enterprise server region data.

02604940 (515077)

- MF Directory Server would fail to start if `mfdscfg.xml` options file `bind_address` value was numeric rather than containing a valid hostname or IP address in standard format. Older versions of this file could contain either `127.0.0.1` represented as a 32-bit integer or `0` which represented listen on all available network adapters. MFDS now accepts either of these numeric address values.

02639711 (529085)

- When creating a Communications Process using the ESCWA API, any input hostname address value would always be set to `*`.

02670494 (547019)

- Fileshare server registrations in the MF Directory Server were not being preserved after the Directory Server was restarted and the **Save** legacy Micro Focus Servers option was checked.

02597483 (504062)

- In ESCWA, MFDS did not correctly support a shared memory (`smem`) listener configuration.

(677003)

- When starting enterprise server regions with ISC listeners, transient internal CCI servers with an MFNAME: prefix can appear in the MFDS or ESCWA user interface server list. To display these server types you must check the **Show System Server Types** option.

(484006)

- Fix issue with security configuration rollback if there was an issue verifying proposed configuration for MF Directory Server using ESCWA.

(665224)

- For Windows x64-only products, the Micro Focus Directory Server was not determining the correct directory for Visual COBOL binaries.

(657093)

- XRM openstring values were not saved to the configured vault when importing from a repository into the MF Directory Server.

(683175)

- In some circumstances, when importing legacy MF Directory Server configuration data the External Security Manager (ESM) password was not migrated to the Micro Focus Vault Facility correctly.

02574313 (525025)

- The `mfActualEndpoint` addresses for enterprise server listeners were not being updated or written to when using an XML file repository.

(495017)

Micro Focus License Administration

[Back to the list](#)

- An issue causing the CES daemon to crash has been resolved.

02816509 (617028)

Run-Time System

[Back to the list](#)

- Some native COBOL programs invoked via the `cobrun` trigger could display their command line parameters incorrectly.

02695958 (607020)

- Previously, the window position of COBOL programs executed with `runw/runmw` would not get restored correctly.

02560848 (453001)

- The RANDOM intrinsic function, when called from native COBOL programs, could sometimes return negative values when using large seed values.

02687376 (615064)

- Previously, accessing files on SMB Azure file shares could result in a COBRT181 error unless the remote_64bit_access tunable was set.

02745899 (633033)

- Previously, the setupenv.bat script used the built-in RANDOM environment variable to generate unique temporary filenames. This has now been changed to use a PowerShell command to generate a UUID, and then uses that in the generated temporary filenames instead.

02787305 (647052)

- Display issues when mixing COBOL ADIS displays with displays of a different type have been resolved.

02581162 (477021)

- Display issues, when mixing COBOL ADIS displays with displays of a different type, have been resolved.

02581162 (520022)

- Tab characters have been removed from one of the supplied copybooks: cbltypes.cpy.

02783984 (643089)

- Previously, running a COBOL program would erroneously fail with the COBRT253 Cannot load file - unsupported format (Fatal) error if COBPATH was explicitly set to not include the directory where the program was located. This has now been changed to return the COBRT173 Called program file not found in drive/directory error.

(588003)

- The tutorial instructions for COBOL calling Java static method (COBOL/Java Interoperability project) have been updated to specify the setting of the COBSW environment variable; this variable is required to address a display issue with the program output.

(567033)

- A new tunable - entry_point_mapper_invalid_path_error - which is off by default, has been added to control whether the COBOL Run-Time System should report an error if the ENTRYNAMEMAP environment variable refers to invalid/non-existent filename and directory paths.

(589018)

- Previously, enabling CTF tracing in .NET applications on Windows that used the native file handler (or SQL) could result in a COBRTS164 error. This had now been fixed.

02704607 (615004)

SQL: COBSQL

[Back to the list](#)

- COBSQL now correctly handles host variable arrays that require COMP/COMP5 conversion.

02668849 (543111)

- COBSQL has been updated to correctly handle an END-PERFORM problem caused by the new swap byte logic.

02668849 (562025)

- COBSQL has been updated to support sign conversion of CHARSET ASCII + SIGN EBCDIC.

02683191 (573002)

- COBSQL has been modified such that it no longer inserts group information in the EBCDIC conversion statement when the group variable is a FILLER.

02555993 (442071)

- COBSQL was updated to correctly handle EBCDIC conversion of EXEC SQL OPEN USING statements.
02804887 (651165)
- COBSQL has been updated to handle EBCDIC conversion of numerical values contained within redefined group variables.
02584237 (481010)
- COBSQL has been updated to fix compilation issues related to ALPHA-LIT-CONT directive support.
02594669 (489083)
- To correct a compile problem caused by redefined variables, COBSQL has been updated to closely track group variable information while determining which variables to convert.
02570841 (464033)
- COBSQL now properly handles the EBCDIC conversion of FETCH FIRST/NEXT statements.
(649057)
- COBSQL has been updated to fix a swap-byte conversion issue that occurred because an SQLCODE=100 was returned after a multi-row FETCH.
02702058 (596010)
- COBSQL has been modified in this release to handle EBCDIC conversion of FETCH ROWSET statements.
02687410 (637117)
- COBSQL has been updated to properly terminate EXEC SQL statements that are replaced by dummy lines during SYBASE precompilation.
02722549 (625013)
- COBSQL now correctly handles EBCDIC conversion of EXEC SQL statements that contain group items as host variables.
02791368 (649037)
- COBSQL now recognizes the NOAMODE directive and handles it correctly at run time.
02592714 (516075)
- COBSQL now correctly handles source lines that contain a comma in column 8 immediately followed by a COMP host variable.
02675814 (547024)
- COBSQL was updated to support ENTRY statements broken into multiple lines.
02426309 (374014)
- COBSQL was updated to use heap instead of an array to handle redefined variables.
02666211 (71231)
- COBSQL has been modified to handle periods in column 72 when the next line is empty.
02485117 (414080)
- COBSQL was updated to handle inline comments after END-EXEC token.
02624353 (520008)
- COBSQL now generates run-time logic correctly for signed numeric data items.
02811569 (658027)
- COBSQL now correctly handles signed numeric data items in a group.
02811569 (656026)

SQL: DB2 ECM

[Back to the list](#)

- A problem with .NET 6 processing that erroneously truncated CHAR and VARCHAR values returned from SELECT statements has been fixed.
02790279 (653118)
- A problem that occurred when compiling a program using the DB2 ECM caused a -1309 SQLCODE compiler error instead of a connection pop-up dialog.
02354465 (503026)
- A problem using an mfd daemon resource for connection credentials compiling a program using the DB2 ECM has been fixed.
02354465 (643020)
- DB2ECM now compiles without problem when the HOSTVAR directive is used.
02686034 (564020)
- The DB2 ECM produced a connection dialog box instead of automatically connecting when the mfd daemon was not started and mfaclient.ini contained valid database connection credentials. This has been resolved.
02354465 (644030)

SQL: OpenESQL

[Back to the list](#)

- The native SQL runtime sometimes hung when it encountered the EXEC SQL ROLLBACK TO SAVEPOINT command. This has been resolved.
02565661 (469019)
- A problem that caused an unwarranted rollback when the last SQL statement issued was a commit or rollback, and the next SQL statement was a disconnect has been resolved.
02731137 (628044)
- OpenESQL now handles EBCDIC application correctly when the AMODE(31) directive is used in a 64-bit environment.
02541041 (454020)
- DSNREXX now handles multiple SQL Statements correctly and without corrupting memory.
02599095 (504116)
- A problem that prevented the OpenESQL runtime from releasing all pinned .NET objects for MFSQLEMESSAGETXT has been fixed.
02690852 (612080)
- OpenESQL has been updated to support user IDs containing a dot.
02637077 (525103)
- A problem with incorrectly cleaning up the ODBC environment sometimes caused OpenESQL to throw a memory access violation error. In this release, the ODBC environment is cleaned up such that this error no longer occurs.
02742293 (630097)
- WITH RETURN cursors are now opened as KEYSET type instead of DYNAMIC type.
02541903 (461001)
- A compiler error that was caused when using the SQL(GEN-SQLCA) directive without separately defining SQLSTATE in program code has been fixed.
02743040 02794285 (629124)
- The ODBC ECM error code 12 was sometimes returned during a compile with SQL directives when processing an interface.
02543269 (425092)

- Running Visual Studio 2022 in a language other than US English or Japanese prevented the **Micro Focus SQL Tools** menu from appearing.
(663030)
- A problem that sometimes caused the OpenESQL runtime to leak memory when handling threads has been fixed.
02646010 (531005)
- The THREAD=ISOLATE SQL compiler directive option now works correctly when a native connection is used by a managed program running in the same thread.
02670859 (625018)
- The Oracle RM switch module now supports Oracle Client version 21c.
02850631 (673121)

Visual Studio Code

[Back to the list](#)

- An issue where Language Server fails to start when a .NET SDK is not available has been resolved.
(508011)

Visual Studio IDE

[Back to the list](#)

- When the **Store credentials** option is unchecked in the **Enterprise Server Sign On** dialog box, the credentials are now used when starting a server in the running instance of Visual Studio.
02545553 02766720 (476012)
- The PATH environment variable is now fully expanded when running a 32-bit application under the debugger.
02610282 (515003)
- A program compiled to `.int` can now be specified as the debug target for a 64-bit project.
(640128)
- An issue with missing Japanese translations of some menu items has been resolved.
(544122)
- Visual Studio support has been improved to better handle variable names that appear in structures.
(409031)

XML Support

[Back to the list](#)

- XML PARSE has been updated to properly handle XML instance documents with a large number of content characters within tags.
02575649 (472007)
- The XMLPARSE feature is now available in the Enterprise Server for Stored Procedures product.
02822761 (663037)
- XML READ now performs much faster when a big OCCURS value is used in the XML data-item.
02630023 (525082)

Other Issues Resolved in This Release

The numbers listed are the Support Incident Numbers followed by the Issue number (in parentheses).

- 02556886 (468003)
- (662117)
- 02537488 (453046)
- 02624110 (520012)
- 02723517 (618034)
- 00363234 (28048)
- 00477923 (61180)
- 02822038 (508052)
- 02394824 02778550 (351052)
- 00373450 02406104 (11527)
- (61096)
- (442036)
- 02823160 (675050)
- 02725405 (628033)
- 02780781 (647035)
- 02743825 (629142)
- 02686079 02733133 (629006)
- 02600111 (597005)
- 02583111 (485001)
- 02783874 (648018)
- 02646617 (540015)
- (513014)
- (568005)
- 02677554 (560014)
- 02730120 (628029)
- (649040)

Unsupported or Deprecated Functionality

This section includes information about features or functionality that are not supported.

- The SafeNet Sentinel licensing system has been deprecated. This product uses the Micro Focus AutoPass licensing technology. Contact your account manager to replace your existing SafeNet Sentinel with AutoPass licenses. Also, see *Advanced Installation Tasks > Licensing Coexistence when Upgrading to Release 10.0* in the *Installation* section in your product Help.
- The HOSTSIGNS Compiler directive is no longer supported. Micro Focus recommends that you use the following Compiler directives instead: SIGN-FIXUP, HOST-NUMMOVE, and HOST-NUMCOMPARE. This is a change since version 3.0 of this product.

Additional Software Requirements

To ensure full functionality for some Visual COBOL features, you might be required to obtain and install additional third-party software.

See this information on the Product Documentation pages on OpenText Support for Micro Focus Products, in the product help for Visual COBOL for Visual Studio 2022 ([click here](#)).

Installation

Before Installing

Downloading the Product

1. Log into the Software Licenses and Downloads (SLD) site at <https://sld.microfocus.com/mysoftware/download/downloadCenter>.
2. Select your account and click **Entitlements**.
3. Search for the product by using any of the available search parameters.
4. Click **Show all entitlements**.
5. Click **Get Software** in the Action column for the product you want to download or update.

In the **File Type** column, you see entries for "Software" for any GA products, and "Patch" for any patch updates.

6. Click **Download** on the relevant row.

On Windows

System Requirements

Hardware Requirements

Visual COBOL has the following requirements in addition to the requirements of Microsoft Visual Studio. See the Visual Studio documentation for details of the Microsoft requirements.

The maximum disk space requirements are, approximately:

Visual COBOL	Sentinel RMS License Manager
1.2Gb	75MB

- This includes the space needed to cache information locally so that you can modify the installation without the original source media.
- The disk space requirements include the versions of JRE and .NET Framework supplied with the setup file.

Operating Systems Supported

For a list of supported operating systems, see *Supported Operating Systems and Third-party Software* in your product documentation.

Note:

- A 64-bit Windows is required. You can produce both 32-bit and 64-bit applications with Visual COBOL installed on a 64-bit operating system.

Software Requirements

The setup file will check your machine for whether the prerequisite software is installed and will install any missing prerequisites and the product components. A supported version of Microsoft's Visual Studio must be installed in advance.

Besides the software listed below, the setup file also installs the 64-bit AdoptOpenJDK 17.0.4 (LTS) with Hotspot.

This product includes OpenSSL version 3.0.8.

- [Visual Studio IDE](#)
- [Selecting the Visual Studio components to install](#)
- [Installing Visual Studio features that are not currently installed](#)
- [License Manager requirements](#)
- [Other Requirements](#)

Visual Studio IDE

You must have Microsoft's Visual Studio 2022 version 17.8 or a newer one installed in advance.

You need one of the advanced versions of Visual Studio listed below:

Professional, Enterprise or Community Edition - see the next section for the Visual Studio components you must install.

Microsoft's Visual Studio Express Edition is not supported.

Important:

- When installing Visual Studio, ensure you select the Help Viewer component for installing if you want to view the Visual COBOL product help inside Visual Studio. When you select components to install in the Visual Studio installer, click **Individual components** and check **Help Viewer** in the **Code tools** section.

The following software is also required:

- Microsoft .NET Framework 4.7.2. This is included with Visual Studio.

Selecting the Visual Studio components to install


The Visual Studio installer enables you to customize and only install the workloads and components that are most suitable for your area of development. For example, you can select the components that are required for .NET desktop development, ASP.NET Web or C++ development.

If not already installed, the Visual COBOL setup file will install the following components:

- .NET Framework version 4.7.2.
- Debugger
- Data services

A number of workloads and components are optional and only required by specific types of applications or tasks:

- Azure, WCF, Web, WPF, MSVC, or SQL CLR application development.

 **Important:** The latest version of the **C++ x64/x86 build tools** component, which is part of the MSVC Workload, is required to generate some IMTK clients.

If you require any of these, you can select them when you start the Visual Studio installer or, enable them after completing the installation - see the next section.

Installing Visual Studio features that are not currently installed

If a feature of Visual Studio was not installed during the Visual Studio installation, the respective functionality or the project templates for it are not available. You can install a missing feature in one of the following ways:

Rerun the Visual Studio installer:

1. Start the Visual Studio installer and choose to modify an existing Visual Studio instance.
2. Select the workloads and the components that are missing (for example, **ASP.NET and web development** or **Help Viewer**).
3. Start the Visual Studio installation.

Use the **Quick Launch** control in Visual Studio:

1. Start Visual Studio.
2. Type the name of the feature in the **Quick Launch** control - for example, type `ASP.NET` or `Help Viewer`.

A drop-down list with any features matching your search string appears. If the feature is not already installed, one of the search results will be an option to install it.

Use the `Install Missing Feature(s)` command in Visual Studio:

1. Start Visual Studio.
2. Click **Help > Micro Focus Product Help > Install Missing Feature(s) > Feature Name**.

Follow the instructions in the installer to install the missing feature.

3. Alternatively, if a Visual COBOL project template requires a Visual Studio feature which is not currently installed, the IDE displays an information bar with instructions to install the feature.

License Manager requirements

- For local servers, you do not need to install the Micro Focus License Administration tool separately, as the setup file installs a new Visual COBOL client and a new licensing server on the same machine.
- If you have any network license servers, you must update them before you update the client machines.
- If you are upgrading from Visual COBOL release 2.2 or earlier, uninstall the license manager before installing the product.

You can download the new version of the license server software by following these steps:

1. Log into the Software Licenses and Downloads (SLD) site at <https://sld.microfocus.com/mysoftware/download/downloadCenter>.
2. Select your account and click **Downloads**.
3. Select a product and a product version from your orders.
4. In the list of software downloads, locate the **License Manager**.
5. Click **Download** to download an archive with the installers.
6. Run the installer suitable for your Operating System to install License Manager on your machine.

Other Requirements

Various actions and operations within your COBOL development environment depend on certain files that Microsoft distributes in the following package: the Windows SDK package. See *Microsoft Package Dependencies* for a full list of actions and operations that require one or both of these packages.

By default, the product installation installs the latest versions of the Microsoft Windows 10 SDK, and the Microsoft Build Tools for Visual Studio 2017, to their default locations.

If you need to use any other version of these packages, or use them installed to a non-default location, use the `cblms` command line utility post-installation to manage this; see *Managing the Microsoft Build Tools and Windows SDK Packages* for more information.

Product Co-Existence

- Visual COBOL and COBOL Server cannot coexist on the same machine.
- Micro Focus Visual COBOL and Visual COBOL cannot coexist on the same machine regardless of which IDE (Visual Studio or Eclipse) you install.

Installation Restrictions and Requirements

Before starting the installation you should consider the following:

- If, when you install Visual COBOL, the machine does not have Microsoft Visual C++ 2017 Redistributable Runtime already installed, it is installed as required by Visual COBOL. The installation of Microsoft Visual C++ Redistributable Runtime adds a number of `.dll` files, without digital signatures, into the `winsxs` directory.
- You need to be logged in with a user-ID that has write access to the registry structure under `HKEY_LOCAL_MACHINE`, `HKEY_CLASSES_ROOT`, and `HKEY_CURRENT_USER` so the installation software can set the environment appropriately. You also need to be logged on with Administrator privileges.
- Various actions and operations within your COBOL development environment depend on certain Microsoft files distributed in the following packages: the Windows SDK package and the Microsoft Build Tools package. By default, a standard product installation downloads and installs these. Refer to *Microsoft Package Dependencies* to see if these packages are required. If you do not plan to use your development tool in a way that will depend on any of these packages, you can run a non-standard installation, which will skip their download and installation, thus saving disk space and time taken for installation. Refer to *Advanced Installation Tasks* for details on the available installation options.

Basic Installation

The instructions in this section apply when you are performing a basic installation of this product for the first time. If you are an administrator, you can perform a basic installation on a local machine before performing a more advanced installation when rolling out the product to developers within your organization.

For considerations when installing this product as an upgrade, for additional installation options or non-default installations, see *Advanced Installation Tasks* in your product Help.

Installing



Note:

- This version of the product is a full install.
- See *Before Installing* first for important information. Also, see *Installing as an Upgrade*, if you have an earlier version of Visual COBOL installed on your machine.

To install this product:

1. Run the `vcvs2022_100.exe` file and follow the wizard instructions to install the prerequisite software and the product.
2. If, after installing, there are issues with using the Micro Focus functionality, you might need to execute the following command from a Visual Studio command prompt:

```
devenv /updateconfiguration
```



Note:

- If you are installing onto a machine that has an existing Micro Focus product that uses an older Sentinel RMS License Manager, you might be prompted to remove it and install the Micro Focus

License Administration. By doing this you maintain the existing Sentinel RMS license files while adding the Micro Focus License Administration. If you are unsure about existing licenses on your computer or removing the Sentinel RMS License Manager, consult your System Administrator. If you want to proceed, remove Sentinel RMS License Manager by using **Program and Features**, and rerun the installation file.

- Trial licenses cannot be used with remote desktop services. If you want to use your product in this way, please contact OpenText Support for Micro Focus Products to obtain a relevant license.
- We recommend that you install any updates for Visual Studio and the .NET Framework that are available at the [Microsoft Download](#) site.
- If you install JDK you might be prompted to install the latest update. The latest update is not required for use with Visual COBOL but you can install it if you wish.

Advanced Installation Tasks

This section includes instructions about how to perform a non-default installation, install this product as an upgrade, or about how to install the additional components.

The advanced installation tasks include:

- *Installing as an Upgrade* - included in these Release Notes
- *Command line installation options* - included in these Release Notes
- *Installing on Microsoft Terminal Server and Citrix* - available in the product Help and on the Product Documentation pages on OpenText Support for Micro Focus Products

See this information on the Product Documentation pages on OpenText Support for Micro Focus Products, in the product help for Visual COBOL for Visual Studio 2022 ([click here](#)).

On Windows

Installing as an Upgrade

- This release cannot be installed as an upgrade to an earlier release of Visual COBOL. You must uninstall the previous version before installing 10.0.

Licensing Coexistence when Upgrading to Release 10.0

With release 10.0 of the Visual COBOL product suite, the SafeNet Sentinel licensing technology has been deprecated. This can result in some compatibility issues if you install 10.0 on a machine where there are other Micro Focus products or versions installed that use SafeNet Sentinel licensing. While the 10.0 installation process has been designed to address such issues, you should be aware of the following scenarios and if any action might be required to ensure licensing works as expected:

Scenarios

Your installed products use SafeNet Sentinel Licenses (Windows and UNIX)



Warning: Installing 10.0 deprecates SafeNet Sentinel licensing on the machine.

If you use SafeNet Sentinel licenses for any other Micro Focus products, such as Enterprise Analyser or Relativity, you need to contact your account manager to obtain AutoPass licenses for these products. See the *Troubleshooting* section further in this topic, *Action 7* for how to obtain a list of your installed licenses.

Your older products use AutoPass licenses (Windows and UNIX)

Existing AutoPass licenses are compatible with the 10.0 products.

- Upgrading to 10.0 (UNIX)** After installing 10.0 on a machine with a previous version of licensing installed, the lserv daemon is retained (and might be running) but is not required. See *Troubleshooting > Action 2* for details.
- Downgrading from 10.0 (Windows and UNIX)** In order to revert to a previous version of the product (for example, if 10.0 is installed but no longer required), the 10.0 product and licensing must be uninstalled. See *Troubleshooting > Action 1* for details.
- Installing a product or Patch Update of an older product release (UNIX)** Use the "skip license installation" command line arguments.
- See *Troubleshooting > Action 3* for details.
 - Else, see *Troubleshooting > Action 4* to reset mfcsed.
 - SystemD may be overwritten - see *Troubleshooting > Action 6*.
- Installing a product or Patch Update of an older product release (AIX only)** If after 10.0 is installed a customer installs a Patch Update for an older release, the lserv entry is moved back to /etc/inittab.
- See *Troubleshooting > Action 3* about how to avoid this.
 - To correct the /etc/inittab entry, see *Troubleshooting > Action 5*.
 - Alternatively, re-run the 10.0 license install. See *Troubleshooting > Action 6*.

Troubleshooting

Action 1 To reset licensing from the 10.0 installation to an older product configuration, you need to perform the following:

Windows Uninstall the product and the License Manager from "Uninstall a Program" in the Windows Control Panel.

UNIX Execute the following commands:

```
sudo $COBDIR/bin/Uninstall_[Product Name]_10.0.sh.
sudo /opt/microfocus/licensing/bin/
UnInstallMFLicenseServer.sh
```

Action 2 (UNIX) To disable the lserv daemon on a machine, execute the following commands:

```
cd /var/microfocuslicensing/bin
sudo ./stopmfcsed.sh
sudo systemctl stop MFSafeNet
sudo systemctl disable MFSafeNet
```

Action 3 When installing an older release or Patch Update, use `-skipsafenet -skipautopass` to the install command. This will skip the licensing installation for that release.

Action 4 To restart mfcsed from the correct location, execute the following commands:

```
cd /var/microfocuslicensing/bin
sudo ./stopmfcsed.sh
cd /opt/microfocus/licensing/bin
sudo ./startmfcsed.sh
```

Action 5 To reset the inittab on AIX 7.3/7.4:

1. Edit the /etc/inittab file.
2. Delete the line:

```
mFls:2345:wait:sh /var/microfocuslicensing/bin/startlserv.sh 2>&1
```


Action 6 To reinstall the 10.0 licensing and reset any issues from installing a previous version, execute the following:

```
cd [10.0-COBDIR-location]/licensing
sudo MFLicenseServerInstall.sh force
```

Action 7 In order to get a list of the installed licenses:

- Windows**
1. From a COBOL command environment, execute `mfsupportinfo`.
 2. View the **Micro Focus Licensing** section.
- UNIX**
1. In a terminal, run `cobsetenv` to set the product environment.
 2. Run `mfsupport`.
 3. See `mfpoll.txt` for the licenses details.

Visual COBOL Installation Options

To install Visual COBOL you run `vcvs2022_100.exe` which contains a number of product `.msi` files (Windows Installer packages). When run, `vcvs2022_100.exe` performs some initial system checks then sequentially installs the `.msi` files.

`vcvs2022_100.exe` can take a number of parameters, enabling you to specify a number of different types of installation:

- Standard Installation

Format:

```
vcvs2022_100.exe
```

Summary:

Full installation including License Manager and Visual COBOL. During installation you can specify options including the location to which the components are installed.

- Non-standard Installation

Format:

```
vcvs2022_100.exe skipmstools=1
```

Summary:

Full installation, minus the Microsoft package dependencies. A standard installation downloads and installs the latest Windows SDK packages. Refer to *Microsoft Package Dependencies* to see if you will depend on these packages, and if not, use the option above to skip installation of the packages, thus reducing the footprint and duration of the installation process.

- Non-interactive Installation

Format:

```
vcvs2022_100.exe /passive
```

Summary:

Full installation, but the components are installed non-interactively using default options and directories.

- Silent Installation

Format:

```
start /wait vcvs2022_100.exe /q
```

Summary:

Full installation, but the components are installed non-interactively with no user interface, using default options and directories.

- Modified Silent Installation

Format:

```
start /wait vcvs2022_100.exe /q InstallFolder=d:\otherdirectory
```

Summary:

Full installation, but the components are installed non-interactively with no user interface, and Visual COBOL is installed to `d:\otherdirectory`.

To see what parameters you can use, execute the following from the command line:

```
vcvs2022_100.exe /?.
```

**Note:**

- Log files that are created during installation are saved in the folder specified by the TEMP environment variable. To change the location or name of the files, use the `/log` parameter on your setup command line and specify the path and file name, for example: `filename /log d:\temp\log.txt`. This creates a log file, named `log.txt`, in the `d:\temp` directory.

After Installing

- See *Changes in Behavior or Usage* in your product documentation and in the Release Notes for important information about changes in this release that might affect existing applications.
- Check the *Product Documentation* section of the [OpenText Support and Services Documentation Web site for Micro Focus products](#) for any documentation updates.

On Windows

Starting the Product

You are now ready to run Visual COBOL:

Windows 10 • From your Windows desktop, click **Start > Visual Studio 2022**.

Windows 11 • Click the **Start** button in the Task Bar. Use the search field in the Start menu to find and start **Visual Studio 2022**.

Enterprise Server Security Considerations

Starting with this release, the Enterprise Server security functionality provided by the VSAM External Security Manager (VSAM ESM) module is enabled by default out of the box. This means you now need to supply valid credentials when you interact with:

- Enterprise Server Common Web Administration (ESCWA)
- The Micro Focus Directory Server (MFDS)
- enterprise server regions via:
 - ESCWA
 - Certain command-line utilities (such as `casstart`)
 - The Server Explorer window in the IDE or in the new Data Tools available in 10.0
 - IMTK deployment

For more information about the default VSAM Security Manager, see *VSAM ESM Module* in your product Help.

Upgrading an Existing Security Configuration

If security is already configured for a domain (Data Tools, MFDS, or the default Enterprise Server security), the installation process does not change this configuration. If data already exists in either the old or new

VSAM ESM default data directory, it will not be altered. However, Micro Focus recommends backing up the following before reinstalling or updating the product - the Data Tools and MFDS configuration files (`commonwebadmin.json` and `mfdsacfg.xml`), the MFDS repository data, and the VSAM ESM Module security data. By default, the MFDS repository data and the VSAM ESM Module data are located under `%ProgramData%\Micro Focus (Windows)` or `$COBDIR/etc` (UNIX).

Default Generated Password for SYSAD

The installation generates a random password for the system administrator account, SYSAD. To retrieve this password, execute the following from an Visual COBOL command prompt or Visual COBOL command prompt (Windows) or from a terminal that has the COBOL environment set (UNIX):

```
mfsecretsadmin read microfocus/temp/admin
```

The password value stored in this vault location is not used by the default Security Manager (VSAM ESM) to validate input credentials. Its purpose is to enable users to initially discover their randomly generated password. Additionally, Server Explorer uses this location to pre-populate the **Micro Focus Servers** connection and the credentials dialog box at region start-up. Once entered, you can optionally save the credentials in IDE-specific storage. Micro Focus recommends that once the credentials are safely known or changed that you remove this value from the vault (using `mfsecretsadmin delete microfocus/temp/admin`).

Change the Default Password for SYSAD

Micro Focus recommends that you promptly replace this password with one that conforms to your security policy. You can do this from the ESCWA logon page - click **Change Password**. Alternatively, you can use the `esfadmin SETPASSWORD` command and specifying the "vsam_esm" module file.

Authentication in the Browser-Based ESCWA

You need to provide credentials to access ESCWA. After the installation, the ESCWA logon page shows information on how to obtain the default admin (SYSAD) generated password. You can disable this message in the ESCWA Security Settings dialog ("Show Default Security Warning on Log On").

For local installations, the default Directory Server will automatically be authenticated with the ESCWA credentials. Otherwise, you might need to provide its own credentials. You may use the same credentials as the ones for ESCWA.

Note the default 5-minute (300 second) session time out setting for inactivity in ESCWA. If required, you can change this from the ESCWA Security Settings dialog ("Session Inactivity Timeout").

Authentication Inside the IDE and the Data Tools Utility

The Server Explorer window in the IDE and in Data Tools, requires credentials for the **Micro Focus Servers** node to connect to the default local ESCWA and the MFDS. Additionally, you need to provide credentials to start any regions. By default, the credentials will be pre-populated in the dialog using the values stored in the `microfocus/temp/admin` vault location. These credentials can optionally be stored by the IDE so they do not need to be manually input again.



Note: If you delete the SYSAD user or change the password generated for it by the installer in the default VSAM Security Manager, you need to provide new sufficiently authorized credentials for the Server Explorer connection.

Fileshare

If you want to view or delete Fileshare instances in ESCWA, you now need to log on using authorized credentials (such as the default SYSAD user).

Command-Line Utilities

There are multiple command line utilities that control and access enterprise server region. These use Enterprise Server credentials specified as parameters - for example, `casstart /z`.

See *Administration and Configuration Commands* in your product Help for individual commands to determine how to specify authorized credentials.

Samples and Tutorials

There are a variety of samples and tutorials supplied with the product. Many of these assume that security is not enabled, so to work through these unaltered default security will first need to be disabled. See *To Disable the Default Enterprise Server Security Configuration* in your product Help. If security is not disabled, you will need to take it into account when you:

- Use ESCWA
- Start a region
- Run a cas command line utility

In Server Explorer inside the IDE, the SignOn dialog boxes to ESCWA will have the default generated SYSAD credentials pre-populated. If the SYSAD password has been changed, or you need to use different credentials, you need to sign on using the required details.

Micro Focus Common Client

The `mf-client.dat` file which is used by the Micro Focus Common Client (MFCC), is configured out-of-the-box to use the default generated "readonly" credentials from the `microfocus/common/readonly` vault location. This means that access to the Micro Focus Directory Server using the default security configuration works automatically for read-only access.

MFCC is used by COBOL web service proxy programs, the Interface Mapping Toolkit service-deployment mechanism, Fileshare clients (when configured appropriately), various utilities such as `cassub` (depending on the operating mode), the CICS Web Interface and CICS Web Services, and product components such as MFCS and ESCWA. See *Micro Focus Common Client* in your product Help.

Managing the Microsoft Build Tools and Windows SDK Packages

There are a number of COBOL development features that depend on the Microsoft Build Tools and Windows SDK packages. By default, the product installer downloads and installs these packages to their default locations. The installer then sets your COBOL environment to depend on those downloaded versions.

You can use the Microsoft Build Tools and Windows SDK Packages configuration utility - `cb1ms` - to view which versions are in use, and also configure your COBOL environment if you require something other than the standard usage.

For example, some project types (for example, .NET projects) require a different version of the Microsoft Build Tools (the Visual Studio 2019 version) than the one installed (the Visual Studio 2017 version). If you have already installed the correct version for *.NET*, run `cb1ms` after product installation, to update your environment to use the correct package.

There is an option within the product installer to skip the installation of the default packages (`skipmstools=1`); however, this does skip both packages, so make sure that you do already have the package(s) that you require before setting this - see *Microsoft Package Dependencies* for details on the package(s) you may require.

The Microsoft Build Tools and Windows SDK Configuration Utility

Use the `cb1ms` command line utility to view and set the package versions in effect for your COBOL environment.



Important: If you are updating or clearing package versions, you must run this utility from a command prompt with administrative privileges.

Syntax:

```
cblms <option>
```

Parameters:



Note: <option> settings are case insensitive.

<option> can be one of:

-U

Updates the COBOL environment to use the latest versions of the Microsoft Build Tools and SDK packages that are located in the default folders. Any open IDE instance or command prompt must be restarted before these changes take effect.

-U<ms-pkg>

Updates the COBOL environment to use the latest version of the particular package type that is located in the default folder. Any open IDE instance or command prompt must be restarted before these changes take effect.

-U<ms-pkg>:<version>

Updates the COBOL environment to use a specific version of the particular package type that is located in the default folder. Any open IDE instance or command prompt must be restarted before these changes take effect.

-U<ms-pkg>:<path>

Updates the COBOL environment to use the latest version of the particular package type that is located in the (non-default) folder specified. Any open IDE instance or command prompt must be restarted before these changes take effect.

-U<ms-pkg>:<path>?<version>

Updates the COBOL environment to use a specific version of the particular package type that is located in the (non-default) folder specified. Any open IDE instance or command prompt must be restarted before these changes take effect.

-L

Lists all versions of the Microsoft Build Tools and SDK packages that are located in the default folders.

-L<ms-pkg>

Lists all versions of a particular package type that are located in the default folder.

-L<ms-pkg>:<path>

Lists all versions of a particular package type that are located in the (non-default) folder specified.

-Q

Displays the versions currently in use by the COBOL environment.

-Q<ms-pkg>

Displays the version of the selected package type that is currently in use by the COBOL environment.

-R

Clears all version information. (Only use this option when instructed to by OpenText Support for Micro Focus Products.)

-H

Displays the available command line options.

Legend:

- <ms-pkg>** *<ms-pkg>* can be one of **S** or **SDK** for the Microsoft SDK, or **B** or **BT** for the Microsoft Build Tools.
- <path>** *<path>* is the path in which to locate packages that are not installed to the default location for their package type.
- <version>** *<version>* is the package version with which to update when the latest version is not the one required. When specifying *version*, it must be in the form:
- *n.n.n.n* for a Windows SDK
 - *n.n.n* for Build Tools
 - *n* for list ID - the list ID is displayed using `cblms -L`.

The following example updates the COBOL environment to use version 10.0.17134.0 of the Windows 10 SDK, installed in `C:\WinSDK\10`.

```
cblms -USDK:C:\WinSDK\10\10.0.17134.0
```

Viewing the Product Help

Visual COBOL is configured to display the product help available online on the OpenText Support for Micro Focus Products website: <https://www.microfocus.com/support-and-services/documentation/>.

You can view the product help in one of the following ways:

Online help (default)



Note:

- Your Visual Studio must be configured to show online help by default. Make sure **Help > Set Help Preferences** in Visual Studio points to **Launch in Browser**.
- Ensure that you have an up-to-date version of your browser.

You can access the Help in one of the following ways:

- Click **Help > Micro Focus Product Help > Product Documentation**.
- Alternatively, press **F1** inside the editor or from a UI part.

This opens the Visual COBOL help or Microsoft's MSDN depending on which keyword in the editor or part of the UI you are querying.

Local help



Note: If you've had an earlier version of Visual COBOL installed on your machine, you need to uninstall any older version of the documentation as follows:

1. Click **Help > Add and Remove Content** inside Visual Studio.
This starts the Microsoft Help Viewer.
2. Click the **Manage Content** tab and click **Disk**.
3. Click **Remove** next to the line for the Visual COBOL documentation.
4. Click **Update**.

The local help is not shipped with the installer. If you prefer to view the help locally on your machine, you need to download and install it manually as described below.

1. Download the local help files:

- a. Find the download link for local help in your Electronic Product Download email or in the **Product Updates** section on the OpenText Support for Micro Focus Products website and save the files on your machine.
 - b. Expand the archive on your machine. Ensure that the .msha and the .cab files are in the same folder.
2. Ensure that the Visual Studio Help Viewer is installed:
- a. Click **Help** inside Visual Studio.
 If no **View Help** command is available, you need to install the Help Viewer manually. See *Installing missing components of Visual Studio* in *Software Requirements* for instructions on how to install it.
3. Install the help in the Help Viewer:
- a. Click **Help > Add and Remove Content** inside Visual Studio.
 This starts the Microsoft Help Viewer.
 - b. Click the **Manage Content** tab and click **Disk**.
 - c. Click the browse button next to **Disk** and navigate to the folder in which you extracted the local help files.
 - d. Select `helpcontentsetup.msha` and click **Open**.
 This loads the Visual COBOL documentation.
 - e. Click **Add** and then **Update**.
 After the installation is complete, the Visual COBOL product Help appears in the Help Viewer.
4. Configure Visual Studio to use local help:
- a. Start Visual Studio.
 - b. Ensure that the Visual Studio Help Library is pointing to local help - from the Visual Studio menu click **Help > Set Help Preferences > Launch in Help Viewer**.
 - c. Click **Help > View Help**.

This opens the product help in Microsoft's Help Viewer.


For full details of the Visual Studio Help system, see the MSDN.



Note: On some Windows versions, an issue with Microsoft Help Viewer and Internet Explorer's security being turned on can cause the Help content to be displayed as raw HTML code. To resolve the issue, you need to turn off the Internet Explorer Enhanced Security Configuration (IE ESC) for both administrators and users. Check the Microsoft Windows help for more information on how to do this.

Repairing

If any product files, registry settings or shortcuts are accidentally removed at any point, you can perform a repair on the installation to replace them.

 **Important:** Before performing a repair of the installation, Micro Focus recommends that you create backups of any configuration files of the product that you might have changed.

To repair your installation:

1. From the **Control Panel**, click **Uninstall a program** under **Programs**.
2. Right-click your Micro Focus product, and select **Repair**.

Uninstalling

To uninstall the product, you cannot simply delete its files from your hard disk. To uninstall the product:

1. Log in with the same user-ID as you used when you installed the product.
2. Click **Uninstall a program** under **Programs** in **Control Panel**.

3. Select the product and click **Remove** or **Uninstall** as appropriate.

During the uninstall process, only those files added during the installation (to the installation and Samples directories) are removed. If the installation installed the Microsoft Windows 10 SDK or Microsoft Build Tools packages, these are left in place, although the Micro Focus-related registry entries for these packages are removed.

If the product directory has not been removed, delete any unwanted files and subdirectories within it using Windows Explorer.



Note: The installer creates separate installations for Visual COBOL Micro Focus Analysis Services Integration, and Micro Focus License Administration. Uninstalling only Visual COBOL does not automatically uninstall the Micro Focus License Administration or any of the prerequisite software.

To completely remove the product you must uninstall the Micro Focus License Administration as well.

You can optionally remove the prerequisite software. For instructions, check the documentation of the respective software vendor.

Some registry entries are not removed by the uninstallation process and you need to manually delete them.

The following folders might not be removed:

- The *Micro Focus Product Name* folder in the Start menu - you can delete it manually.
- %systemdrive%\Users\Public\Documents\Micro Focus - includes the binaries and the log files of the samples which you have built.
- %ProgramData%\Micro Focus - includes some data files used by the Micro Focus licensing system.
- %Program Files%\Micro Focus - you can delete it manually.

To silently uninstall the product, you need the setup file and you need to execute the following at the command line:

```
start /wait install-file.exe /quiet /uninstall
```

In addition, the following registry entries are not removed. These are created the first time that an Enterprise Server that has been enabled for performance monitoring starts up:

- Micro Focus Server\Performance\Active Servers
- Micro Focus Server\Performance\PerfIniFile

Licensing Information



Note:

- The SafeNet Sentinel licensing system has been deprecated. This product uses the Micro Focus AutoPass licensing technology. Contact your account manager to replace your existing SafeNet Sentinel with AutoPass licenses. Also, see *Advanced Installation Tasks > Licensing Coexistence when Upgrading to Release 10.0* in the *Installation* section in your product Help.
- Personal Edition licensing is only available with Visual COBOL for Visual Studio 2022.
- When you activate Visual COBOL Personal Edition, you can use it for a limited period of 365 days. After this period, you can either register a new Personal Edition license for 365 days or acquire a valid full license of Visual COBOL in order to continue using the product.
- If you have purchased AutoPass licenses for a previous release of this product, those licenses will also enable you to use this release.
- If you are unsure of what your license entitlement is or if you wish to purchase additional licenses, contact your sales representative or [OpenText Support for Micro Focus Products](#).

To activate Visual COBOL Personal Edition

To activate Personal Edition:

1. Start Visual COBOL.

If you have not installed a license for Visual COBOL, starting the IDE and trying to create a COBOL project opens the **Micro Focus Visual COBOL Product Licensing** dialog box. If you cancel this dialog box, you can invoke it again from **Help > Micro Focus Product Help > Product Licensing**.

2. Copy the authorization code which you were sent after registering for Personal Edition, and paste it into the **Authorization code** field.
3. Click **Finish**.

You should receive a message that the activation has been successful.

To buy and activate a full unlimited license

To buy a license for Visual COBOL, contact your sales representative or Micro Focus OpenText Support for Micro Focus Products.

For instructions on using the Micro Focus Licensing Administration Tool, see *Licensing* in the Visual COBOL help.

To start Micro Focus License Administration

To start the GUI Micro Focus License Administration

Windows 10 From your Windows desktop, click **Start > Micro Focus License Manager > License Administration**.

Windows 11 Click the **Start** button in the Task Bar. Use the search field in the Start menu to find and start **License Administration**.

To start the command-line Micro Focus License Administration tool

1. At a command prompt, navigate to:

```
C:\Program Files (x86)\Micro Focus\Licensing
```

2. Type `cesadmintool.bat`, and press **Enter**.

Configuring licensing for older products

If you use release 10.0 and previous releases on the same machine on UNIX, you need to set the environment variable `MFCES_INIT_LOCATION` to `/opt/microfocus/licensing/bin/ces.ini` in order for licensing to work for the older products. Also, see *Advanced Installation Tasks > Licensing Coexistence when Upgrading to Release 10.0* in the *Installation* section.

Installing licenses

You need a license file (with an `.xml` extension for AutoPass licenses). You need to install AutoPass licenses into the existing Micro Focus License Administration tool, and not in the AutoPass License Server.

Applying your license file

To use the GUI Micro Focus License Administration

1. Start Micro Focus License Administration.
2. Click the **Install** tab.
3. Do one of the following:
 - Click **Browse** next to the **License file** field and select the license file (which has an extension of `.xml`).
 - Drag and drop the license file from Windows Explorer to the **License file** field.
4. Click **Install Licenses**.

Alternatively, you can install the license file from within the IDE as follows:

1. Start Visual COBOL.

If you have not installed a license for Visual COBOL, trying to use the Micro Focus functionality for the first time after you install the product results in a warning message. Visual Studio displays an information bar with a message that Visual COBOL does not have a valid license. You can use the **Install license** link in the bar, or close the bar.

2. Click **Help > Micro Focus Product Help > Product Licensing** to open the **Product Licensing** dialog box.
3. Click **Browse** next to the **License file** field.
4. Select the license file (which has an extension of `.xml`), and then click **Open**.
5. Click **Authorize** to install the license.

You should see a dialog box with a confirmation that the licenses have been installed successfully.

To use the command-line Micro Focus License Administration tool

1. Start the command-line Micro Focus License Administration tool.
2. Select the **Manual License Installation** option by entering 4.
3. Enter the name and location of the license file.

If you have an authorization code



Note: Authorization codes are only available with Sentinel RMS licensing.

Authorizing your product when you have an Internet connection



Note:

- This topic only applies if you have an authorization code. Authorization codes are only available with Sentinel RMS licensing.
- It is not possible to install licenses remotely. You must be logged into the machine on which you are installing the licenses.

The following procedure describes how to authorize your product using a local or network license server. The license server is set up automatically when you first install the product.

To use the GUI Micro Focus License Administration

1. Start Micro Focus License Administration.
2. Click the **Install** tab.
3. Type the authorization code in the **Enter authorization code** field.
4. Click **Authorize**.

If you change the name of the machine running your license server after it has granted licenses, the licenses stop working.

To use the command-line Micro Focus License Administration tool

1. Start the command-line Micro Focus License Administration tool.
2. Select the **Online Authorization** option by entering **1** and pressing **Enter**.
3. Enter your authorization code at the **Authorization Code** prompt and then press **Enter**.

Authorizing your product when you don't have an Internet connection



Note: This topic only applies if you have an authorization code. Authorization codes are only available with Sentinel RMS licensing.

This method of authorization is required if the machine you want to license does not have an Internet connection or if normal (automatic) authorization fails.

To use the GUI Micro Focus License Administration

1. Start Micro Focus License Administration.
2. On the **Install** tab, click **Manual Authorization**.
3. Make a note of the contents of the **Machine ID** field. You will need this later.
4. Do one of the following:
 - If your machine has an Internet connection, click the OpenText Support for Micro Focus Products Web link in the Manual Authorization Information window.
 - If your machine does not have an Internet connection, make a note of the Web address and type it into a Web browser on a machine that has an Internet connection.

The Micro Focus OpenText Support for Micro Focus Products Manual product authorization Web page is displayed.

5. Type the authorization code in the **Authorization Code** field. The authorization code is a 16-character alphanumeric string supplied when you purchased your product.

6. Type the Machine ID in the **Machine ID** field.
7. Type your email address in the **Email Address** field.
8. Click **Generate**.
9. Copy the generated license string (or copy it from the email) and paste it into the box under the **License file** field on the Install page.
10. Click **Install Licenses**.

To use the command-line Micro Focus License Administration tool

In order to authorize your product from the command-line Micro Focus License Administration tool you must have the following:

- Access to a computer which is connected to the Internet.
- Your authorization code (a 16-character alphanumeric string).
- The machine ID. To get this, start the Micro Focus License Administration tool and select the **Get Machine Id** option by entering 6. Make a note of the "Old machine ID".

If you have previously received the licenses and put them in a text file, skip to step 6.

1. Open the Micro Focus license activation web page <http://supportline.microfocus.com/activation> in a browser.
2. Enter your authorization code and old machine ID and, optionally, your email address in the **Email Address** field.
3. Click **Generate**.
4. Copy the licenses strings from the web page or the email you receive into a file.
5. Put the license file onto your target machine.
6. Start the Micro Focus License Administration tool and select the **Manual License Installation** option by entering 4.
7. Enter the name and location of the license file.

To obtain more licenses

If you are unsure of what your license entitlement is or if you wish to purchase additional licenses for Visual COBOL, contact your sales representative or OpenText Support for Micro Focus Products.

Updates and OpenText Support for Micro Focus Products

Our Web site provides up-to-date information of contact numbers and addresses.

Further Information and OpenText Support for Micro Focus Products

Additional technical information or advice is available from several sources.

The product support pages contain a considerable amount of additional information, such as:

- Product Updates on [Software Licenses and Downloads](#), where you can download fixes and documentation updates.
 1. Log into the Software Licenses and Downloads (SLD) site at <https://sld.microfocus.com/mysoftware/download/downloadCenter>.
 2. Select your account and click **Entitlements**.
 3. Search for the product by using any of the available search parameters.
 4. Click **Show all entitlements**.
 5. Click **Get Software** in the Action column for the product you want to download or update.

In the **File Type** column, you see entries for "Software" for any GA products, and "Patch" for any patch updates.
 6. Click **Download** on the relevant row.
- The *Examples and Utilities* section of the OpenText Support for Micro Focus Products Web site, including demos and additional product documentation. Go to <https://supportline.microfocus.com/examplesandutilities/index.aspx>.
- The *Support Resources* section of the OpenText Support for Micro Focus Products Web site, that includes troubleshooting guides and information about how to raise an incident. Go to <https://supportline.microfocus.com/supportresources.aspx>

To connect, enter <https://www.microfocus.com/en-us/home/> in your browser to go to the Micro Focus home page, then click **Support & Services > Support**. Type or select the product you require from the product selection dropdown, and then click **Support Portal**.



Note: Some information may be available only to customers who have maintenance agreements.

If you obtained this product directly from Micro Focus, contact us as described on the Micro Focus Web site for Micro Focus products, <https://www.microfocus.com/support-and-services/contact-support/>. If you obtained the product from another source, such as an authorized distributor, contact them for help first. If they are unable to help, contact us.

Also, visit:

- The Micro Focus Community Web site, where you can browse the Knowledge Base, read articles and blogs, find demonstration programs and examples, and discuss this product with other users and Micro Focus specialists. See <https://community.microfocus.com>.
- The Micro Focus YouTube channel for videos related to your Micro Focus product. See [OpenText YouTube Channel for Micro Focus Products](#).
- Micro Focus webinars: <https://www.microfocus.com/en-us/resource-center/webinar>.

Information We Need

If your purpose in contacting Micro Focus is to raise a support issue with OpenText Support for Micro Focus Products, you should collect some basic information before you contact us, and be ready to share it when you do.

See the *Preparing to Raise a Support Case* topic on the Product Documentation pages on OpenText Support for Micro Focus Products, in the product help for Visual COBOL for Visual Studio 2022 ([click here](#)).

Creating Debug Files

If you encounter an error when compiling a program that requires you to contact OpenText Support for Micro Focus Products, your support representative might request that you provide additional debug files (as well as source and data files) to help us determine the cause of the problem. If so, they will advise you how to create them.

Copyright and Disclaimer

© Copyright 2024 Micro Focus or one of its affiliates.

The only warranties for this product and any associated updates or services are those that may be described in express warranty statements accompanying the product or in an applicable license agreement you have entered into. Nothing in this document should be construed as creating any warranty for a product, updates, or services. The information contained in this document is subject to change without notice and is provided "AS IS" without any express or implied warranties or conditions. Micro Focus shall not be liable for any technical or other errors or omissions in this document. Please see the product's applicable end user license agreement for details regarding the license terms and conditions, warranties, and limitations of liability.

Any links to third-party Web sites take you outside Micro Focus Web sites, and Micro Focus has no control over and is not responsible for information on third-party sites.