IDOL

Software Version 24.4

Windows and Linux

FIPS Enablement Technical Note

opentext™

Legal notices

Documentation updates

The title page of this document contains the following identifying information:

- Software Version number, which indicates the software version.
- Document Release Date, which changes each time the document is updated.
- Software Release Date, which indicates the release date of this version of the software.

To check for updated documentation, visit https://www.microfocus.com/support-and-services/documentation/.

Support

Visit the MySupport portal to access contact information and details about the products, services, and support that OpenText offers.

This portal also provides customer self-solve capabilities. It gives you a fast and efficient way to access interactive technical support tools needed to manage your business. As a valued support customer, you can benefit by using the MySupport portal to:

- View information about all services that Support offers
- Submit and track service requests
- Contact customer support
- Search for knowledge documents of interest
- View software vulnerability alerts
- Enter into discussions with other software customers
- Download software patches
- Manage software licenses, downloads, and support contracts

Many areas of the portal require you to sign in. If you need an account, you can create one when prompted to sign in.

Contents

Introduction

This technical note describes how to set up and run OpenText IDOL in a Federal Information Processing Standard (FIPS) compliant system.

IDOL uses a cryptographic module which complies with Federal Information Processing Standard 140-2 (FIPS 140-2). This standard defines the technical requirements that Federal Agencies must use for cryptographic-based security systems that protect sensitive or valuable data.

To comply with FIPS 140-2, OpenText IDOL:

- integrates validated and NIST-certified third party cryptographic modules, and uses the modules as the only providers of cryptographic services.

- uses FIPS-approved cryptographic functions.

- uses FIPS-approved and NIST-validated technologies

- uses security controls defined in NIST 800-53 (or applicable security controls such as DoD 8500.2), prescribed for cryptographic modules by FIPS 140-2 and applicable for OpenText IDOL design, implementation, and operation.

When using SSL in FIPS mode, all encrypted ACI communication between all IDOL components and HTTPS traffic between IDOL and third parties (where SSL is supported by the third party) is secured using the FIPS validated OpenSSL Module.

To review the OpenSSL FIPS certificate, refer to the NIST Website: OpenSSL FIPS certificate.

There are two options for running FIPS-enabled IDOL components:

- Use the standard installation components. In this case, the components use OpenSSL3. See Install and Configure FIPS Mode for Standard IDOL, on the next page.

- Use the separate FIPS-enabled Red Hat Enterprise Linux (RHEL) 7 and RHEL 8 platform downloads. In this case, the components use the system version of OpenSSL (expected to be in the 1.0.x series for RHEL7 and the 1.1.x series for RHEL8). See Install and Configure FIPS Mode for RHEL7 and RHEL8, on page 7.

Install and Configure FIPS Mode for Standard IDOL

The following topics describe how to enable FIPS on the standard versions of the IDOL components.

Install IDOL

To run the OpenSSL3 versions of IDOL components, you can download and install the standard IDOL packages for your platform.

For details of how to install your IDOL components, refer to the *IDOL Getting Started Guide*, or the documentation for the component that you want to install.

Configure Your IDOL System for FIPS

After you install the IDOL components, you must set environment variables to configure OpenSSL, and configure SSL communications for IDOL.

> **NOTE:** The `FIPSMode` configuration parameter does not have any effect when you have installed the standard versions of IDOL components.

To configure FIPS in your IDOL system

1. Set the following environment variables in your system:

   - `OPENSSL_CONF`. The location of an OpenSSL configuration file. The IDOL packages include a suitable sample configuration file, `IDOL_openssl_fips.cnf` in the `openssl` directory.

   - `OPENSSL_MODULES`. The directory that contains the FIPS shared library file. The IDOL packages include these files in the `openssl` directory.

   For more detailed information about OpenSSL configuration, refer to the OpenSSL3 Documentation.

2. Open your IDOL component configuration file in a text editor.

3. Configure SSL for your IDOL platform. You must configure SSL for incoming connections, and for connections between your IDOL components. All connections between your servers must be SSL encrypted (that is, you must configure SSL for both incoming and outgoing communications, where applicable).

   For details of how to configure SSL, refer to *IDOL Expert*, or the Administration Guide for your product. For example:

   ```
   [Server]
   SSLConfig=SSLOptions
   ```

```
[SSLOptions]
SSLMethod=TLSV1.2
SSLPrivateKey=/path/to/privatekey
SSLCertificate=/path/to/certificate
SSLCheckCommonName=True
SSLCACertificate=/path/to/certificate.authority.certificate
```

4. Save and close your configuration file.

5. Restart the component for your changes to take effect.

To verify that your IDOL system is now FIPS-enabled, see Verify FIPS Mode, on page 9.

Additional Configuration for NTLM

When your products interact with NTLM, you must use algorithms from the legacy provider. For more information, see the OpenSSL Legacy Provider documentation.

The IDOL packages include `legacy.dll` on Windows platforms, and `legacy.so` on all other platforms.

To use the legacy libraries for NTLM

- Set the `OPENSSL_MODULES` environment variables to include the directory that contains `legacy.dll` or `legacy.so`.

- (Windows only) Set the `PATH` environment variable to include the directory that contains the `libcrypto-3-x64.dll` library. This file is available as part of your IDOL component installation.

Install and Configure FIPS Mode for RHEL7 and RHEL8

The following topics describe how to enable FIPS for the RHEL7 and RHEL8 FIPS-enabled versions of the IDOL components.

Prerequisites

This section describes the prerequisites for installing IDOL in a FIPS-compliant system on RHEL7 and RHEL8, using the system OpenSSL libraries.

RHEL 7

You must install the FIPS version of IDOL on a Red Hat Enterprise Linux 7 platform that has FIPS mode enabled. For information about how to enable FIPS in RHEL7, see the following section of the Red Hat documentation:

https://access.redhat.com/documentation/en-US/Red_Hat_Enterprise_Linux/7/html/Security_Guide/chap-Federal_Standards_and_Regulations.html

RHEL 8

You must install the FIPS version of IDOL on a Red Hat Enterprise Linux 8 platform that has FIPS mode enabled. For information about how to enable FIPS mode, refer to the Red Hat documentation.

You must also install the package `compat-openssl10`. You can do this by running the following command:

```
yum install compat-openssl10
```

Install IDOL

To install and use IDOL in a FIPS-compliant system that uses the system OpenSSL libraries on RHEL7 and RHEL8, you must download the FIPS-enabled version of the installer or component ZIP package. The packages have a file name of the form:

*Product_Version*_LINUX_X86_64_RHEL7FIPS.[exe|zip]

Where *Product* is the product name, and *Version* is the version number.

For details of how to install your IDOL components, refer to the *IDOL Getting Started Guide*, or the documentation for the component that you want to install.

Configure IDOL

After you install the FIPS-enabled IDOL components, you must configure each component to use FIPS mode, and configure SSL communications for IDOL.

> **NOTE:** Even after you install the FIPS-enabled version of the component, you must explicitly configure FIPS mode to enable the functionality.

You can use the following procedure for any IDOL component for which a FIPS-enabled package is available.

To configure IDOL in FIPS mode

1. Open the component configuration file in a text editor.

2. Find the `[Service]` section, and add the `FIPSMode` parameter, set to `True`. For example:

   ```
   [Service]
   FIPSMode=True
   ```

3. Configure SSL for your IDOL platform. You must configure SSL for incoming connections, and for connections between your IDOL components. All connections between your servers must be SSL encrypted (that is, you must configure SSL for both incoming and outgoing communications, where applicable).

   For details of how to configure SSL, refer to *IDOL Expert*, or the Administration Guide for your product. For example:

   ```
   [Server]
   SSLConfig=SSLOptions

   [SSLOptions]
   SSLMethod=TLSV1.2
   SSLPrivateKey=/path/to/privatekey
   SSLCertificate=/path/to/certificate
   SSLCheckCommonName=True
   SSLCACertificate=/path/to/certificate.authority.certificate
   ```

4. Save and close your configuration file.

5. Restart the component for your changes to take effect.

To verify that your IDOL system is now FIPS-enabled, see Verify FIPS Mode, on the next page.

Verify FIPS Mode

After you install and configure your IDOL components, you can start the servers.

After the servers have started, you can verify that the component is running in FIPS mode by checking the application log. By default, this file is in the logs subdirectory of your component directory, with the file name `application.log`.

For example:

`/opt/IDOL/IDOLServer-13.0.0/content/logs/application.log`

When the component is successfully running in FIPS mode, this log has the following information line:

`Running with FIPS mode active`

Send documentation feedback

If you have comments about this document, you can contact the documentation team by email. If an email client is configured on this system, click the link above and an email window opens with the following information in the subject line:

Feedback on OpenText IDOL 24.4 FIPS Enablement Technical Note

Add your feedback to the email and click **Send**.

If no email client is available, copy the information above to a new message in a web mail client, and send your feedback to MFI-swpdl.idoldocsfeedback@opentext.com.

We appreciate your feedback!