IDOL

Software Version 23.2

OEM Licensing 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

Overview

The OEM licensing scheme restricts access to IDOL by applying ACI encryption to all requests, so that only the OEM application, which knows the encryption keys, can communicate with IDOL. This enables OpenText to provide a single license with no host or port restrictions that the OEM can distribute with all copies of their software. Even though the OEM license can be used to start IDOL on any machine, end users (customers of the OEM) cannot abuse this license because they do not have the encryption keys required to communicate with IDOL.

> **NOTE:** You can also operate ACI servers with an Enterprise OEM license. The Enterprise OEM license uses License Server to provide a standard license, and also includes an embedded OEM encryption key that allows optional ACI request encryption, without any additional configuration in your ACI components. When you use encryption for a request, it acts like OEM encryption (with an encrypted request and unencrypted response).
>
> This option provides a way for you to migrate an OEM system to the standard licensing model without requiring you to immediately change existing applications that use OEM encryption.

Restrictions

- Unlike a standard License Server-based license, there are no host, IP, MAC address or port restrictions on the OEM license.

- ACI communication is possible only between the OEM application and the IDOL component, or between the IDOL components that share the OEM license. This is enforced by using ACI encryption.

- Index and service port actions are not restricted by any form of encryption.

Setting Up Licensing

All ACI communication actions sent to IDOL components in an OEM-licensed environment must be ACI encrypted. IDOL components access the `licensekey.dat` file to determine the encryption keys required to decode encrypted action.

> **NOTE:** You must not use the `CommsEncryptionType` and `CommsEncryptionTEAKeys` (deprecated) configuration parameters to encrypt ACI communications because the key would be publicly available.

IDOL components also require a `versionkey.dat` file, which determines the versions of the component that the license can run.

To set up licensing in an OEM environment

- Encrypt ACI communications between IDOL components and the front-end application by making the appropriate API call in your application and passing in the OEM encryption keys that were provided to you. For example:

  In the C API, you could make the following call:

  ```
  const char* szKeys = "MjR8CJCUGcb4RbRdNDKbK9RXX3pEswAiZ";
  aciInitEncryption(TRUE, "TEA", szKeys);
  ```

  where the value of `szKeys` is the encryption key provided with the license.

  In the Java API, you could make the following call:

  ```
  BteaEncryptionCodec encryptionCodec = new BteaEncryptionCodec(
      "MjR8CJCUGcb4RbRdNDKbK9RXX3pEswAiZ");
  aciServerDetails.setEncryptionCodec(encryptionCodec);
  ```

- Redistribute the `licensekey.dat` and `versionkey.dat` files with your application by copying them to the working directory of each IDOL component. The IDOL components then read the license from the `licensekey.dat` instead of the `[License]` section of the component's configuration file.

  The `licensekey.dat` file is generated by OpenText and provided to you along with your license.

  You can download `versionkey.dat` from the Software Licenses and Downloads portal (SLD), in the License Server package or as a standalone download package. You must download a new `versionkey.dat` when you upgrade your IDOL components.

- Unlike standard ACI encryption, the ACI responses from the IDOL component are not encrypted by default. You can optionally encrypt the response returned by an IDOL component by setting the `EncryptResponse` action parameter to **True** in the ACI action you run. However, in most cases OpenText recommends that you use SSL/TLS for secure communications.