IBM Cognos 8
Enhanced Encryption Module for OpenSSL

Version 8.4.1

Installation and Configuration Guide

Information Management software

Product Information

This document applies to IBM Cognos 8 Version 8.4.1 and may also apply to subsequent releases. To check for newer versions of this document, visit the IBM Cognos Information Centers (http://publib.boulder.ibm.com/infocenter/cogic/v1r0m0/index.jsp).

Copyright

Table of Contents

Introduction

This document is intended for use with IBM Cognos 8. IBM Cognos 8 is a Web-based business intelligence solution with integrated reporting, analysis, scorecarding, and event management features.

This document provides instructions for installing the IBM Cognos Enhanced Encryption Module for OpenSSL and for configuring the module to work with an existing security infrastructure, such as Entrust. IBM Cognos 8 comes with standard encryption and other features to ensure that IBM Cognos 8 communications and sensitive data are secure. If you purchase the IBM Cognos Enhanced Encryption Module for OpenSSL, you can replace the standard IBM Cognos 8 encryption with enhanced encryption, which uses up to a 168-bit key to encrypt data. For environments using the Entrust security infrastructure, you must purchase and install the Entrust security infrastructure before you install the IBM Cognos Enhanced Encryption Module for OpenSSL.

Audience

To use this guide, you should have basic Windows and UNIX administration skills and be familiar with your Entrust encryption infrastructure.

Related Documentation

Our documentation includes user guides, getting started guides, new features guides, readmes, and other materials to meet the needs of our varied audience. The following documents contain related information and may be referred to in this document.

Note: For online users of this document, a Web page such as **The page cannot be found** may appear when clicking individual links in the following table. Documents are made available for your particular installation and translation configuration. If a link is unavailable, you can access the document on the IBM Cognos Resource Center (http://www.ibm.com/software/data/support/cognos_crc.html).

Document	Description
IBM Cognos 8 Installation and Configuration Guide	Installing, upgrading, configuring, and testing IBM Cognos 8, changing application servers, and setting up samples

Finding Information

Product documentation is available in online help from the **Help** menu or button in IBM Cognos products.

To find the most current product documentation, including all localized documentation and knowledge base materials, access the IBM Cognos Resource Center (http://www.ibm.com/software/data/support/cognos_crc.html).

You can also read PDF versions of the product readme files and installation guides directly from IBM Cognos product CDs.

Using Quick Tours

Quick tours are short online tutorials that illustrate key features in IBM Cognos product components. To view a quick tour, start IBM Cognos Connection and click the **Quick Tour** link in the lower-right corner of the Welcome page.

Getting Help

For more information about using this product or for technical assistance, visit the IBM Cognos Resource Center (http://www.ibm.com/software/data/support/cognos_crc.html). This site provides information on support, professional services, and education.

Printing Copyright Material

You can print selected pages, a section, or the whole book. You are granted a non-exclusive, non-transferable license to use, copy, and reproduce the copyright materials, in printed or electronic format, solely for the purpose of operating, maintaining, and providing internal training on IBM Cognos software.

Chapter 1: IBM Cognos Enhanced Encryption Module for OpenSSL

The IBM Cognos Enhanced Encryption Module for OpenSSL is a separate IBM Cognos product that replaces the standard encryption libraries that come with IBM Cognos 8 with enhanced versions. Enhanced encryption libraries are packaged separately to adhere to government regulations controlling the export of encryption mechanisms.

Use enhanced encryption when a threat-risk analysis or other assessment of your security risks indicates a need for stronger security. In such an environment, it is also recommended that you use another certificate authority from Microsoft or Sun.

If you use another certificate authority, it should be in place before you install and then configure the enhanced encryption module in IBM Cognos Configuration. For environments using the Entrust security infrastructure, any additional third-party components should also be in place.

Important: If you run your IBM Cognos 8 product in a 64-bit application server environment, an Entrust security infrastructure is not supported.

Cryptographic services are used by IBM Cognos 8 components. The cryptographic services include:

- secure socket layer (SSL) services, to ensure that a conversation between two parties has not been tampered with in transit and to optionally allow for that conversation to be encrypted
- a method to ensure that some BI bus messages are not tampered with in transit
- a common symmetric key (CSK) that is shared between components
- mechanisms to encrypt and decrypt data using the CSK
- encryption of temporary files on disk to protect sensitive information during processing

Chapter 2: Installing and Configuring the IBM Cognos Enhanced Encryption Module for OpenSSL

You can install the IBM Cognos Enhanced Encryption Module for OpenSSL on Windows or UNIX. It must be installed on each computer that contains an IBM Cognos 8 component, such as the gateway, servers, Content Manager, and Framework Manager.

Important: After you install the IBM Cognos Enhanced Encryption Module for OpenSSL and configure IBM Cognos 8 to use enhanced encryption, you cannot return to standard encryption.

The process for installing enhanced encryption depends on your situation.

If you just installed IBM Cognos 8 and want to install enhanced encryption at the same time, do the following:

❏ Install the IBM Cognos Enhanced Encryption Module for OpenSSL (p. 11).

❏ Configure IBM Cognos 8 to use enhanced encryption (p. 15).

If you already use IBM Cognos 8 with standard encryption and you want to add enhanced encryption, do the following:

❏ Export data (p. 9).

❏ Install the IBM Cognos Enhanced Encryption Module for OpenSSL (p. 11).

❏ Configure IBM Cognos 8 to use enhanced encryption (p. 15).

❏ Import data (p. 20).

Export Data

If you install the IBM Cognos Enhanced Encryption Module for OpenSSL at the same time as you install IBM Cognos 8, you do not need to export data.

When you change from standard to enhanced encryption, existing data remains encrypted using the standard encryption keys. Any new data that you create is encrypted using the enhanced encryption keys.

You may choose to keep standard encryption for your existing data. IBM Cognos 8 can use the data as before.

If you choose to encrypt your existing data again using the enhanced encryption keys, you must export all the data in your content store to a deployment archive before you install the IBM Cognos Enhanced Encryption Module for OpenSSL. After the module is installed and you configure IBM

Cognos 8 to use enhanced encryption, you must import the data from the deployment archive back into your content store.

Steps

1. In the source environment, open IBM Cognos Administration.
2. On the **Configuration** tab, click **Content Administration.**
3. On the toolbar, click the new export button .
4. Type a unique name and, if you want, a description and screen tip for the deployment specification. Select the folder where you want to save it, and click **Next**.

   By default, this name is used for the new deployment archive. If you want to keep this name for the new archive, we recommend that you do not use spaces in the name.
5. Click **Select the entire content store**, select the check box to include user account information, and click **Next**.

   If you do not include user account information, you lose your folders and credentials information.
6. In the **Specify a deployment archive** page, under **Deployment archive**, select **New archive**.
7. If you want to use a name other than the default, type a name for the deployment archive.

   Tip: We recommend that you do not use spaces in the name.

   If the name matches the name of an existing deployment archive, the characters _# are appended.
8. If you want to secure the archive, under **Encryption**, click **Set the encryption password**, type a password, and click **OK**.
9. Click **Next.**

   The summary information appears.

   Tip: If you want to change information, click **Back** and follow the instructions.
10. Click **Next.**
11. In the **Select an action** page, select **Save and run once** and then click **Finish**.
12. In the **Run with options** page, select the time option and then click **Run**.
13. In the IBM Cognos 8 page, if you want to view the deployment record, select the **View the details of this export after closing this dialog** check box.
14. Click **OK**.

    IBM Cognos 8 exports the content you specified to the deployment archive and saves the deployment specification. This may take a few minutes.
15. When the export is done, the deployment archive appears on the Administration page.

The location where deployment archives are saved is set in the configuration tool. The default location is *c8_location*/deployment.

You can now install the IBM Cognos Enhanced Encryption Module for OpenSSL.

Installing the IBM Cognos Enhanced Encryption Module for OpenSSL

You install the IBM Cognos Enhanced Encryption Module for OpenSSL from the IBM Cognos Encryption Module for OpenSSL CD.

As part of the installation of the Enhanced Encryption Module for OpenSSL, you are prompted to specify which components to install. The components depend on your encryption environment. For environments other than those that use the Entrust security infrastructure, the components include:

- OpenSSL Encryption Connection Provider

  This component contains encryption enhancements that are used by all IBM Cognos 8 components. It must be installed on each computer that contains an IBM Cognos 8 component, including the gateway, servers, Content Manager, and Framework Manager.

- OpenSSL Enabled Gateway

  This component contains encryption enhancements that the gateway uses. It must be installed on the gateway computer.

IBM Cognos 8 respects the file mode creation mask (umask) of the account running the installation program. This affects the installation directories only. It does not affect the file permissions within the directories. However, run-time generated files, such as logs, respect the umask. We recommend umask 022 for the installation directory.

For an up-to-date list of the software environments supported by IBM Cognos products, see the IBM Cognos Customer Service Center (http://www.ibm.com/software/data/support/cognos_crc.html). The support site includes information about operating systems, system requirements, patches, browsers, Web servers, directory servers, database servers, OLAP servers, and more.

Before installing the IBM Cognos Enhanced Encryption Module for OpenSSL, do the following:

- Install a certificate authority (CA), if you are using one.

  For Entrust, install the Entrust security infrastructure.

  For instructions about installing or using your CA, see the documentation provided with it.

- Install and configure IBM Cognos 8.

  For instructions, see the *Installation and Configuration Guide*.

- For Entrust, create a separate Public Key Infrastructure (PKI) account in Entrust for each IBM Cognos 8 installation.

Steps for UNIX

1. Mount the IBM Cognos Enhanced Encryption Module for OpenSSL CD with Rock Ridge file extensions.

Important: To mount the IBM Cognos CD on HP-UX, do the following:

- Add the pfs_mount directory in your path.

  For example,

  PATH=/usr/sbin/:$PATH

  export PATH

- To start the required NFS daemons and run the daemons in the background, type

  bg pfs_mountd and then type **bg pfsd**

- To mount the drive, type

  pfs_mount -t rrip <device><mount_dir> -o xlat=unix

  For example,

  pfs_mount /dev/dsk/c0t2d0 /cdrom -o xlat=unix

  You can now install or copy files as a non-root user using an IBM Cognos CD from this drive.

- When the installation is complete, type **pfs_umount /cdrom** and kill the pfsd and pfs_mountd daemons to unmount the CD.

2. Go to the directory that is appropriate for your operating system and start the installation:

   - If you use X Windows, type

     ./issetup

   - Otherwise, type

     ./issetupcc

3. Follow the directions in the installation wizard and copy the required files to your computer.

4. Choose how to proceed in the **Finish** page of the installation wizard:

   - If you want to view the transfer log or the summary-error log, click the appropriate **View** button.

   - If you want to see late-breaking information about IBM Cognos 8, select **View the Readme** and then select **Finish**.

     Tip: For character-mode installations on UNIX and Linux, close the readme text file by pressing Crtl + C or q.

5. Check whether the following .jar files exist in *JRE_location*/lib/ext:

   - sunjce_provider.jar

   - US_export_policy.jar

   - local_policy.jar

   - bcprov-jdk14-134.jar

Tip: An example of the installation location of a Java Runtime Environment is /*directory*/java/*java_version*/jre.

These files must be present in your Java Runtime Environment (JRE) before you can use the cryptographic operations, such as data encryption and key management, implemented by IBM Cognos 8.

6. If any .jar files are missing from *JRE_location*/lib/ext or if the files already exist in this location because they were copied as part of an IBM Cognos 8 installation, go to *series8_location*/bin/jre/*version*/lib/ext directory and copy the appropriate .jar files to the *JRE_location*/lib/ext directory.

7. Select the language to use for the installation.

8. Follow the directions in the installation wizard to copy the required files to your computer.

9. In the **Finish** page of the installation wizard:

   - If you want to view the transfer log or the summary-error log, click the appropriate **View** button.

   - If you want to see late-breaking information about IBM Cognos components, click **View the Readme**.

10. Click **Finish**.

You must now configure IBM Cognos 8 to use enhanced encryption (p. 15).

Steps for Windows

1. Insert the IBM Cognos Enhanced Encryption Module for OpenSSL CD.

   If the Welcome page does not appear, in the win32 directory on the CD, double-click the issetup.exe file.

2. Select the language to use for the installation, and click **Next**.

3. Follow the instructions to copy the required files to your computer.

   Important: If you have a distributed installation, the files must be installed on all computers where a Cognos 8 component is installed.

4. In the **Finish** page of the installation wizard:

   If you want to view the transfer log or the summary-error log, click the appropriate **View** button.

   If you want to see late-breaking information about IBM Cognos components, click **View the Readme**.

5. Click **Finish**.

You must now configure IBM Cognos 8 to use enhanced encryption (p. 15).

Uninstall the IBM Cognos Enhanced Encryption Module for OpenSSL

To uninstall the IBM Cognos Enhanced Encryption Module for OpenSSL, you must uninstall the IBM Cognos 8 BI server components. This is required if you no longer require IBM Cognos 8 or are upgrading to new software.

Steps for UNIX or Linux

1. If the console attached to your computer does not support a Java-based graphical user interface, determine the process identification (pid) of the IBM Cognos 8 process by typing the following command:

   ps -ef | grep cogbootstrapservice

2. Stop the IBM Cognos 8 process:

   - If you run XWindows, start IBM Cognos Configuration, and from the **Actions** menu, click **Stop**.
   - If you do not run XWindows, type:

     kill -TERM pid

3. To uninstall IBM Cognos 8, go to the *c8_location*/uninstall directory and type the appropriate command:

   - If you use XWindows, type

     ./uninst -u

   - If you do not use XWindows, type

     ./uninstcc -u

4. Follow the prompts to begin the uninstallation.

5. When you are prompted to select the packages you want to uninstall, click the check box for **IBM Cognos 8 Business Intelligence Server** and then click **Next**.

6. Continue following the prompts to complete the uninstallation.

   When the uninstallation is complete, you are prompted to restart the computer.

7. Delete all temporary Internet files.

Steps for Windows

1. From the **Start** menu, click **Programs, IBM Cognos 8, Uninstall IBM Cognos 8**.

   The **Uninstall** wizard appears.

   Tip: IBM Cognos 8 is the default name of the Program Folder that is created during the installation. If you chose another name, go to that folder to find the program.

2. Follow the prompts to begin the uninstallation.

3. When you are prompted to select the packages you want to uninstall, click the check box for **IBM Cognos 8 Business Intelligence Server** and then click **Next**.

4. Continue following the prompts to complete the uninstallation.

   When the uninstallation is complete, you are prompted to restart the computer.

   The Cognos_uninst_log.htm file records the activities that the Uninstall wizard performs while uninstalling files.

   Tip: To find the log file, look in the Temp directory.

5. Delete all temporary Internet files.

   For more information, see your Web browser documentation.

   Uninstalling does not remove any files that changed since the installation, such as configuration and user data files. Your installation location remains on your computer, and you retain these files until you delete them manually.

Configure IBM Cognos 8 to Use Enhanced Encryption

After installing IBM Cognos Enhanced Encryption Module for OpenSSL, you must configure IBM Cognos 8 to use the new encryption features.

In installations that have standard encryption, you have a choice of algorithms that use a 40-bit key or a 56-bit key. When you install the IBM Cognos Enhanced Encryption Module for OpenSSL, you have a choice of algorithms with a range from 40 bits to 168 bits. To encrypt your data using enhanced encryption keys, you must select one of the algorithms that does not use a 40-bit key.

In addition, the number of supported ciphersuites increases when you install the IBM Cognos Enhanced Encryption Module for OpenSSL. A ciphersuite provides the quality of protection for the connection. It contains cryptographic, authentication, hash, and key exchange algorithms. The SSL protocol selects the highest priority suite that the client and the server both support.

Configure IBM Cognos 8 in Entrust Security Infrastructures to Use Enhanced Encryption

To configure IBM Cognos 8 to use enhanced encryption for the Entrust security infrastructure, you:

- delete the IBM Cognos cryptography component that came with IBM Cognos 8
- add a new cryptography component for the Entrust encryption solution
- specify resource properties for the new component

Ensure that the key store passwords match the one in your Entrust Profile (EPF).

To prevent gateway errors, ensure that the Internet Guest Account has read and write permission to the Entrust .epf file and read permission to the Entrust .ual file.

Steps

1. Start IBM Cognos Configuration.

2. In the **Explorer** window, under the **Security** group, click **Cryptography**.
3. In the **Properties** window, under **Advanced algorithm settings**, change the **Digest algorithm** to the appropriate message digest or secure hash algorithm for your security policy.
4. If you want to change the default **Signing key pair algorithm**, do so.

   The key size for each value automatically changes from 512 bits to 1024 bits when you install the enhanced encryption module.
5. In the **Explorer** window, under the **Security** group and the **Cryptography** component, right-click the **IBM Cognos** resource, and click **Delete**.
6. Under the **Security** group, right-click **Cryptography**, and click **New resource**, **Provider**.
7. In the **Name** field, type a name for the encryption service you are creating.
8. In the **Type** field, click the arrow, and click **Entrust**, and then click **OK**.

   A branch with the name you assigned appears below **Cryptography**.
9. Click the branch you created.

   Resource properties appear in the properties window.
10. In the **Properties** window, enter the appropriate values.

Property	Description
INI file location	The location of the Entrust initialization file (.ini).
Identity file distinguished name (DN)	The distinguished name associated with the profile of the Entrust identity.
Identity file location	The location of the Entrust identity profile file (.epf). A file should exist for each installation of IBM Cognos 8.
Use Entrust Server Login	The parameter that controls whether users must enter a password to log on to the Entrust PKI.
Identity file password	The password users must enter if the Use Entrust Server Login property is False. The password must match the one in your Entrust Profile (EPF).

Property	Description
Confidentiality algorithm	The level of encryption that is required to comply with your security policy: • Advanced Encryption Standard with Cipher Block Chaining (CBC) Mode - 128 bits • Data Encryption Standard with Cipher Block Chaining (CBC) Mode - 56 bits • RSA security RC2 - 128 bits • RSA security RC2 (40-bit key) • Triple DES/DES EDE (Encrypt-Decrypt-Encrypt) - 168 bits
PDF Confidentiality algorithm	The encryption algorithm to use when encrypting PDF data.
Supported ciphersuites	The cipher suites that are supported in your security environment. Remove the ones that are not applicable and change the priority of the remaining cipher suites by moving them up or down in the list so that the strongest cipher suites are at the top of the list. We recommend that you do not mix standard (40 to 56 bits) cipher suites with strong (128 to 168 bits) cipher suites.
Signing Key Store Location	The location of the key store that contains the signing key pairs.
Encryption Key Store Location	The location of the key store that contains encryption key pairs.

Important: Record your passwords in a secure location.

11. From the **File** menu, click **Save**.

When you save your properties, or exit IBM Cognos Configuration, IBM Cognos Configuration:

- checks for errors and configuration integration
- generates cryptographic information
- checks the integrity of your encryption data
- backs up configuration files
- saves configuration parameters
- saves global information

- registers the IBM Cognos 8 service

If the properties contain errors, they are not saved. You must correct the errors before proceeding.

Configure SSL

If you use the Secure Socket Layer (SSL) for IBM Cognos components, you must also enable SSL in the application server environment. You then identify the SSL server certificate to IBM Cognos components. For information about enabling SSL for IBM Cognos components, see the *Installation and Configuration Guide*. For information about configuring the application server to use SSL, refer to the application server documentation and your certificate authority documentation, if necessary.

Configure IBM Cognos 8 in Non-Entrust Environments to Use Enhanced Encryption

To configure IBM Cognos 8 to use enhanced encryption in environments that do not use the Entrust security infrastructure, you:

- choose the security algorithm for your security policy
- specify resource properties for the security policy

Steps

1. Start IBM Cognos Configuration.
2. In the **Explorer** window, under the **Security** group, click **Cryptography**.
3. In the **Properties** window, under **Advanced algorithm settings**, change the **Digest algorithm** to the appropriate message digest or secure hash algorithm for your security policy.
4. If you want to change the default **Signing key pair algorithm**, do so.

   The key size for each value automatically changes from 512 bits to 1024 bits when you install the enhanced encryption module.
5. In the **Explorer** window, under **Security**, **Cryptography**, click **IBM Cognos**.
6. In the **Properties** window, change the **Confidentiality algorithm** and **Supported ciphersuites** properties to a value that complies with your security policy.

Property	Description
Confidentiality algorithm	The level of encryption that is required to comply with your security policy. ● Advanced Encryption Standard with Cipher Block Chaining (CBC) Mode - 128 bits ● Data Encryption Standard with Cipher Block Chaining (CBC) Mode - 56 bits ● RSA security RC2 - 128 bits ● RSA security RC2 (40-bit key) - 40 bits ● RSA security RC4 - 128 bits ● RSA security RC4 (40-bit key) - 40 bits ● Triple DES/DES EDE (Encrypt-Decrypt-Encrypt) - 168 bits
PDF Confidentiality algorithm	The encryption algorithm to use when encrypting PDF data.
Supported ciphersuites	The cipher suites that are supported in your security environment. Remove the ones that are not applicable and change the priority of the remaining cipher suites by moving them up or down in the list so that the strongest cipher suites are at the top of the list. We recommend that you do not mix standard (40 to 56 bits) cipher suites with strong (128 to 168 bits) cipher suites.

7. From the **File** menu, click **Save**.

   When you save your properties, or exit IBM Cognos Configuration, IBM Cognos Configuration

   - checks for errors and configuration integration
   - generates cryptographic information
   - checks the integrity of your encryption data
   - backs up configuration files
   - saves configuration parameters
   - saves global information
   - registers the IBM Cognos 8 service

If the properties contain errors, they are not saved. You must correct the errors before proceeding.

If you exported data that is encrypted using standard encryption keys, you must now import the data back into IBM Cognos 8 to encrypt the data using enhanced encryption keys.

Import Data

You import data using the IBM Cognos 8 deployment tool. You fill in a deployment specification, and then you import the data from the deployment archive.

If you install the IBM Cognos Enhanced Encryption Module for OpenSSL at the same time as you install IBM Cognos 8, you do not need to import data.

Steps

1. In the source environment, open IBM Cognos Administration.

2. On the **Configuration** tab, click **Content Administration**.

3. Click the new import button.

4. In the **Deployment archive** box, click the deployment archive that you want to import and then click **Next**.

5. If you are prompted to enter the encryption password, type the password and click **OK**.

6. Type a unique name and, if you want, a description and screen tip for the deployment specification. Select the folder where you want to save it, and click **Next**.

7. When the **Select the Content Store options** page appears, select the check box to include user account information, and click **Next**.

   The summary information appears.

8. Click **Next**.

9. In the **Select an action** page, select **Save and run once** and then click **Finish**.

10. In the **Run with options** page, select the time option, select whether to upgrade or keep the report specification version, and then click **Run**.

11. In the IBM Cognos 8 page, if you want to view the deployment record, select the **View the details of this import after closing this dialog** check box.

12. Click **OK**.

    IBM Cognos 8 imports the content you specified to the deployment archive and saves the deployment specification. This may take a few minutes.

    If the **View run history details** page appears, you can monitor the import until it is complete. If you click **Close**, the import continues in the background.

13. To check if the import is complete, do the following:

- In the **Administration** page, in the **Actions** column for the deployment specification, click **More**.
- Click **View run history**.
- Check if the **Status** column shows Succeeded.

Upgrading the IBM Cognos Enhanced Encryption Module for OpenSSL

You must use the IBM Cognos 8 Enhanced Encryption Module for OpenSSL with IBM Cognos 8. If you are using a version of the IBM Cognos Enhanced Encryption Module for OpenSSL prior to IBM Cognos 8, you must upgrade to IBM Cognos 8.

Index