

# Fujitsu Enterprise Postgres 18 for x86 - Advanced Edition with Cryptographic Module

## Read First

Linux

# Preface

---

## Purpose of this document

This document provides an overview of the Fujitsu Enterprise Postgres Advanced Edition with Cryptographic Module, its features, and how to install it.

Read this before using Fujitsu Enterprise Postgres Advanced Edition with Cryptographic Module.

## Intended readers

This document is intended for use with Fujitsu Enterprise Postgres Advanced Edition with Cryptographic Module.

## Structure of this document

The structure and content of this manual is shown below.

### [Chapter 1 Fujitsu Enterprise Postgres Advanced Edition with Cryptographic Module Basics](#)

Describes an overview of the Fujitsu Enterprise Postgres Advanced Edition with Cryptographic Module, its features, and how to install it.

### [Appendix A Installation and Uninstallation \(Compatibility\)](#)

Describes how to install and uninstall in an interactive mode.

## Export restrictions

Exportation/release of this document may require necessary procedures in accordance with the regulations of your resident country and/or US export control laws.

## Issue date and version

Edition 1.0: December 2025
----------------------------

## Copyright

Copyright 2024-2025 Fujitsu Limited

# Contents

---

Chapter 1 Fujitsu Enterprise Postgres Advanced Edition with Cryptographic Module Basics.....	1
1.1 Feature Differences from Fujitsu Enterprise Postgres Advanced Edition.....	1
1.2 Operating Environment.....	2
1.2.1 Required Operating System.....	2
1.3 Install.....	2
1.4 Setup.....	3
1.5 Uninstall.....	4
1.6 Application Development.....	4
Appendix A Installation and Uninstallation (Compatibility).....	5
A.1 Install.....	5
A.2 Uninstall.....	6

# Chapter 1 Fujitsu Enterprise Postgres Advanced Edition with Cryptographic Module Basics

Fujitsu Enterprise Postgres Advanced Edition with Cryptographic Module is a product that is configured to use algorithms that are approved by the security requirements for cryptographic modules (FIPS 140), one of the FIPS (Federal Information Processing Standard) standards.

The Fujitsu Enterprise Postgres Advanced Edition with Cryptographic Module provides the same feature as the Fujitsu Enterprise Postgres Advanced Edition.

This chapter describes the differences between Fujitsu Enterprise Postgres Advanced Edition with Cryptographic Module and Fujitsu Enterprise Postgres Advanced Edition regarding the features, operating environment, installation, setup, and application development.

## 1.1 Feature Differences from Fujitsu Enterprise Postgres Advanced Edition

### Encryption features

If you use a cryptographic module provided by Fujitsu Enterprise Postgres Advanced Edition with Cryptographic Module, you cannot use algorithms and parameters not approved for FIPS 140, so the following cryptographic functionality differences exist:

- Saving Passwords in md5 format on the server  
Use the default scram-sha-256.
- Some algorithms and parameters used to connect and authenticate using SSL  
Not only are they not available as encryption algorithms for communication paths, but they are also not available as signature algorithms for certificates, encryption algorithms for encrypting and storing private keys, and so on. Additionally, X25519 cannot be used as the elliptic curve for ECDH key exchange (key establishment).  
Fujitsu Enterprise Postgres 18 adds X25519 as the default elliptic curve for ECDH key exchange. Therefore, when using SSL with Fujitsu Enterprise Postgres Advanced Edition with Cryptographic Module 18, specify a value for the "ssl\_groups" parameter (which defines the elliptic curves used for ECDH key exchange) that does not include X25519.
- The following are not available
  - md5 in SQL functions
  - Some algorithms of the extension module pgcrypto
  - Some functions of the extension module uuid-ossip

Algorithms not approved for FIPS 140

Classification	Details
Algorithms	BF, CAST, DES, DESX, IDEA, RC2, RC4, RC5, SEED, ARIA, CAMELLIA, SM4
Digest	MD2, MD4, MDC2, DES, RIPEMD-160, WHIRLPOOL, BLAKE2, SM3, MD5, MD5-SHA1
MAC	BLAKE2, CMAC, KMAC, POLY1305, SIPHASH
KDF	KBKDF, KRB5KDF, SCRYPT, X942KDF, X963KDF
Asymmetric keys	RSA-PSS, RSA-OAEP, SM2
Asymmetric encryption	RSAES-OAEP

### Application development

JDBC driver and .NET Data Provider

Prepare the Java or .NET runtime required for your application to work with the JDBC driver and the .NET Data Provider. The implementation of the encryption algorithms used to connect these applications to the database server is provided by the respective runtimes.

## Features not provided

- Windows client(32bit)

## 1.2 Operating Environment

---

Describes the operating environment for Fujitsu Enterprise Postgres Advanced Edition with Cryptographic Module.

### 1.2.1 Required Operating System

---

One of the operating systems shown below is required in order to use Fujitsu Enterprise Postgres Advanced Edition with Cryptographic Module.

- RHEL8.6 or later minor version
- RHEL9.2 or later minor version
- SLES 15 SP4 or later minor version

#### Using RHEL

To use the JDBC driver, WebAdmin, and the database multiplexing feature, the following packages are required in addition to those listed in the "Required Operating System" in the Fujitsu Enterprise Postgres Installation and Setup Guide for Server.

- java-17-openjdk

For the RHEL versions listed below, please install the version listed or later.

- RHEL 8.6: 17.0.5.0.8-3.el8\_6 or later
- RHEL 8.7: 17.0.5.0.8-4.el8\_7 or later

#### Using SLES

To use the JDBC driver, WebAdmin, and the database multiplexing feature, the following packages are required in addition to those listed in the "Required Operating System" in the Fujitsu Enterprise Postgres Installation and Setup Guide for Server.

- java-17-openjdk

#### When SELinux is enabled

If the boolean selinuxuser\_execstack is off (allow\_execstack is off) in an SELinux-enabled environment, programs that directly or indirectly link cryptographic modules provided by Fujitsu Enterprise Postgres Advanced Edition with Cryptographic Module may not work correctly. These programs include Fujitsu Enterprise Postgres server and client commands and application programs that link libpq or libecpg. Set up SELinux to grant execstack rights to these programs.

## 1.3 Install

---

Describes the install for Fujitsu Enterprise Postgres Advanced Edition with Cryptographic Module.

### Install

To use Fujitsu Enterprise Postgres Advanced Edition with Cryptographic Module, you must install the cryptographic module. Install version 3 of the cryptographic module on each machine on which you want to install the following Fujitsu Enterprise Postgres Advanced Edition with Cryptographic Module features:

- Server feature
- Pgpool-II
- pgBackRest
- Client feature

The method for installing the encryption module varies depending on the platform on which the product is being implemented.

- Linux

Install the encryption package (rpm).

The path of the package and storage directory for the cryptographic module is shown below.

Package	Package storage directory
FJSVfsep-crypto-*.rpm	CRYPTO64/Linux/packages/<os>

<os> is the operating system of the runtime environment. Depending on the runtime environment, refer to either RHEL8, RHEL9, or SLES15.

\* is the version, OS, etc.

- Windows

Install using the installer.

The installation directory name for the encryption module is shown below.

Platform	Installation directory
Linux	/opt/fsepcryptov3
Windows	C:\Program Files\Fujitsu\fsepcryptov3

The disk space required to install the cryptographic module is 60 megabytes.

For more information on how to install, refer to the Fujitsu Enterprise Postgres Installation and Setup Guide for Server and the Fujitsu Enterprise Postgres Installation and Setup Guide for Client.



### Note

You should not specify the openssl\_conf and openssl\_modules parameters in postgresql.conf.

## 1.4 Setup

Describes the setup for Fujitsu Enterprise Postgres Advanced Edition with Cryptographic Module.

### Using the WebAdmin

When using WebAdmin, you need to set up WebAdmin. Additionally, Java runtime is required when setting up WebAdmin. Prepare the Java runtime and set the JAVA\_HOME environment variable to the installation location of the OpenJDK 17 Java runtime.

Example)

```
# export JAVA_HOME="Installation location of JRE 17"
```

For setup using the WebAdminSetup command, refer to "Setting Up WebAdmin" in the Fujitsu Enterprise Postgres Installation and Setup Guide for Server.

### Using the database multiplexing feature

If you want to take advantage of the database multiplexing feature, you need a Java runtime.

Prepare the OpenJDK 17 Java runtime and set the JAVA\_HOME environment variable to where the Java runtime environment will be installed.

Example)

```
# export JAVA_HOME="Installation location of JRE 17"
```

If Mirroring Controller connects to an instance with SSL, set the following in the server definition files of the primary server and standby server. For more information, refer to "Creating, Setting, and Registering the Primary Server Instance" in the Fujitsu Enterprise Postgres Cluster Operation Guide(Database Multiplexing).

- db\_instance\_ext\_jdbc\_conninfo

If you are using a Red Hat build of OpenJDK on RHEL to connect via SSL, or if you are using the OpenJDK that comes with SLES to connect via SSL, add the following to your connection parameters:

```
sslfactory=org.postgresql.ssl.DefaultJavaSSLFactory
```

Use the NSS database for storing certificates and private keys. To enable the JDBC driver to access the NSS database, specify the properties you want to specify for the JVM startup options in the environment variable JAVA\_TOOL\_OPTIONS.

## 1.5 Uninstall

---

Describes the uninstall for Fujitsu Enterprise Postgres Advanced Edition with Cryptographic Module.



### Information

.....  
If installed in interactive mode, refer to "[A.2 Uninstall](#)" and uninstall in interactive mode.  
.....

After uninstalling the following features of Fujitsu Enterprise Postgres Advanced Edition with Cryptographic Module, uninstall the cryptographic module.

- Server feature
- Pgpool-II
- pgBackRest
- Client feature

For more information on how to uninstall, refer to the Fujitsu Enterprise Postgres Installation and Setup Guide for Server and the Fujitsu Enterprise Postgres Installation and Setup Guide for Client.

## 1.6 Application Development

---

Describes the application development for Fujitsu Enterprise Postgres Advanced Edition with Cryptographic Module.

### Applications using the JDBC driver

If you are using a Red Hat build of OpenJDK on RHEL to connect via SSL, or if you are using the OpenJDK that comes with SLES to connect via SSL, add the following to your connection parameters:

```
sslfactory=org.postgresql.ssl.DefaultJavaSSLFactory
```

Use the NSS database as the keystore and truststore. Specify the JVM startup options so that the JDBC driver can access the NSS database.

# Appendix A Installation and Uninstallation (Compatibility)

Describes how to install and uninstall Fujitsu Enterprise Postgres Advanced Edition with Cryptographic Module in an interactive mode.



See

For details on installation and uninstallation, refer to the following.

- "Installation and Uninstallation (Compatibility)" in the Fujitsu Enterprise Postgres Installation and Setup Guide for Server
- "Installation and Uninstallation of the Linux Client (Compatibility)" in the Fujitsu Enterprise Postgres Installation and Setup Guide for Client

## A.1 Install

Describes the install for Fujitsu Enterprise Postgres Advanced Edition with Cryptographic Module.

### Advance preparation (for RHEL)

If you use WebAdmin, you need the Java runtime to set up WebAdmin.

WebAdmin can be set up when installing Fujitsu Enterprise Postgres Advanced Edition with Cryptographic Module. Before installation, prepare the Java runtime and set the JAVA\_HOME environment variable to the Java runtime installation location.

Example)

```
# export JAVA_HOME="/JREInstallDir"
```

You can also be set up after installation using the WebAdminSetup command. Before setup, prepare the Java runtime and set the JAVA\_HOME environment variable to the Java runtime installation location. For information about set up using the WebAdminSetup command, refer to "Setting Up WebAdmin" in the Fujitsu Enterprise Postgres Installation and Setup Guide for Server.

### Advance preparation (for SLES)

Before installation, specify the installation directory of JRE 8 in the JAVA\_HOME environment variable. If you specify OpenJDK 1.8 that comes with SLES, specify -Dcom.suse.fips=false in the JAVA\_TOOL\_OPTIONS environment variable, export it, and then install it. After installation, specify an empty string in the JAVA\_TOOL\_OPTIONS environment variable and export it.

Example)

```
# JAVA_TOOL_OPTIONS=-Dcom.suse.fips=false ./install.sh
```

If you set up WebAdmin during installation, after installation, change the Java runtime used by WebAdmin to OpenJDK 17. For instructions on changing the JRE after installation, refer to "Procedure when Modifying the JRE Installation" in the Fujitsu Enterprise Postgres Installation and Setup Guide for Server.

### Install

To use Fujitsu Enterprise Postgres Advanced Edition with Cryptographic Module, you must install the cryptographic module. Install version 3 of the cryptographic module on each machine on which you want to install the following Fujitsu Enterprise Postgres Advanced Edition with Cryptographic Module features:

- Server feature
- Pgpool-II
- pgBackRest
- Client feature



## A.2 Uninstall

---

Describes the uninstall for Fujitsu Enterprise Postgres Advanced Edition with Cryptographic Module.

### **Advance preparation (for SLES)**

Before uninstallation, make sure that JRE 8 is installed and export the JAVA\_HOME environment variable. If you want to specify OpenJDK 1.8 that comes with SLES, specify -Dcom.suse.fips=false in the JAVA\_TOOL\_OPTIONS environment variable, export it, and then uninstall. After uninstalling, specify the JAVA\_TOOL\_OPTIONS environment variable as an empty string and export it.