

# White paper

## Fujitsu Security Solution AuthConductor™ Client

---

### Development Background

- “Multiple passwords are impossible for employees to remember and troublesome to enter.”
- “The process for recovering forgotten passwords is complicated.”
- “Unauthorized access may lead to confidential information leakage.”

As a solution to these and other issues, Fujitsu has been providing biometric authentication solutions as an alternative to ID and password authentication since 1999, and has developed a variety of supporting sensor technology. We not only address the operation of individual user terminals, but also provide a consolidated solution for management of user (employee) access by IT administrators and implementation of the access policy for confidential information sites and systems.

In order to respond to global market needs, Fujitsu AuthConductor™ Client has been developed from the ground up with a architecture that reflects all our accumulated know-how and a re-evaluation of ease of usability. While continuing to offer the strength of its easy “add on” deployment that does not require tinkering with the customer’s current system and trademark convenience, this new global-ready solution enables syncing with centralized management by Windows Active Directory.

### Fujitsu Advantages

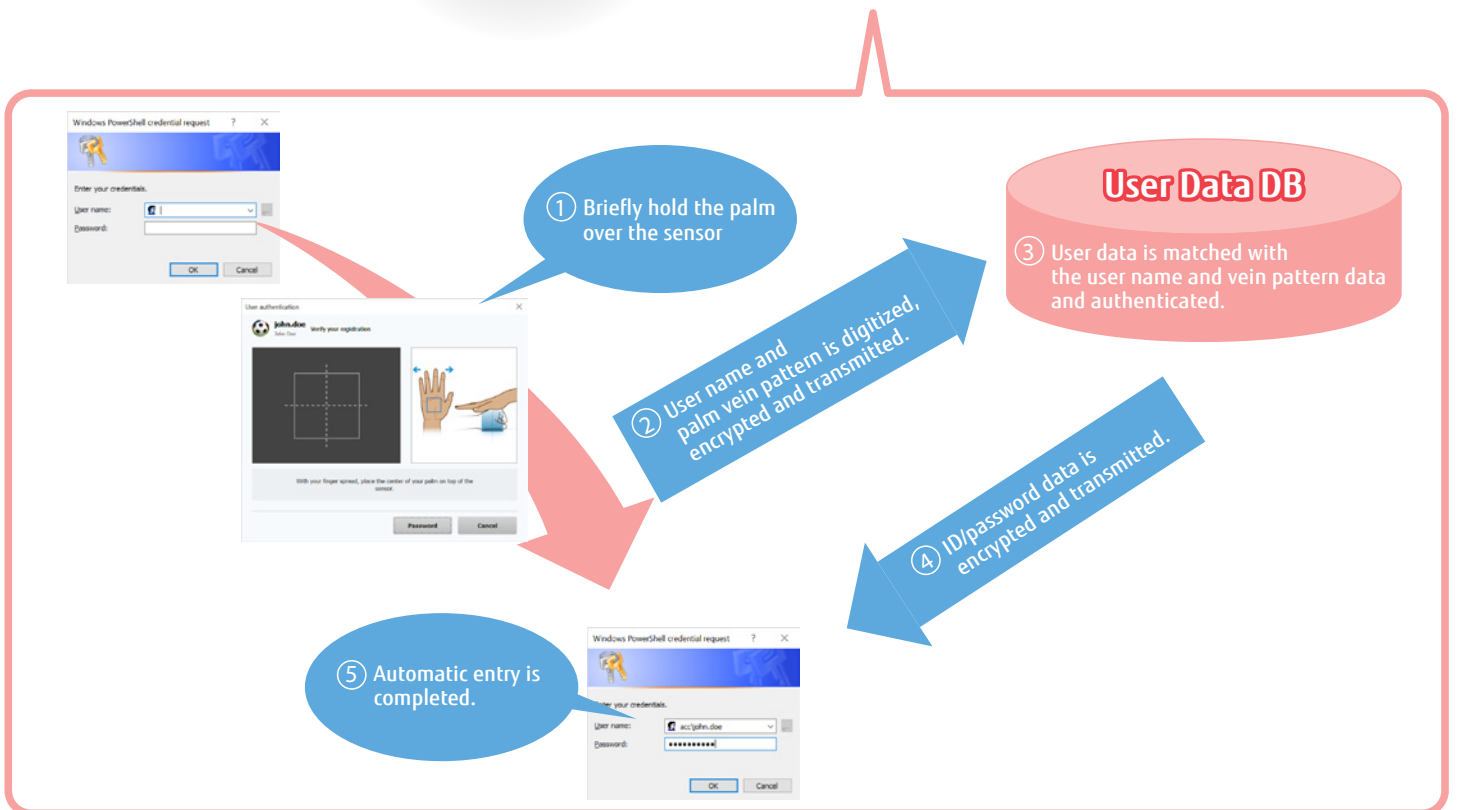
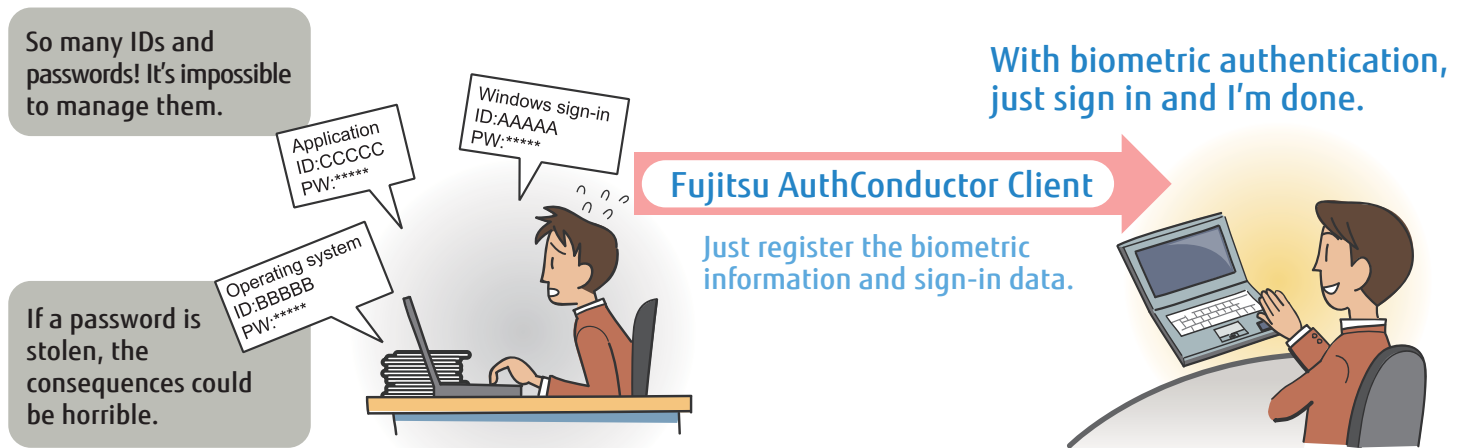
- In-house development (from basic research to device provision)
  - Speedy provision of ever improved products is the result of our ability to closely coordinate and synergize the efforts of our “Basic Research”, “Sensor Device Development/Production” and “PC Development/Production” units.
- Sole manufacturer fully supporting both “fingerprint” and “palm vein patten” authentication.
  - For customers with a mixed operational environment of both fingerprint and palm vein authentication and other operational circumstances, Fujitsu can provide a variety of solution proposals tailored to budgetary and other needs.
- Know-how backed by a long and proven record of achievements
  - Fujitsu has producing fingerprint sensors for PCs since 1999. Among the many manufacturers of personal computers, Fujitsu was the first to provide a biometric authentication product.
  - Currently Fujitsu annually ships over 500,000 PCs that are equipped with a fingerprint sensor as a standard feature.
  - Through our provision of diverse solutions, Fujitsu can leverage a wealth of cumulative know-how.
- Tackling total solutions as a system maker

As a creator of system solutions, Fujitsu plans to provide total solutions that use biometrics in the future.

- Consolidated management of a fusion of diverse ID/password management systems, etc.

### Product Profile

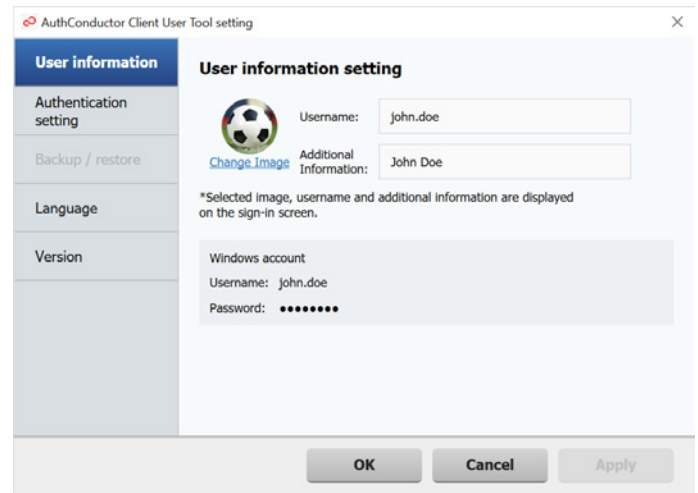
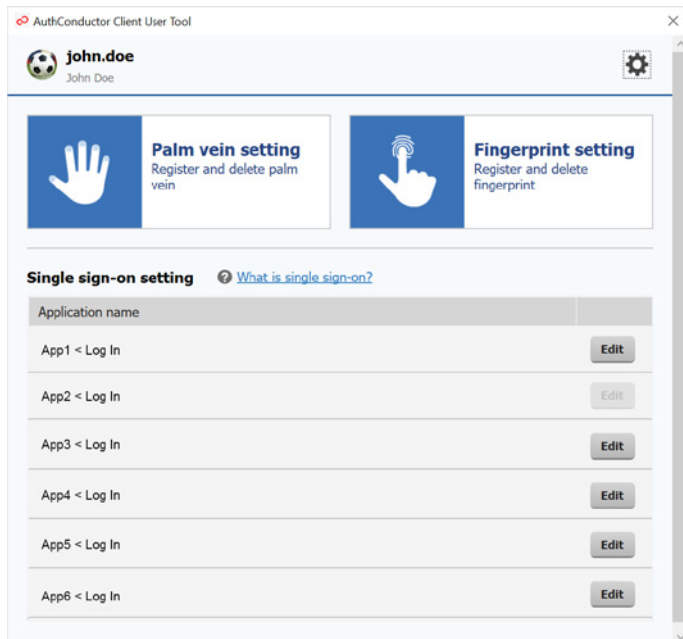
Fujitsu Security Solution AuthConductor™ Client is a consolidated biometric authentication software solution that realizes Single Sign-on (SSO) by using replacing conventional manual ID/password entry with palm vein or fingerprint sensor scanning to log into Windows, various types of applications and websites. The central consolidated management solution eliminates the need for administrators to set passwords for users and for users to memorize them, nor is there any more concerns about forgotten passwords or information leakage risk. The add-on architecture means that there is no need to modify applications or to make changes in the existing system. The simply deployment is a big advantage of this solution.



## Customer Benefits

Just by deploying this solution/software, customers can immediately begin enjoying the following benefits:

- For each PC user (employee)
  - Elimination of the need to memorize multiple combinations of IDs and passwords.
  - By using AuthConductor(TM) Client to set Single Sign-on (SSO) access, users can automatically log on Windows\* and multiple systems and applications with just a single and simple log-on operation.  
\*In the LIFEBOOK/STYLISTIC series of notebook PCs, BIOS password entry can also be substituted with biometric authentication.
  - Elimination of the necessity of periodically updating of passwords.
- For system administrators and information system departments
  - Reduced risk of password leakage since general user awareness of passwords for system operation is not necessary.
  - Elimination of tasks required for recovery/reissuance of passwords forgotten by general users.
  - Reduction of work load due to elimination of management tasks associated with periodic password updating including promoting implementation by general users.
  - Elimination of administrative tasks associated with the management of IDs and passwords for each of the various systems.
  - Log acquisition simplifies sure confirmation of activity by users in the event of an audit and can also serve as an effective measure to prevent internal fraud and crime.
  - Central consolidated management of general user IDs and passwords and swift addition/deletion of specific user data from the management menu. Termination of temporary/provisional access is simple.
- Other benefits
  - Optimization of the UI (User Interface) enables easy selection of major functions from the Main Screen, and the arrangement of the various setting screens is logical and easy to understand.



Possible mixed use of security devices (vein sensor, fingerprint sensor)

Product lineup

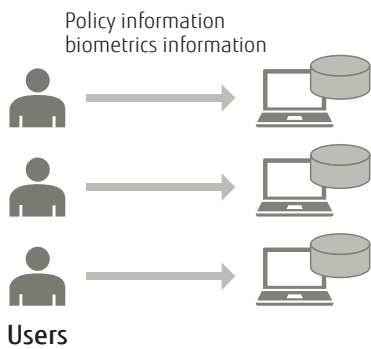
Fujitsu offers the following solution lineup with choices to fit the customer's desired deployment scale. Each can be smoothly deployed without any large-scale changes to the customer's existing system.

■ Software

Fujitsu AuthConductor™ Client Basic	Fujitsu AuthConductor™ Client Premium	Fujitsu AuthConductor™ Client Premium for Active Directory
<b>For Individuals, Family office</b>	<b>For SME with Local Administrator</b>	<b>For LA with Central Administrator</b>

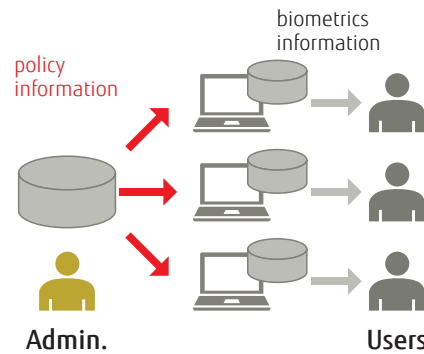
Focus on convenience

- The users register biometrics information and manage by themselves.
- Low cost, No need to construct a system



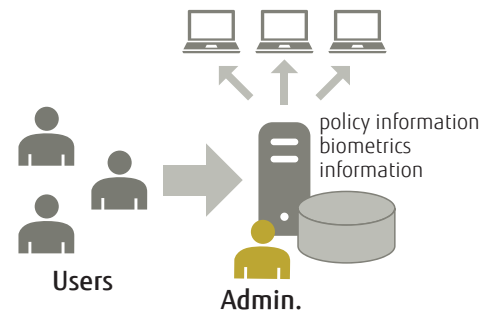
Set up by administrator and operated by user

- Administrator provides a terminal and software with preset information.
- No need to design the network infrastructure



The administrator manages consolidated authentication information.

- Multiple user who has registered authentication can operate each terminal.
- Managing access logs.



No Administrator	Managed by Administrator
Policy settled for each terminal.	Policy setting could be centralized
Biometrics information is stored to each terminal	stored to server
PC bundled	Software Product

■ Main types of compatible vein sensors



Integrated palm vein sensor in LIFEBOOK/STYLISTIC



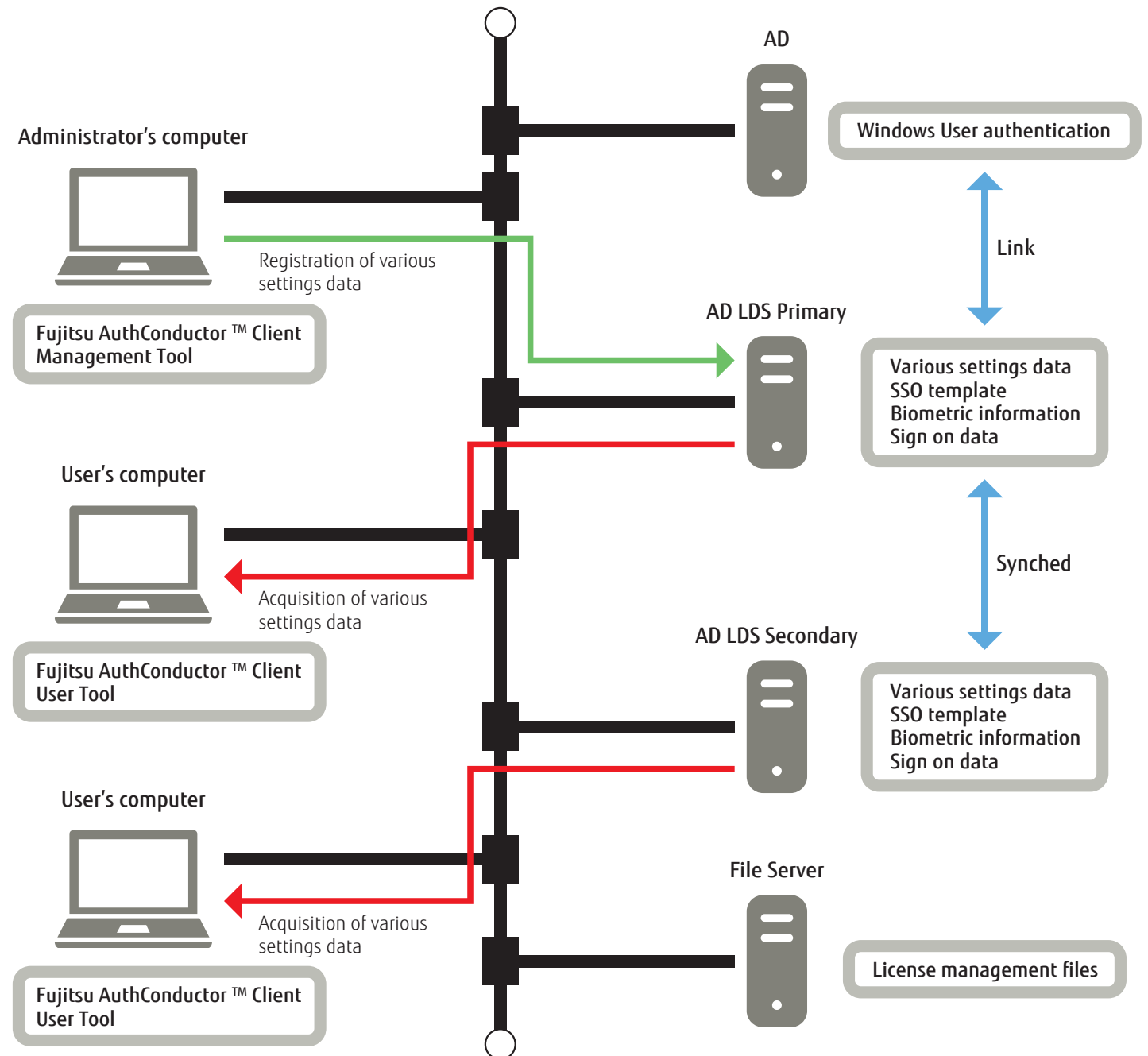
PalmSecure-F Pro Standard



PalmSecure-F Pro Mouse

### System configuration(Fujitsu AuthConductor™ Client Premium for Active Directory)

The diagram below shows the system configuration for consolidated management with Fujitsu AuthConductor™ Client synced with Windows Active Directory. Active Directory accounts currently in operation at the customer's enterprise are used as is, and Single Sign-on (SSO) to Windows and various applications is enabled using biometric authentication. Administrators use the Management Tool to easily perform the various types of settings including settings for the user's permitted scope of functionality and Single Sign-on access. Consolidated management of the various settings is executed in the AD LDS, and when users use their User Tool, AD LDS acquires the various settings and controls the range of the User Tool Activity.



### Palm vein authentication benefits and the Fujitsu advantage

Fujitsu's original palm vein authentication sensor makes possible high accuracy, dependable authentication. Palm vein authentication is the simple, highly reliable method to authenticate identity. This is based on biometric information which is the most reliable way to accurately confirm an individual's identity, and the veins in the palm of the hand are especially appropriate for this method. The vein pattern of each individual is unique – even in the case of identical twins.

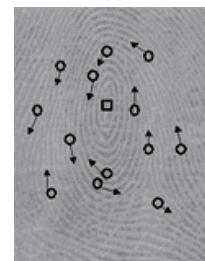
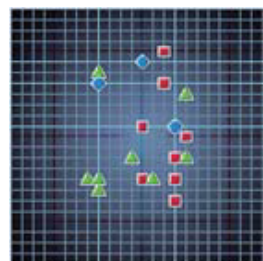
- Because the scanning and authentication of biometric information requires zero contact with the sensor device, the process is very hygienic. Low user resistance or hesitation to use the device and broad applicability of the system in a diversity of scenes makes it ideal. (Fujitsu original advantage)
- High-speed authentication is possible just by the natural motion of briefly holding the palm over the sensor.
- Thicker veins and the large number of veins in the palm make possible the high degree of accuracy and stability of authentication. (False acceptance rate of less than 0.00008% in the case of PalmSecure sensor V2)
- Biometric information is internal to the body, making forgery extremely difficult. Moreover, the authentication process only functions with hemoglobin is flowing in the veins.
- High responsiveness enables dependable authentication unaffected by the palm condition.
- Solutions are backed by over 10 years of proven performance in businesses including financial institutions that demand the highest security and reliability.

### Fingerprint authentication benefits and the Fujitsu advantage

The history of the development of fingerprint authentication is long, and the technology is quite mature. Because it is relatively low in cost and easy to use, it has achieved mainstream status as a method of biometric authentication.

- Provided in LIFEBOOK notebook PCs (both as a standard feature and a customer made option)
- Fujitsu's originally developed Characteristic Point Extraction Method converts the fingerprint pattern into special point registration data. The captured fingerprint image is not saved nor can it be reconstructed from the point registration data. Fingerprint authentication is achieved with a high degree of accuracy. (false acceptance rate is less than 0.001%\*).

\*In the case of a solution using the latest hardware and software.



**Characteristic data are analyzed and extracted from the fingerprint pattern and recorded.**

\*It is impossible to reconstruct the image data from the registered data.

○:Center  
 □:Key point  
 ↗:Whorl direction

## Contact Us

### HONG KONG

Fujitsu Business Technologies Asia Pacific Ltd.  
 Tel: (852) 3910-8228  
 Email: fpc.hksales@hk.fujitsu.com  
 hk.fujitsu.com/pc

### SINGAPORE

Fujitsu Asia Pte Ltd.  
 Tel: (65) 6710-5403  
 Email: info@sg.fujitsu.com  
 sg.fujitsu.com/pc

### CHINA

FUJITSU (CHINA) HOLDINGS CO.,LTD. - PC  
 CHINA DIVISION  
 Tel: (86) 21-26079126  
 Email: fpcacn.support@cn.fujitsu.com  
 cn.fujitsu.com/pc

### INDONESIA

Pt. Fujitsu Indonesia  
 Tel: (62) 21-570-9330  
 Email: callcenter@id.fujitsu.com  
 id.fujitsu.com/pc

### PHILIPPINES

Fujitsu Philippines, Inc.  
 Tel: (63) 2-841-8488  
 Email: info@ph.fujitsu.com  
 ph.fujitsu.com/pc

### MALAYSIA

Fujitsu (Malaysia) Sdn. Bhd  
 Tel: (60) 3-8230-4188  
 Email: askfujitsu@my.fujitsu.com  
 my.fujitsu.com/pc

### TAIWAN

Fujitsu Taiwan Ltd.  
 Tel: (886) 02-2311-2255  
 Email: lifebook@tw.fujitsu.com  
 tw.fujitsu.com/pc

### THAILAND

Fujitsu (Thailand) Co., Ltd.  
 Tel: (66) 0-2302-1500  
 Email: info@th.fujitsu.com  
 th.fujitsu.com/pc

### VIETNAM

Fujitsu Vietnam Limited (Hanoi)  
 Tel: (84) 4-2220-3113  
 Email: sales@vn.fujitsu.com  
 vn.fujitsu.com/pc

© Copyright 2018 Fujitsu Business Technologies Asia Pacific Ltd.

Fujitsu, the Fujitsu logo and Fujitsu brand names are trademarks or registered trademarks of Fujitsu Limited in Japan and other countries. Other company, product and service names may be trademarks or registered trademarks of their respective owners, the use of which by third parties for their own purposes may infringe the rights of such owners. Technical data are subject to modification and delivery subject to availability. Any liability that the data and illustrations are complete, actual or correct is excluded. Designations may be trademarks and/or copyrights of the respective manufacturer, the use of which by third parties for their own purposes may infringe the rights of such owner. All rights reserved.