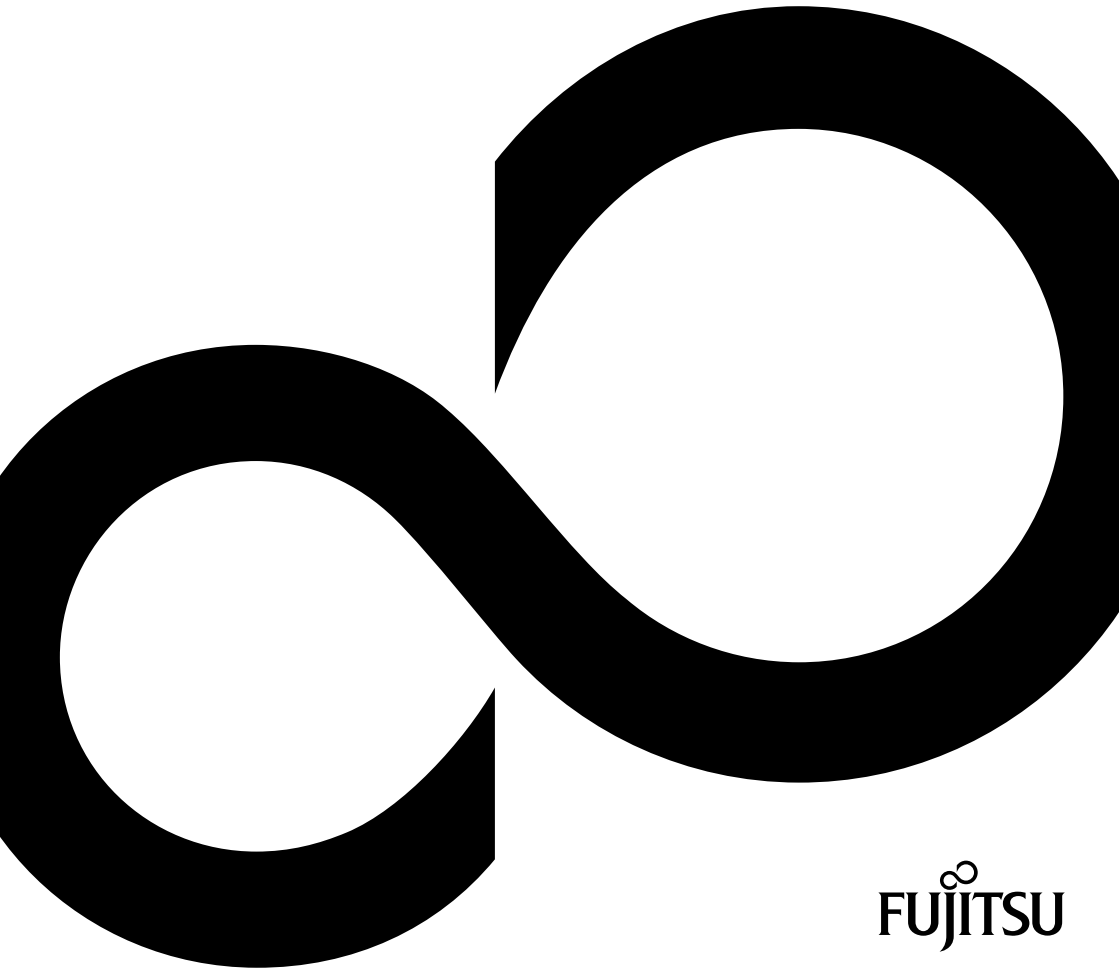


Workplace Protect



Thank you for buying an innovative product from Fujitsu

The latest information about our products, tips, updates etc. can be found on the Internet at:
"<http://www.fujitsu.com/fts/>"

You can find driver updates at: *"<http://support.ts.fujitsu.com/download>"*

If you have any technical questions, please contact:

- our Hotline/Service Desk *"<http://support.ts.fujitsu.com/contact/servicedesk>"*
- Your authorized sales partner
- your sales outlet

We hope you enjoy using your new software from Fujitsu!



Published by / Contact address in the EU

Fujitsu Technology Solutions GmbH

Mies-van-der-Rohe-Straße 8

80807 Munich, Germany

<http://www.fujitsu.com/fts/>

Copyright

© Fujitsu Technology Solutions GmbH 2016. All rights reserved.

Edition date

08/2016

Order no.: A26361-F2727-Z323-1-7619, edition 4

Workplace Protect

Operating Manual

About Workplace Protect	3
Important notes	5
Installation Workplace Protect	6
Overview of the user interface	11
Security settings	14
Setting the security devices	23
Applications	34
Using the security functions of Workplace Protect	50
TFTP server	52
Manufacturer's notes	55

Remarks

Notes on the product description are consistent with the design specifications from Fujitsu and are made available for comparison purposes. The actual results may differ because of several factors. Technical data is subject to change without notification. Fujitsu does not accept any responsibility for technical or editorial errors or omissions.

Trade marks

Fujitsu, the Fujitsu logo and PalmSecure are registered trademarks of Fujitsu Limited or its subsidiaries in the United States of America and other countries.

Microsoft and Windows are trademarks or registered trademarks of Microsoft Corporation in the United States and/or other countries

All other trademarks mentioned here are the property of their particular owner.

Copyright

No part of this publication may be copied, reproduced or translated without previous written permission from Fujitsu.

No part of this publication may be stored or transmitted in any electronic manner without written permission from Fujitsu.

Contents

About Workplace Protect	3
Notational conventions	4
Important notes	5
Installation Workplace Protect	6
Requirements	6
Workplace Protect – install managed mode on the computers in the network.....	6
Workplace Protect – managed mode in Workplace Manager	8
Uninstall administered computers in the network	8
Install Workplace Protect in local mode	8
Repair Workplace Protect.....	9
Uninstall Workplace Protect	10
Uninstall Workplace Protect using Setup	10
Uninstall Workplace Protect through Windows	10
Overview of the user interface	11
Start screen	11
Menus / Functions	12
Set the language	13
Perform the necessary authentication in Workplace Protect.....	13
Security settings	14
Authentication levels.....	14
Authentication Levels in the local mode	15
Authentication Levels in the managed mode	16
Biometric data on the smartcard	16
Pre-Boot Authentication.....	16
Activate and configure SystemLock	17
Unlocking a PC locked with SystemLock	18
Fingerprint PBA activation and configuration	19
Deactivate Fingerprint PBA	19
Enabling and configuring PalmSecure™ PBA	20
Disabling PalmSecure™ PBA	20
Authentication configuration	21
Application settings.....	22
Setting the security devices	23
PalmSecure™ palm vein imaging	24
Read in palm	24
Make fingerprint settings	25
Read in fingerprint.....	25
Face recognition settings.....	26
Editing the face recognition settings.....	28
Licence settings for face recognition	28
Presence sensor settings	29
Changing the password settings	29
Changing the Windows password	29
Changing the BIOS password.....	30
Deleting a BIOS password	30
Changing the hard disk password.....	31
Smartcard	31
Insert the smartcard	31
The smartcard is valid and contains login details.....	31

Contents

The status of the smartcard is unknown. The smartcard must be unlocked using the PIN.....	31
The smartcard is not supported.....	31
Configuring a SmartCard.....	31
Changing the SmartCard settings.....	32
Configure RFID card.....	32
Log off or lock session.....	33
Applications.....	34
Using Password Safe.....	34
Creating a new Password Safe database.....	34
Importing existing Password Safe database.....	35
Deleting an existing Password Safe database.....	35
Creating a new group.....	36
Using Encrypted Container.....	39
Create new Encrypted Container / Prepare new drive.....	39
Reintegrate the Encrypted Container (mount).....	40
Unmounting an Encrypted Container (unmount).....	41
Edit existing Encrypted Container.....	41
Delete the existing Encrypted Container / Drive.....	41
Export drive key.....	42
Importing Encrypted Container File (VHD).....	42
Easy Restore.....	43
Start Easy Restore.....	44
Create data backup.....	45
Configure the server for backup/restore.....	47
Download boot image (Windows PE).....	49
Restoring data.....	49
Using the security functions of Workplace Protect.....	50
Log on to the system again.....	50
Log on to the system using a password.....	50
Log on to the system with biometric authentication options.....	50
Log on to the system with SmartCard.....	51
TFTP server.....	52
Setting up the TFTP server.....	52
Manufacturer's notes.....	55
Open Source Software in Workplace Protect.....	55

About Workplace Protect

The main purpose of the *Workplace Protect* software package is the protection of the network, the individual computers and data from unauthorised access.

Function	Description
User authentication for Microsoft Windows	Authentication by: <ul style="list-style-type: none"> • <i>PalmSecure™</i> (palm recognition) • <i>SmartCard</i> • <i>Fingerprint</i> • <i>RFID card</i> • <i>Face recognition</i>
Pre-boot authentication	Authentication at the BIOS level by using <ul style="list-style-type: none"> • Fingerprints - only for LIFEBOOK, • Palm vein recognition - only for LIFEBOOK, • Smartcard (SystemLock)
Single Sign On to Microsoft Windows	The passing on of login details from the BIOS login system to the operating system as an additional option for pre-boot authentication
Password Safe	Secure storage of login data
Encrypted Container	Encoded storage that is made available to the user as a virtual drive
Easy Restore	Backup the computer and easily restore the contents of the hard disk

These operating instructions provide detailed information about the use of this product, which is available in two forms:

- Local mode: local installation on one computer, where the user must make many settings him or herself in consultation with the system administrator.
- Managed mode: Installation on a network, where the system administrator centrally configures the functions for the computers in the network.

Please read the instructions through carefully and enjoy the powerful functions of *Workplace Protect*.

Notational conventions



Pay particular attention to texts marked with this symbol. Failure to observe this warning destroys the system, or may lead to loss of data. The warranty will be invalidated if the system becomes defective through failure to take notice of this warning.



Indicates important information which is required to use the system properly



indicates an activity that must be performed

This font

indicates data entered using the keyboard in a program dialogue or command line, e.g. your password (`Name123`) or a command used to start a program (`start.exe`)

This font

indicates information that is displayed on the screen by a program, e.g.: **The installation is complete.**

This font

indicates product names, Internet addresses and the names of system components.

"This font"

indicates names of chapters and terms that are being emphasised.

Important notes



Workplace Protect can only be run under the *Windows 7*, *Windows 8.1* and *Windows 10* operating systems.

As soon as a wizard has been run through once, a tick is shown in the corresponding icon.

To be able to use the various security devices, the particular device must be recognised by the operating system and the matching device driver installed.

You can receive driver updates via *DeskUpdate* or from <http://support.ts.fujitsu.com/download>.

For *PalmSecure*[™] drivers, use the search option with the term *PalmSecure*.

If you have any technical questions, please contact our Hotline/Service Desk (<http://support.ts.fujitsu.com/contact/servicedesk>).



The images in this manual are examples and may be different to those produced by your system, depending on configuration and mode.

Installation Workplace Protect



You will find the installation package for *Workplace Protect*

- on the Internet at <http://fujitsu.com/fts/support>
- with DeskUpdate

Requirements



Please read the release notes for *Workplace Protect*, these may contain more up-to-date information than this manual.

Hardware

Fujitsu Computer, see Feature Finder on the Internet <http://www.fujitsu.com/fts/solutions/high-tech/solutions/workplace/manageability/feature-finder.html> (search term *Workplace Protect*).

SmartCard readers, if SmartCards are to be processed (e.g. for *SystemLock*).

Biometric devices on the computers in the network where login is required with fingerprint, face or palm recognition.

Operating system

Windows 7, *Windows 8.1* (32 Bit or 64 Bit) and *Windows 10* (64 Bit) with the current operating system updates. Depending on the operating system, use the 32-bit or 64-bit version of the software *Workplace Protect*.



Uninstall *Workplace Protect* before you upgrade the operating system to *Windows 10*.

Fujitsu drivers

Before performing the installation, you must ensure that the latest Fujitsu drivers for biometric devices and the SmartCard reader as well as current BIOS versions are installed on the computers so that they operate correctly.

Internet access

Internet access is required to activate licenses for face recognition.

Workplace Protect – install managed mode on the computers in the network

First install the *Workplace Manager* software and there import the computers in the network to which the *Workplace Protect - managed mode* should be distributed. You will find a detailed description of the installation and import in the manual for *Workplace Manager*.



Make sure all computers that should be managed are visible in the group *All computers* (see the *Workplace Manager* manual).

The installation requires administrative rights.



Installation on the managed computers in the network causes *Workplace Manager agents* and an enhanced login mechanism (*Windows Login*) to be installed. These support face recognition, SmartCards, palm recognition (PalmSecure™) and password entry.

The *Windows 8 and 8.1 Picture Password* and *PIN Password* login methods are disabled.

- To distribute the program, use the procedure that is general practice in your network.

The following example shows an unattended distribution of the software to the computers in the network. The unattended installation is executed automatically. Nothing needs to be entered in the dialog boxes.

The following command is entered in the command line (%WPM_HOSTNAME% must first be replaced by the name of the server on which the *Workplace Manager* is installed):

```
WorkplaceProtect64_Setup.exe /s /v"/qn
WPM_MANAGED=1 WPM_HOSTNAME=%WPM_HOSTNAME%
WPM_SERVERPORT=3298 WPM_CLIENTPORT=3298 REBOOT=ReallySuppress"
```

The information means the following:

Command/information	Description
WPM_MANAGED=1	Command to the Setup to install a <i>Managed Client</i> .
WPM_HOSTNAME	Name of the server on which the <i>Workplace Manager</i> is installed.
WPM_SERVERPORT	Value of the server port which was assigned during the installation (standard value 3298).
WPM_CLIENTPORT	Value of the client port which was assigned during the installation (standard value 3298).
REBOOT=ReallySuppress	Suppresses a restart of the managed computer after installation.

If you have already installed a previous version of Workplace Protect, you can also use the upper command line for the update. Also take care here that the ports are set as for the previous installation.



If the software is installed on the computers in the network, the computers register themselves with *Fujitsu Workplace Manager Server*.

The computers which have logged onto the server will be displayed, after an import of the computers (see the manual for *Workplace Manager*) in the work area *Registered Computers* (see the manual for *Workplace Manager*).

Computers with which there are problems when registering on the server are recorded in the *Registration problems* list (see *Workplace Manager* manual).

The installation of the computers managed in the network is completed.



Please make sure that users restart their computers after installation.

Recommendation: Installation at night and restart afterwards.

Workplace Protect – managed mode in Workplace Manager

If *Workplace Protect* is installed in local mode on a computer in the network, this version is converted into a managed mode of *Workplace Manager* by the installation described above.

In this version, the user at the computer in the network can no longer enter all the usual settings. The recording of biometric data and the use of the *Encrypted Container* and *Password Safe* are allowed (if use is not ruled out by the administrator). You will find more information about these functions in the *Workplace Protect* operating manual.

The following settings are assigned:

- Lock the computer when the SmartCard is withdrawn. This setting can be changed via a *Windows Group Policy*.
- The password settings are pre-set in the *Workplace Manager* so that *Workplace Protect* remembers the authentication password for the entire session of *Workplace Protect*.

Uninstall administered computers in the network



Access to the *Encrypted Container* or the *Password Safe* is not possible after uninstalling *Workplace Protect* on the computers.

Therefore tell your users to make a note of the passwords from the *Password Safe* and that they should back up the files from the *Encrypted Container* before uninstalling *Workplace Protect* on the computers.

Install Workplace Protect in local mode



You require administrative rights for the installation of *Workplace Protect*.

To install *Workplace Protect*, proceed as follows:

- ▶ Depending on the operating system platform, double-click on the file *WorkplaceProtect32_Setup.exe* or on the file *WorkplaceProtect64_Setup.exe*.
- ▶ In the *User account control* dialog window, click on *Yes*.
- ▶ The *Workplace Protect* installation wizard is shown.
- ▶ Follow the instructions on the screen.
- ▶ Confirm the license conditions.
- ▶ Enter the desired installation directory or use the default installation directory.



In the *Target directory* window, you can change the installation directory for *Workplace Protect*.

The standard installation directory is:

`%ProgramFiles%\Fujitsu\WorkplaceProtect.`

- ▶ Confirm with *Next*.
- ▶ Click on *Install*.

The installation process starts.

You will be asked to restart the system to finish the installation.

- ▶ Confirm with *Yes*.

The system will restart.

Repair Workplace Protect

If the installation was damaged by *Workplace Protect*, you can repair it.

A repair will be required, for example, if files which are needed are accidentally deleted, or if drivers are installed later which access *Workplace Protect*.



The settings and the user data are retained.

Proceed as follows to repair the *Workplace Protect* installation:

- ▶ Depending on the operating system platform, double-click on the file `WorkplaceProtect32_Setup.exe` or `WorkplaceProtect64_Setup.exe`.

The installation wizard starts.

- ▶ In the *Program maintenance* window, select the *Repair program* option and confirm with *Next*.
- ▶ Click on *Install*.

The components already installed will be repaired, for instance missing files will be reinstalled.

You will be asked to restart the system to finish the installation.

- ▶ Confirm with *Yes*.

Uninstall Workplace Protect

Uninstall Workplace Protect using Setup



If you are going to uninstall *Workplace Protect*, first of all export the access data for the *Encrypted Container* and *Password Safe* applications, otherwise this data will be lost (see chapters "Export drive key" and "Using Password Safe").

- ▶ Depending on the operating system platform, double-click on the file `WorkplaceProtect32_Setup.exe` or on the file `WorkplaceProtect64_Setup.exe`.
- ▶ In the *Program maintenance* window, select the *Remove program* option.
- ▶ Click on *Next*.
- ▶ Click on the notification *I wish to perform the uninstall* and confirm with *Remove*.

Workplace Protect is uninstalled.

You will be asked to restart the system to finish the process.

- ▶ To restart the system, confirm with *Yes*.
- ▶ To restart the system later, click on *No*.

Uninstall Workplace Protect through Windows

- ▶ Uninstall *Workplace Protect* as software, as described in the operating instructions for your operating system.

A message is displayed, warning that all the settings of *Workplace Protect* will be deleted during the uninstall process.

- ▶ Confirm with *Yes*.
- ▶ If you haven't yet backed up the settings, click on *No* to abort the uninstall process.

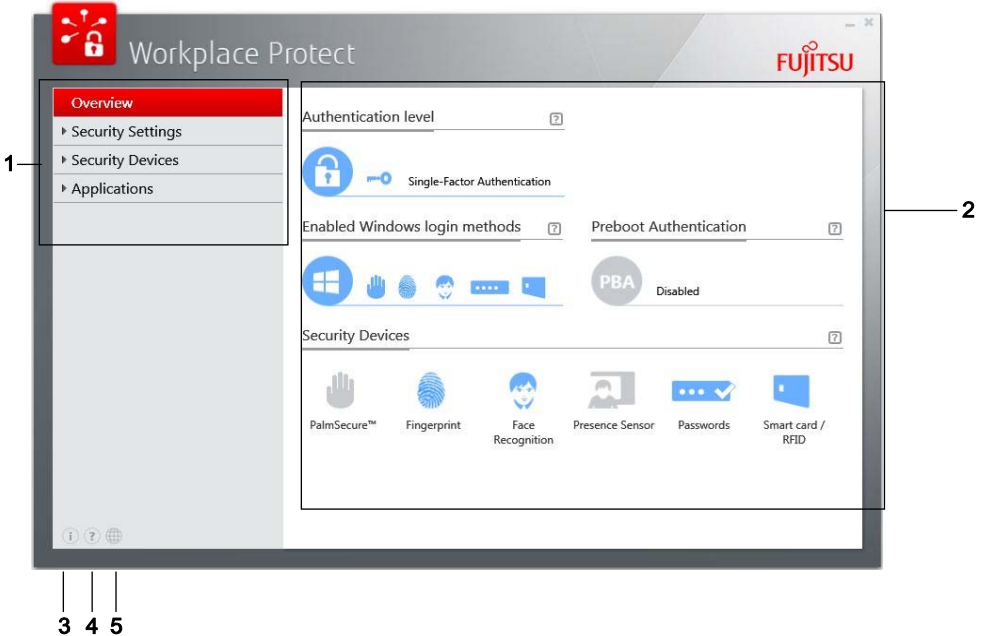
You will be asked to restart the system to finish the process.

- ▶ To restart the system, confirm with *Yes*.
- ▶ To restart the system later, click on *No*.

Overview of the user interface

Start screen

After *Workplace Protect* has started in the local and managed mode, the following screen will appear:






- 1 = Menu bar
- 2 = Display area with icons
- 3 = Information about the current version
- 4 = Access to the online manual
- 5 = Language selection

In managed mode, the options in the user interface are limited for the users in the network because many settings are configured by the administrator in the Workplace Manager.

Menus / Functions

You can call up a function either using the menu bar or by clicking on the relevant icon in the display area.

Menu / Function	Description
<p><i>Summary</i></p>	<p>This gives the following overview:</p> <ul style="list-style-type: none"> • Authentication Level set (Single-Factor, Multi-Factor with Template-on-Card or Multi-Factor with Secret) • Valid logon methods for the Windows logon • Pre-Boot Authentication active/inactive. • Available functions are displayed in blue, functions which are not available are displayed in grey. <p>By clicking on the question mark, you can receive information on the individual functional groups.</p>
<p><i>Security settings</i></p>	<p>General security settings (see the section "Security settings").</p> <ul style="list-style-type: none"> • <i>Authentication Levels:</i> Set the security level (Single-Factor, Multi-Factor with Template-on-Card or Multi-Factor with Secret). • <i>Pre-Boot Authentication:</i> Define the authentication at the start-up of the operating system (depending on the hardware, fingerprint or palm vein sensor or smartcard reader and the licence) • <i>Authentication configuration:</i> Define the logon methods for the applications, the Windows logon and Workplace Protect authentication • <i>Application settings:</i> Define how the computer should behave when the smart card is removed.
<p><i>Applications</i> (In the managed mode, individual or all the applications may be missing, and EasyRestore will only be displayed if the system was ordered with the relevant licence.)</p>	<p>Icons for starting the functions <i>Password Safe, Encrypted Container and Easy Restore.</i></p> <ul style="list-style-type: none"> ▶ To change the settings, click on the required icon (see the section "Authentication configuration").
<p><i>Security devices</i></p>	<p>Overview of the existing security systems (blue icons).</p> <ul style="list-style-type: none"> ▶ To call up or change the settings of a function, click on the relevant icon or on the relevant item in the menu bar.
	<p>Display the current software version</p>
	<p>Online manual</p>
	<p>Select the language for the software</p>

Set the language

To make language settings, proceed as follows:

- ▶ Click on the icon for selecting the language at the left lower edge of the display.



- ▶ Choose the desired language from the list and confirm with *Save*.

The language will be changed.

Perform the necessary authentication in Workplace Protect

When settings are changed, you will be asked to authenticate within the application using one of the configured security devices.



The alternatives for authentication depend on the particular user settings (see chapter "Security settings").

To perform authentication, proceed as follows:

- ▶ Among the available ways to authenticate, click on the option with which you wish to logon.
- ▶ Follow the instructions on the screen.

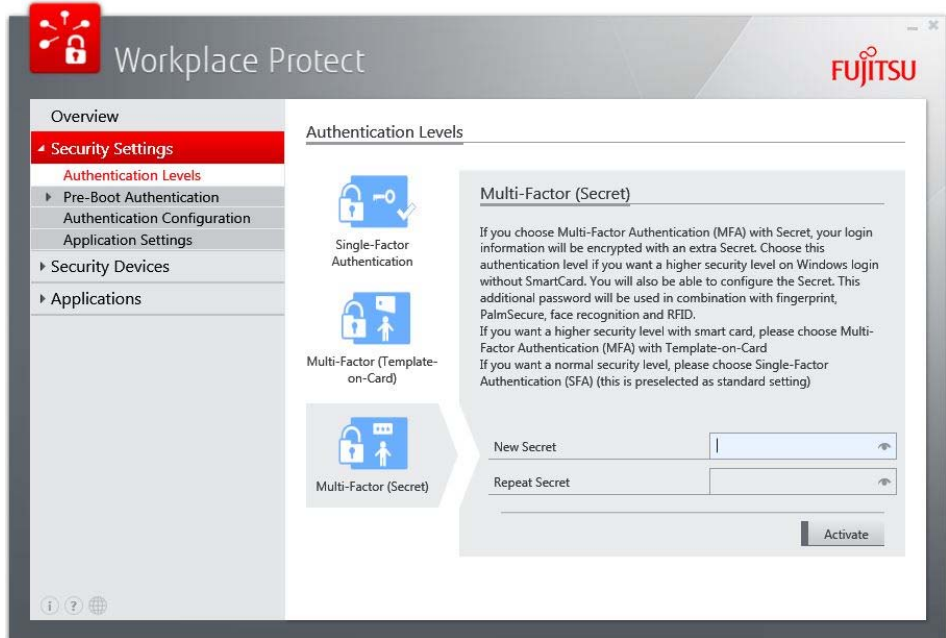
It is possible to save the password for the active session (see chapter "Application settings").

Security settings

Authentication levels




Workplace Protect offers various Authentication Levels. This means that the users must identify themselves in different ways on their computers, depending on the security level set. The more complex the identification procedure, the higher the security level.

The function group *Authentication Levels* shows which security level has been set to log on to the system.



With the *Single-Factor Authentication* the identity of the user is checked using a single feature (factor), for example using a password or a fingerprint.

With the *Multi-Factor Authentication* the identity of the user is verified using different components (factors) which are independent of each other. Only after providing a correct combination of these factors (for example, biometric data and a secret (an additional secret) or a smartcard and biometric data) is it possible for the user to log onto the network or the computer.

Authentication levels	Symbols	Description
<i>Single-Factor Authentication</i>	 <p>Single-Factor Authentication</p>	<p>Normal security features (standard setting). The logon information is stored on the computer. The following security devices are supported on this level:</p> <ul style="list-style-type: none"> • <i>Windows password</i> • <i>PalmSecure</i> (palm vein recognition) • <i>Fingerprint recognition</i> • <i>Face recognition</i> • <i>Smartcard</i> • <i>RFID card</i>
<i>Multi-Factor (Template-on-Card)</i>	 <p>Multi-Factor (Template-on-Card)</p>	<p>You can have increased security features if you can use a smartcard. The biometric data are stored on the smartcard. The following security devices are supported on this level:</p> <ul style="list-style-type: none"> • <i>PalmSecure</i> (palm vein recognition) • <i>Fingerprint recognition with Pre-Boot Authentication</i>
<i>Multi-Factor (Secret)</i>	 <p>Multi-Factor (Secret)</p>	<p>Increased security features without a smartcard. If you log in with a fingerprint, palm vein recognition, face recognition or RFID, an additional secret will be requested. The following security devices are supported on this level:</p> <ul style="list-style-type: none"> • <i>RFID card</i> • <i>PalmSecure</i> (palm vein recognition) • <i>Face recognition</i> • <i>Fingerprint recognition</i>

- ▶ Click on the relevant icon.
- ▶ Follow the instructions on the screen.

Authentication Levels in the local mode

In the local mode of Workplace Protect, the security level of a computer in a domain can be changed by any user who has access to that domain.

If a computer is outside that domain, this setting can only be changed if the user is logged on as an administrator on that computer.



When you change the security level, you will prevent any other users having access to the computer.

Authentication Levels in the managed mode

In the managed mode, the security level is set by the administrator.



If the administrator has set a multi-factor authentication, this will usually allow a short time to log on to the computer with a password, until the multi-factor authentication is completed for all the users.

Biometric data on the smartcard

On the smartcard, in addition to the biometric data, information is also stored about the reading device with which the data were recorded.



The biometric data on the smart card can only be read if the biometric reading device with which the recordings were made is available in the system.

If you are working on different computers with the smartcard, you must save palm-vein images or fingerprint images on the smartcard for each system.

Pre-Boot Authentication

The Pre-Boot Authentication (PBA) is an extension of the BIOS system. This enables authentication to take place as soon as the system starts up.



The menu will only display the methods which can be used by the hardware in certain conditions. It is possible that this menu item will not be displayed at all.

With the *Pre-Boot Authentication*, the following functions are available:

Function	Description
<i>Pre-Boot Authentication</i>	Setting options for the Pre-Boot Authentication <ul style="list-style-type: none">• <i>SystemLock settings (Smartcard)</i>• <i>Fingerprints</i>• <i>Palm vein recognition (PalmSecure™)</i>

If the Pre-Boot Authentication is configured, the user will be requested to provide authentication in the pre-boot phase.

If Single Sign On (SSO) has been enabled, the user receives access to the system and the operating system without further password requests if authentication is successful.



Only one type of *pre-boot authentication* can be used. It is not possible to activate the *SmartCard SystemLock* and *Fingerprint PBA* or *PalmSecure™ PBA* functions at the same time.

Activate and configure SystemLock

You can use your SmartCard to activate *SystemLock*. *SystemLock* is an extension of the system BIOS and allows pre-boot authentication for the use of SmartCards. You will be asked for the SmartCard PIN before the system BIOS boots.



You require a valid license before you can activate SystemLock. This license can only be purchased together with the device.

SystemLock authorisation rights	Description
<i>Admin</i>	<ul style="list-style-type: none"> • Change the system BIOS settings • Change the SystemLock settings in the system BIOS • Boot the operating system • Create new SystemLock SmartCards under Workplace Protect
<i>Superuser</i>	<ul style="list-style-type: none"> • Change the system BIOS settings (not including SystemLock) • Boot the operating system
<i>User</i>	<ul style="list-style-type: none"> • Boot the operating system
<i>Service</i>	<ul style="list-style-type: none"> • Change the system BIOS settings (not including SystemLock)



SystemLock SmartCards with administrator rights together with the PUK have all access rights and should therefore be kept in a secure place. They may only be used by an authorised user (administrator), for instance to create further SystemLock SmartCards.

If SystemLock activation is started with a blank SmartCard, then the SystemLock access data is created by the application and written to it. This SmartCard has administrator rights.

With a SystemLock SmartCard which has already been initialised with administrator rights, the access data is transferred from it.



When activating SystemLock, no administrator BIOS password may be set.



We strongly recommend that you create a second Admin card (see chapter "Activate and configure SystemLock").

Keep this SmartCard and PIN/PUK in a safe place and protect them against unauthorised access.

Proceed as follows to activate *SystemLock*:

- ▶ Click on *Activate SystemLock*.
- ▶ Insert the SmartCard into the SmartCard reader.
- ▶ Enter the PUK and confirm with *Next*.

Security settings

The SystemLock settings are displayed:

Field	Function
<i>Organisation</i>	Default value: name of the PC
<i>Group</i>	Default value: 1

- ▶ Confirm with *Next*.

Process for devices with SystemLock 2.0:



SystemLock 2.0 cannot be configured using *Workplace Protect*.

- ▶ To complete the configuration of SystemLock, reboot your computer and call up the BIOS Settings.
- ▶ Open *SmartCard SystemLock* on the *Security* tab and select *Install Group PC*.

Process for devices with SystemLock 3.0:

With SystemLock 3.0, a wizard is displayed for configuration of the the pre-boot authentication.

- ▶ Set the password for enabling Service. The password for the enabling must be at least 6 characters long.

or

- ▶ Check the check box *Generate a random password*.
- ▶ If you don't want to set a password for enabling Service, check the check box *I'm not interested*.
- ▶ Confirm with *Next*.
- ▶ Confirm with *Finish*.

A summary screen about the successful creation of the SystemLock administrator card is displayed. You then return to the overview page.

Unlocking a PC locked with SystemLock



A PC which has been locked using *SystemLock* can be unlocked in an emergency (e.g. faulty card, incorrect PIN/PUK entered several times) if the password for enabling service was entered during the *SystemLock* set up (see chapter "Activate and configure SystemLock").

To unlock a locked PC, please contact the Hotline/Service Desk (you can find more detailed information at <http://support.ts.fujitsu.com/contact/servicedesk>).

Have ready the password for enabling service and follow the instructions from the Service Desk colleague.

Fingerprint PBA activation and configuration



Fingerprint PBA is a system-wide function. The BIOS administrator password is therefore necessary for enabling.



A fingerprint sensor must be installed in the computer.
You may only use one pre-boot authentication method.



If the Fingerprint PBA was deactivated, only the function *Activate PBA* will be active.
If Fingerprint PBA is already activated, the functions *Deactivate PBA* and *Configure PBA* will be active.

If no fingerprint has yet been recorded for Fingerprint PBA, the recording menu will be started.



You need two registered fingerprints to activate the fingerprint PBA for pre-boot authentication (see chapter "Make fingerprint settings").

- ▶ At the top edge of the display, click on *Pre-Boot-Authentication\Fingerprint*.
- ▶ Click on *Activate PBA*
- ▶ When you are asked, authenticate yourself to the system (see chapter "Perform the necessary authentication in Workplace Protect").
- ▶ Select two stored fingerprints and confirm with *Next*.



The *Next* button only becomes enabled after two fingerprints have been selected.

A wizard for configuration of the pre-boot authentication is displayed.

- ▶ Enter the BIOS Setup password (see chapter "Changing the BIOS password").
- ▶ Confirm with *Next*.

A summary of the settings is displayed.

- ▶ Confirm these with *Finish*.

You then return to the overview page.





Deactivate Fingerprint PBA

- ▶ Select *Pre-Boot Authentication\Fingerprints*.
- ▶ Click on *Deactivate PBA*.
- ▶ Enter the BIOS administrator password.
- ▶ Confirm with *Next*.

You then return to the overview page.

The biometric data is deleted in the BIOS. The biometric data are retained for the Windows logon.

Enabling and configuring PalmSecure™ PBA

-  Only palm vein readers installed in notebooks are supported.
You may use only one PBA method.
 -  You need three registered recordings of one hand to activate the PalmSecure™ PBA for pre-boot authentication (see chapter "PalmSecure™ palm vein imaging").
You may be requested to have an image recorded of your palm veins before you can activate a PBA, even though recordings of your palm veins may already exist.
 -  If the palm vein PBA was deactivated, only the function *Activate PBA* will be active.
If the palm vein `_PBA` is already activated, the functions *Deactivate PBA* and *Configure PBA* will be active.
- ▶ Select *Pre-Boot Authentication/PalmSecure*.
 - ▶ Click on *Activate PBA*.
 - ▶ If the system requests you to do this, provide authentication for yourself (see the section "Perform the necessary authentication in Workplace Protect").
 - ▶ Select *Logon methods / Pre-boot authentication*.
 - ▶ On the *PalmSecure™* tab, click on the *Enable PBA* button.
 - ▶ Enter the BIOS Administrator password (see chapter "Changing the BIOS password").
 - ▶ Confirm with *Next*.
 - ▶ Select the palm recording that you wish to use to authenticate yourself and confirm with *Next*.
-  The *Next* button only becomes enabled after one palm recording has been selected.

A summary of the settings is displayed.

- ▶ Confirm these with *Finish*.

You then return to the overview page.

Disabling PalmSecure™ PBA

- ▶ Select *Pre-boot authentication /PalmSecure*.
- ▶ On the *PalmSecure™* tab, click on the *Disable PBA* button.
- ▶ Enter the BIOS administrator password (see chapter "Changing the BIOS password").
- ▶ Confirm with *Next*.

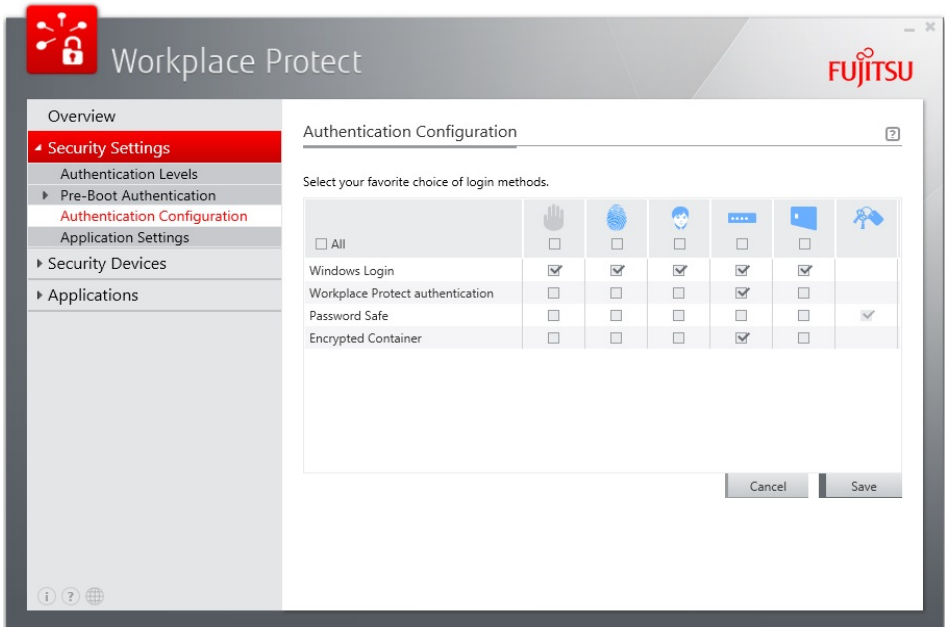
You then return to the overview page.

The biometric data is deleted in the BIOS. The biometric data are retained for the Windows logon.

Authentication configuration

To make settings in the authentication configuration, proceed as follows:

- ▶ Under *Security Settings*, click on *Authentication Configuration*.
- ▶ When you are asked, authenticate yourself to the system (see chapter "Perform the necessary authentication in Workplace Protect").



- ▶ For the authentication methods, check the checkbox for the desired security devices to be able to use them for authentication.

Function	Description
<i>All</i>	Marks all possible authentication methods
<i>Windows logon</i>	Settings for the supported authentication methods during Windows logon
<i>Workplace Protect authentication</i>	The authentication settings specified here will always be used to authenticate the user for the configuration of security devices and security settings.
<i>Password Safe</i>	User authentication for Password Safe
<i>Encrypted Container</i>	User authentication for the Encrypted Container

- ▶ Click on *Legend* in the lower area of the display for an explanation of the icons.
- ▶ Confirm the settings with *Save*.
- ▶ To return to the overview page, click on *Back*.

Application settings

To define the application settings, proceed as follows:

- ▶ In the menu bar, click on *Security Settings - Application Settings*.
- ▶ When you are asked, authenticate yourself to the system (see chapter "Perform the necessary authentication in Workplace Protect").

You can choose from the following functions:

Field	Function
<i>SmartCard settings</i>	<i>Behaviour when the SmartCard is removed</i> <ul style="list-style-type: none">• <i>No action (default setting)</i>• <i>Lock my computer</i>• <i>Log off</i> <p>This action only becomes enabled after a logoff and a logon again with SmartCard / RFID or the system is rebooted.</p>

- ▶ Confirm the changes with *Save*.

You then return to the overview page.

Setting the security devices

i







Only *security devices* that are supported by the system can be selected.

In managed mode, only devices and combinations that have been approved by the administrator are displayed.

If Multi-Factor Authentication is set on the system, the associated methods must also be configured when selecting a security device. Possible combinations are:

- Fingerprint or palm veins and smartcard
- Palm veins or fingerprint or face recognition or RFID and additional password (secret)

Under *security devices*, the following functions are available to you:

Security device	Icon	Description
<i>PalmSecure™</i>		Save palm images, verify or delete those already saved
<i>Fingerprint</i>		Save fingerprints, verify or delete those already saved
<i>Face recognition</i>		Configure face recognition
<i>Presence sensor</i>		Change the settings of the presence sensor
<i>Passwords</i>		Manage passwords for Windows, BIOS and hard drives
<i>SmartCard / RFID</i>		Configure SmartCard or RFID card

i

You can call up a function either using the menu bar or by clicking on the relevant icon in the display area.

If you call up the function with start wizards, a wizard guides you through the settings. In the wizard you will find further information and additional background knowledge.

PalmSecure™ palm vein imaging

The first steps differ, depending on the pre-set Authentication Level.

Single-Factor Authentication If this method is set, the images are saved on the computer.

Multi-Factor (Template on Card) If this method is set for identification on the system, the images are saved on the smartcard.

- ▶ Insert the smartcard into the reader before starting to scan.

NOTE: If you work on different computers with the smartcard, you must save palm-vein images on the smartcard for each system.

Multi-Factor (Secret) If this method is set for identification on the system, the first time the palm-vein imaging is set up, the user is automatically requested to enter the secret first.

- ▶ Enter the secret and click *activate*.

- ▶ Under *security devices*, click on *PalmSecure™/ Start wizards*.
- ▶ Confirm with *Next*.
- ▶ When you are asked, authenticate yourself to the system (see chapter "Perform the necessary authentication in Workplace Protect").
- ▶ Select the hand for which you would like to perform an action.
- ▶ Click on the button of the desired action:

Action	Description
<i>Enroll</i>	Read in and save palm recording
<i>Verify</i>	Verify palm recordings already saved
<i>Remove</i>	Delete palm recordings already saved
<i>Back</i>	Go back to the choice of palm

Read in palm



At least one palm vein must have been read in and stored before you can end the configuration.

- ▶ In the menu bar, click on *Security Devices - PalmSecure™*.
- ▶ Select a hand by clicking on the desired hand.

The hand is marked.

- ▶ Click on *Enroll*.
- ▶ Hold your hand over the palm sensor and move your hand according to the symbols on the screen.

When the recording was correct, this will be notified.

- ▶ Confirm with *Finish*.

You then return to the overview page.

Make fingerprint settings



No fingerprints can be recorded for user accounts which were automatically created by Windows 8 (Administrator, Guest). An error message appears in this case.

The first steps differ, depending on the pre-set Authentication Level.

Single-Factor Authentication If this method is set, the images are saved on the computer.

Multi-Factor (Template on Card) If this method is set for identification on the system, the images are saved on the smartcard.

- ▶ Insert the smartcard into the reader before starting to scan.

NOTE: If you work on different computers with the smartcard, you must save palm-vein images on the smartcard for each system.

Multi-Factor (Secret) If this method is set for identification on the system, the first time the palm-vein imaging is set up, the user is automatically requested to enter the secret first.

- ▶ Enter the secret and click *activate*.

- ▶ Under *security devices*, click *fingerprint / start wizards*.
- ▶ Confirm with *Next*.
- ▶ When you are asked, authenticate yourself to the system (see chapter "Perform the necessary authentication in Workplace Protect").
- ▶ Select the finger for which you would like to perform an action.
- ▶ Click on the button of the desired action:

Action	Description
<i>Record</i>	Read in and save fingerprint
<i>Verify</i>	Verify fingerprints already saved
<i>Remove</i>	Delete fingerprints already saved
<i>Back</i>	Back to the choice of finger

Read in fingerprint



At least two fingerprints must have been read in and stored before you can end the configuration.

- ▶ In the menu bar, click on *Security Devices - Fingerprint*.
- ▶ Select one finger by clicking in the circle above the desired finger.

The circle above the finger will be marked in blue.

- ▶ Click on *Record*.
- ▶ Draw the desired finger evenly over the fingerprint sensor.

Four successful recordings must be made to complete the process.

The finger which has been read in will be marked with a green tick.

- ▶ Confirm with *Next*.
- ▶ Repeat this process for the other fingerprints.

A summary of the settings you have made is displayed.

- ▶ Confirm with *Finish*.

You then return to the overview page.

Face recognition settings

The first steps differ, depending on the pre-set Authentication Level.

Single-Factor Authentication If this method is set, the images are saved on the computer.

Multi-Factor (Template on Card) Not supported

Multi-Factor (Secret) If this method is set for identification on the system, the first time the face recognition is set up, the user is automatically requested to enter the secret first.

- ▶ Enter the secret and click *Activate*.



The advanced functions of face recognition are enabled for a period of 30 days:

- Eye blink detection
- Several profiles accepted
- Session lock, when no system user is detected.
- Setting the security level

To be able to use these advanced functions after the 30 days have expired, please purchase a licence key via the "Licence" tab.

In managed mode, a licence is required for the advanced functions of face recognition. (not enabled for the 30-day period)



For the face recording, ensure there are good lighting conditions.

- ▶ In the menu bar, click on *Security devices - Face recognition / Start wizard*.
- ▶ Confirm with *Next*.
- ▶ When you are asked, authenticate yourself to the system (see chapter "Perform the necessary authentication in Workplace Protect").
- ▶ Select the desired WebCam.
- ▶ If you notice video lags on your system, check the *Low resolution* checkbox.
- ▶ Confirm with *Next*.
- ▶ Place yourself in front of the WebCam in the frame shown.

When the automatic recognition has completed, a configuration wizard is displayed offering further settings options.

- ▶ Make the settings you require:

Setting tab	Function
<i>Session lock</i>	<p>The session is automatically locked when the user is no longer in the recording area of the camera.</p> <p>A presence check is made every 30 seconds.</p> <p>If no authentication by face recognition occurs within a period of 25 seconds, the session is locked. During this period, a window is shown at the lower right-hand edge of the screen.</p> <ul style="list-style-type: none"> ▶ To remain logged on to the system, look at the WebCam.
<p><i>Security level</i></p> <p style="text-align: right;"><i>High</i></p> <p style="text-align: right;"><i>Moderate</i></p> <p style="text-align: right;"><i>Low</i></p> <p><i>Eye blink detection</i></p>	<p>The face is checked very precisely. This increases security but the recognition requires more time.</p> <p><i>This setting is a good compromise</i> between faster recognition and greater security</p> <p>The face is checked very quickly. This decreases security</p> <p>During the authentication, a blink of the eyes is required to prevent authentication with a photo.</p>
<i>Time delay for face recognition</i>	<p>In order not to immediately log on the user again while logging off or locking the computer, the authentication by face recognition is delayed by the time period set.</p> <p>The authentication time delay can be interrupted by pressing any key</p>

A summary of the settings you have made is displayed.

- ▶ Confirm with *Finish*.

You then return to the overview page.

Editing the face recognition settings

Proceed as follows to edit the face recognition settings you have made.

- ▶ In the menu bar, click on *Security devices - Face recognition. / Configure*.
- ▶ If you are asked, authenticate yourself to the system (see chapter "Perform the necessary authentication in Workplace Protect").

You can choose from the following tabs:

Tab	Functions
<i>Settings</i>	Change basic settings
<i>Profile</i>	Create, change, delete or verify face model Licence-free version: use of only one profile possible Licensed version: use of several profiles possible. Tip: It is useful to have several profiles if the computer is used at different locations with different lighting conditions
<i>WebCam</i>	Change WebCam settings: Licence-free version: only one camera can be used Licensed version: several cameras can be used
<i>Licence</i>	Information about the licensing status

Licence settings for face recognition

- ▶ In the menu bar, click on *Security devices - Face recognition. / Configure*.
- ▶ Select the *License* tab.

You can make the following selections:

Field	Description
<i>Your license key</i>	Your license key
<i>Activated at</i>	Time of the license activation
<i>Name</i>	Your name (optional)
<i>Email</i>	Your email address (optional)
<i>Request license</i>	Request a license key for the advanced functions of face recognition

Presence sensor settings



You are required to have a licence to use the presence sensor functions.

To set the functions, proceed as follows:

- ▶ In the menu bar, click on *Security Devices - Presence sensor*.

You have the following functions available:

Field	Function
<i>Presence sensor</i>	<p>Activate presence detection:</p> <p>When the function is active, <i>The user is present</i> indicates that the user was detected in front of the device.</p>
<i>User is absent</i>	<p>Possible settings for absence of the user:</p> <ul style="list-style-type: none"> • <i>Lock computer</i> • <i>Switch off monitor</i> • <i>Switch off monitor and lock computer</i> • <i>Sleep mode</i> • <i>Hibernate mode</i>
<i>User presence</i>	<p>Possible settings for presence of the user:</p> <ul style="list-style-type: none"> • <i>Switch on monitor</i> • <i>Resume the computer from sleep or hibernate</i>



A setting which has already been selected is no longer available for other actions.

- ▶ Confirm the settings with *OK*.

Changing the password settings

To change the password settings, proceed as follows:

- ▶ In the menu bar, click on *Security Devices - Passwords*.

The tab is displayed for changing the passwords for Windows, BIOS and hard disks.

- ▶ Click on the tab to change the corresponding password.

Changing the Windows password

To change the Windows password, proceed as follows:

- ▶ In the menu bar, click on *Security Devices - Passwords*.
- ▶ Click on the tab *Windows password*.

- ▶ Enter the following data:

Field	Function
<i>Current password</i>	Current password
<i>New password</i>	New password
<i>Confirm password</i>	Confirm password


- ▶ Click on *Set password*.

A message is shown concerning saving the password.

Changing the BIOS password

To change the BIOS password, proceed as follows:

- ▶ In the menu bar, click on *Security Devices - Passwords*.
- ▶ Click on the tab *BIOS password*.

 If no BIOS password is set, leave the field *Current password* empty and continue with the field *New password*.


- ▶ Enter the following data:

Field	Function
<i>Select password type</i>	<i>Administrator</i> : The administrator has unrestricted access to the system-BIOS <i>User</i> : The user has restricted access to the system BIOS
<i>Current password</i>	Current password
<i>New password</i>	New password
<i>Confirm password</i>	Confirm password

- ▶ Click on *Set password*.

A message is shown concerning saving the password.

Deleting a BIOS password

 The pre-boot authentication with biometric data (palm veins or fingerprint) becomes deactivated if the BIOS administrator password is deleted.

However, the images of fingerprints or palm veins remain stored in the BIOS system. You can reactivate the images at any time via the pre-boot authentication function.

To delete the BIOS password, proceed as follows:

- ▶ In the menu bar, click on *Security devices - Passwords / Configure*.
- ▶ Click on the tab *BIOS Password*.
- ▶ If the system requests you to do this, provide authentication for yourself (see the section on "Providing the necessary authentications for Workplace Protect" "Perform the necessary authentication in Workplace Protect").

- ▶ Enter the current BIOS password and click on *Delete password*.

A save or delete notification will be displayed for the password.

Changing the hard disk password

To change the hard disk password, proceed as follows:



A BIOS password must be set to be able to set a hard disk password.
The hard disk password is applied during the next system reboot.




- ▶ In the menu bar, click on *Security Devices - Passwords*.
- ▶ Click on the tab *Hard disk password*.
- ▶ Enter the BIOS Setup password.
- ▶ If there is one already present, enter the current hard disk password and then confirm it.
- ▶ Enter the new hard disk password and confirm it.
- ▶ To save the password, click on *Set password*.

A message is shown concerning saving the password.

Smartcard

Insert the smartcard

When you insert the smartcard into the reading device, one of the following symbols may appear.

Symbol	Meaning
	The smartcard is valid and contains login details.
	The status of the smartcard is unknown. The smartcard must be unlocked using the PIN.
	The smartcard is not supported.

Configuring a SmartCard

- ▶ In the menu bar, click on *Security Devices - SmartCard / RFID*.
- ▶ Insert the SmartCard into the module provided.

A wizard with further information on the functionality is shown.

- ▶ Follow the instructions on the screen.

A summary of the settings you have made is displayed.

- ▶ Confirm with *Finish*.

You then return to the overview page.

Changing the SmartCard settings

Proceed as follows to make changes to the SmartCard settings:

- ▶ In the menu bar, click *Security Devices - SmartCard / RFID*.
- ▶ Insert the SmartCard into the module provided.
- ▶ Follow the instructions on the screen.

You arrive at the overview page showing the SmartCard settings.

You can make the following settings here:

Tab	Function
<i>Admin</i>	Activate SystemLock (see chapter "Activate and configure SystemLock")
<i>Change PIN</i>	Change current PIN
<i>Change PUK</i>	Change current PUK
<i>Unblock PIN</i>	Unblock PIN which has been blocked
<i>User management</i>	Delete registered users on the SmartCard
<i>SystemLock cards</i>	Write access data for SystemLock onto SmartCards

- ▶ To make changes to the settings, click on the corresponding tab at the upper edge of the display and follow the instructions on the screen.

Configure RFID card

Single-Factor Authentication If this method is set, the images are saved on the computer.

Multi-Factor (Template on Card) Not supported

Multi-Factor (Secret) If this method is set for identification on the system, the first time the RFID card is set up, the user is automatically requested to enter the secret first.

- ▶ Enter the secret and click on *Activate*.

- ▶ In the menu list, click on *Security devices – Smartcard / RFID / Configure*.
- ▶ Using an optional RFID reader, you can configure an RFID card or an RFID token for authentication.
- ▶ Hold the RFID card over the RFID reader.

A wizard with further information on the functionality is shown.

- ▶ Confirm with *Next*.
- ▶ When you are asked, authenticate yourself to the system (see chapter "Perform the necessary authentication in Workplace Protect").

A summary with the settings you have made is displayed.

You then return to the overview page.



Under *Windows 8* and *Windows 10*, the RFID icon is displayed in the logon screen.



Log off or lock session

Requirement: The corresponding configuration of the actions for logging off or locking the session must have been performed previously (see chapter "Application settings").

To log off from the system or to lock the session, proceed as follows:

- ▶ Log off the system as described in the documentation for your operating system.

or

- ▶ If during "Face recognition settings" you enabled the option *Session Lock*, and no authentication by face recognition occurs within a period of 25 seconds, the session will be locked.

or

- ▶ Leave the recording area of the presence sensor.




or

- ▶ If you have logged on with smartcard / RFID remove the smartcard / RFID card.

Applications

i The *Applications* entry is only shown in the managed mode of *Workplace Protect* when at least one application has been enabled by the administrator in *Workplace Manager*.

The following functions are available in the *Applications* area:

Function	Icon	Description
<i>Password Safe</i>		Configuration of an encrypted database in which your access data will be stored.
<i>Encrypted Container</i>		Configuration of a virtual encrypted drive. Important user data will be stored at a secure location.
<i>Easy Restore</i>		Backup the computer and easily restore the contents of the hard disk.

Using Password Safe

i The function is only shown in the managed mode of *Workplace Protect* if it has been enabled by the administrator in *Workplace Manager*.

i The application checks whether you have already used *Password Safe* in an earlier version of *Workplace Protect*. If an earlier version is found, the *Workplace Protect Password Safe Converter* assistant (wizard) starts, which you must use to update the application.

If you do not have any internet access, contact your administrator so that he/she can provide you with the necessary files.

You must change to the newer version in order to be able to continue working with *Password Safe*.

▶ Enter your master password for the existing database and confirm with OK.

The database that is currently set up will be converted to the new database version.

Creating a new Password Safe database

Proceed as follows to create a new *Password Safe* database:

▶ In the menu bar, click on *Applications - Password Safe*.

A wizard is displayed.

▶ Follow the instructions on the screen.

► Fill in the fields as follows:

Field	Function
<i>Database name</i>	Name of the database
<i>Path</i>	The file path at which the database should be stored.
<i>Import existing Password Safe</i>	Click to import a <i>Password Safe</i> database which already exists.
<i>Path</i>	Can only be selected if the check box is activated. Choice of existing <i>Password Safe</i> database

- Confirm with *Next*.
- Enter a master password of your choice and make a note of it.
- Confirm the master password which you have entered.
- Confirm with *Next*.

A summary of the settings made is displayed.

- Confirm with *Finish*.

You then return to the overview page.

Importing existing Password Safe database

Proceed as follows to import an existing *Password Safe* database:

- Right-click with the mouse over the summary page on the symbol for *Password Safe*.
- If you do not wish to replace a Password Safe which already exists, click on *No*.

or

- If you wish to replace a Password Safe which already exists, click on *Yes*.
- Check the check box *Import existing Password Safe*.
- Select the *Password Safe* database file to be imported.
- Confirm with *Next*.
- Enter the master password.
- Confirm with *Next*.

A summary of the settings made is displayed.

- Confirm with *Finish*.

You then return to the overview page.

Deleting an existing Password Safe database

Proceed as follows to delete an existing *Password Safe* database:

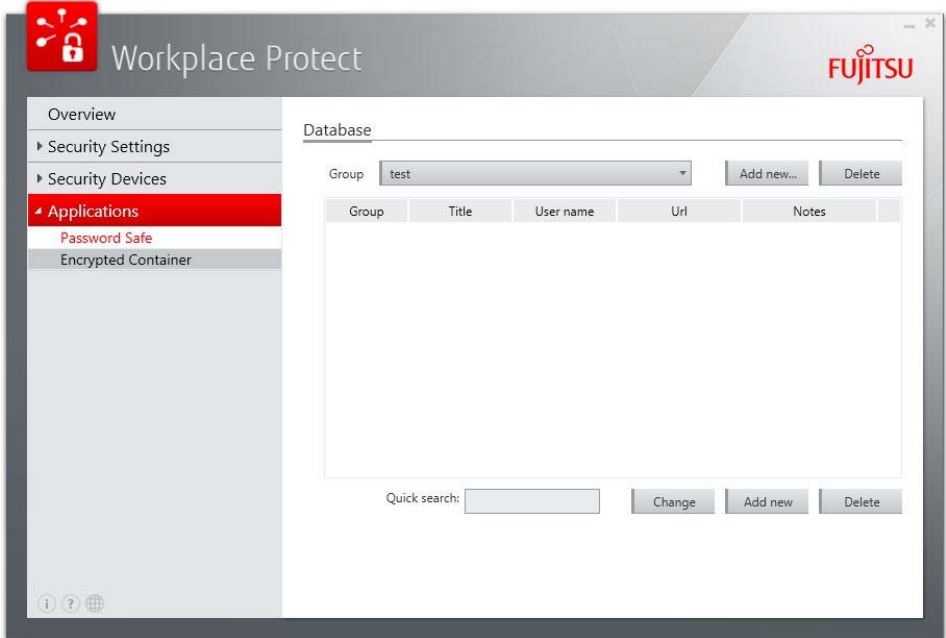
- Open the file path where you have created the Password Safe.
- Delete the relevant *Password Safe* database file.

Creating a new group

Access data for a particular area (e.g. private, business, etc.) can be managed in a group.

To create a new group, proceed as follows:

- ▶ In the menu bar, click on *Applications - Password Safe*.
- ▶ Enter the master password for the database shown.
- ▶ Confirm with *OK*.
- ▶ At the top of the display screen, click on the button for the desired action:



Field	Function
<i>Add new...</i>	Create a new group
<i>Delete</i>	Delete an existing group

Creating, changing or deleting entries with access data in the group

To create, change or delete entries with access data in the group, proceed as follows:

- ▶ In the menu bar, click on *Applications - Password Safe*.
- ▶ Enter the master password for the database shown.
- ▶ Confirm with *OK*.
- ▶ At the bottom of the display screen, click on the button for the desired action:

Field	Function
<i>Change</i>	Edit selected entry in the group
<i>Add new</i>	Create a new entry in the group
<i>Delete</i>	Remove selected entry from the group

- ▶ Follow the instructions on the screen.

Creating a new entry with access data in the group

To create a new entry in the group, proceed as follows:

- ▶ In the menu bar, click on *Applications - Password Safe*.
- ▶ Enter the master password for the database shown.
- ▶ At the lower edge of the display, click on the button *Add new*.
- ▶ Fill in the fields displayed accordingly:

Field	Description
<i>Title</i>	Free choice of information
<i>Group</i>	Group assignment
<i>User name</i>	Username used
<i>URL</i>	Internet address (for online passwords)
<i>Notes</i>	Free choice of notes
<i>Password</i>	Chosen password
<i>Repeat password</i>	Repeat password
<i>Quality</i>	Complexity of the password
<i>Definition for autofill</i>	The configuration (shortcut) for automatic transfer of the access data on the last active window.

- ▶ After you have completed the fields, confirm with *OK*.

Using access data from the group

To transfer saved access data on the last active window, proceed as follows:

- ▶ In the menu bar, click on *Applications - Password Safe*.
- ▶ Enter the master password for the database shown.
- ▶ Right-click on the desired entry.

You can make the following selections:

Field	Function
<i>Open URL</i>	Open the desired Internet page
<i>Copy user name</i>	Copy user name to the clipboard
<i>Copy password</i>	Copy password to the clipboard
<i>Auto fill</i>	The logon information will be transferred to the window which was opened last.

Delete an existing group



All the information within the group must be deleted before you can delete a group.

You can only delete a group all at once.

To delete an existing group, proceed as follows:

- ▶ In the menu bar, click on *Applications - Password Safe*.
- ▶ Enter the master password for the database shown.
- ▶ Click on the *Group* dropdown menu and select the group to be deleted.
- ▶ Click on *Delete* and confirm with *Yes*.

or

- ▶ If you want to keep the group, click on *No*.

Using Encrypted Container



The function is only shown in the managed mode of *Workplace Protect* if it has been enabled by the administrator in *Workplace Manager*.

An *Encrypted Container* is a virtual encrypted drive on which important user data can be stored securely.

Create new Encrypted Container / Prepare new drive

To create a new *Encrypted Container*, proceed as follows:

- ▶ In the menu bar, click on *Applications - Encrypted Container*.

A wizard is displayed.

- ▶ Confirm with *Next*.
- ▶ To generate a new *Encrypted Container*, select *Create new drive*.

A wizard is displayed.



- ▶ Follow the instructions on the screen.

A summary of the possible settings for the *Encrypted Container* is displayed:

Field	Function
<i>Drive designation</i>	Name of the Encrypted Container
<i>Size of the new drive</i>	Set a size between 50 MB and 100 Gb.
<i>Type of data carrier</i>	Select from the drop-down list: <ul style="list-style-type: none">• <i>Dynamically expanding:</i> The file in which the data is stored grows continuously with contents until the specified maximum size of the container is reached.• <i>Fixed size:</i> The file in which the data is stored is created with a fixed size.
<i>Drive letter</i>	Select the drive letter
<i>Storage location</i>	Select the file path at which the Encrypted Container should be created. Network paths are not supported.

- ▶ Use the slide control to choose the size of the virtual drive.
- ▶ Confirm with *Next*.

The *Encrypted Container* will be included in the system as a drive.

A summary of the properties and the corresponding drive key are displayed.



Make a note of the drive key and keep it somewhere safe. You will need it to perform a reinstallation of the software or to import an existing *Encrypted Container* (see chapter "Importing Encrypted Container File (VHD)"). In addition, you can export the drive key separately (see chapter "Export drive key").

- ▶ Confirm with *Finish*.

The *Encrypted Container* is integrated.

You then return to the overview page.

Reintegrate the Encrypted Container (mount)

To mount a previously created *Encrypted Container*, proceed as follows:

- ▶ In the menu bar, click on *Applications - Encrypted Container*.
- ▶ Select the *Encrypted Container* which you would like to mount.
- ▶ Click on *Mount*.
- ▶ When you are asked, authenticate yourself to the system (see chapter "Perform the necessary authentication in Workplace Protect").

The *Encrypted Container* is integrated. The *Integration status* for the respective *Encrypted Container* changes to *Yes*.

Unmounting an Encrypted Container (unmount)

To unmount an Encrypted Container, proceed as follows:

- ▶ In the menu bar, click on *Applications - Encrypted Container*.
- ▶ When you are asked, authenticate yourself to the system (see chapter "Perform the necessary authentication in Workplace Protect").
- ▶ Select the virtual drive you would like to unmount.
- ▶ Click on *Unmount*.
- ▶ The *Encrypted Container* is unmounted. The *Mount state* for the particular *Encrypted Container* changes to *No*.

Edit existing Encrypted Container

Here an *Encrypted Container* which already exists can be edited, deleted, the drive key can be exported or existing *Encrypted Container* files (VHD) can be imported. Proceed as follows:

- ▶ In the menu bar, click on *Applications - Encrypted Container*.
- ▶ In the display area, click on the tab *Administrative Tools*.

Field	Function
<i>Edit drive</i>	Change drive designation and storage path
<i>Delete drive</i>	Selected encrypted drive
<i>Export drive key</i>	Export drive key
<i>Import VHD</i>	Import <i>Encrypted Container</i> file

Delete the existing Encrypted Container / Drive

To delete an existing *Encrypted Container*, proceed as follows:

- ▶ In the menu bar, click on *Applications - Encrypted Container*.
- ▶ In the display area, click on the tab *Administrative Tools*.
- ▶ Select the *Encrypted Container* that you would like to delete.
- ▶ Click on *Delete drive*.
- ▶ Confirm with *Yes*.
- ▶ When you are asked, authenticate yourself to the system (see chapter "Perform the necessary authentication in Workplace Protect").

Export drive key

After a reinstallation of the program, the drive key is required to mount the *Encrypted Container*. The key must be exported beforehand, otherwise no access to the *Encrypted Containers* is possible.

To export the drive key, proceed as follows:

- ▶ In the menu bar, click on *Applications - Encrypted Container*.
- ▶ In the display area, click on the *Administrative Tools* tab.
- ▶ Click on *Export drive key*.
- ▶ When you are asked, authenticate yourself to the system (see chapter "Perform the necessary authentication in Workplace Protect").

The drive key is displayed. Make a note of the key.

- ▶ To return to the *Encrypted Container* list, click on *Back*.

Importing Encrypted Container File (VHD)

You have the facility to import other *Encrypted Container files* (VHD) and to mount them in *Workplace Protect*.



If you delete or redefine the *Encrypted Container*, mounting is no longer possible.

- ▶ In the menu bar, click on *Applications - Encrypted Container*.
- ▶ In the display area, click on the tab *Administrative Tools*.
- ▶ Click on *Import VHD*.
- ▶ Enter the drive key.
- ▶ Enter the path where the file to be imported is located.
- ▶ Click on *Import container*.

Easy Restore

With *Easy Restore*, the contents of a hard disk can be easily encrypted and stored on a shared network folder with a personal password. The backup can be rebuilt from this without any difficulty by pressing the F5 button during the system boot. Storage and restore are possible in the company network. Neither additional software nor supplementary media (e.g. DVD, USB stick) are needed.

Requirements for Easy Restore from a company's own server

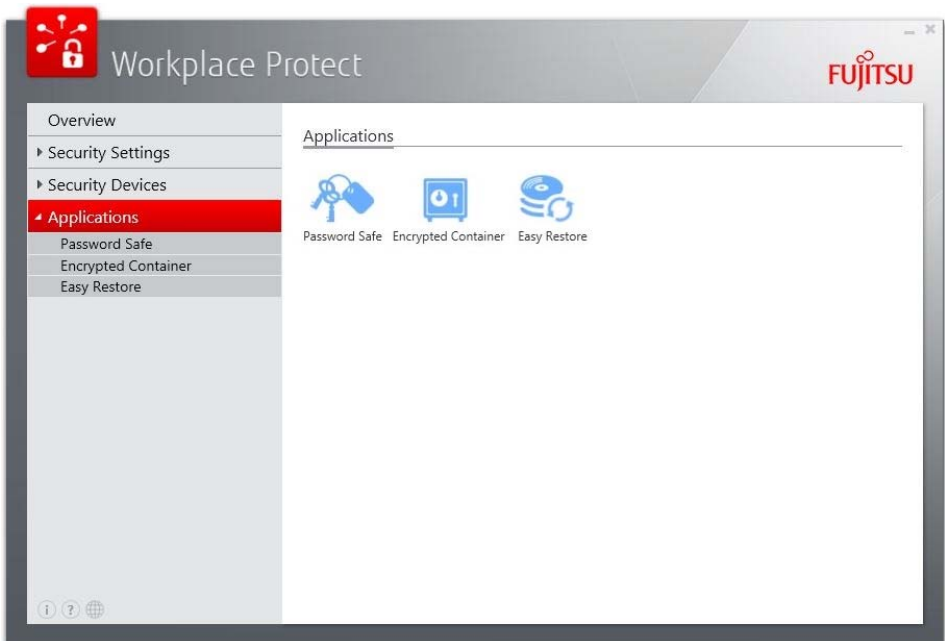
- TFTP server (for setting up the server, please refer to this manual, TFTP server, page 52)
- The function must be enabled for use in the Workplace Manager software.
- A licence is required.
- *Windows 10* is not supported.

Easy Restore can only be used on selected systems from Fujitsu.

To be able to use the *Easy Restore* function in your company network, the license for *Workplace Embedded Tools* must be ordered at the same time as the system is ordered (order number S26361-F2542-E437).

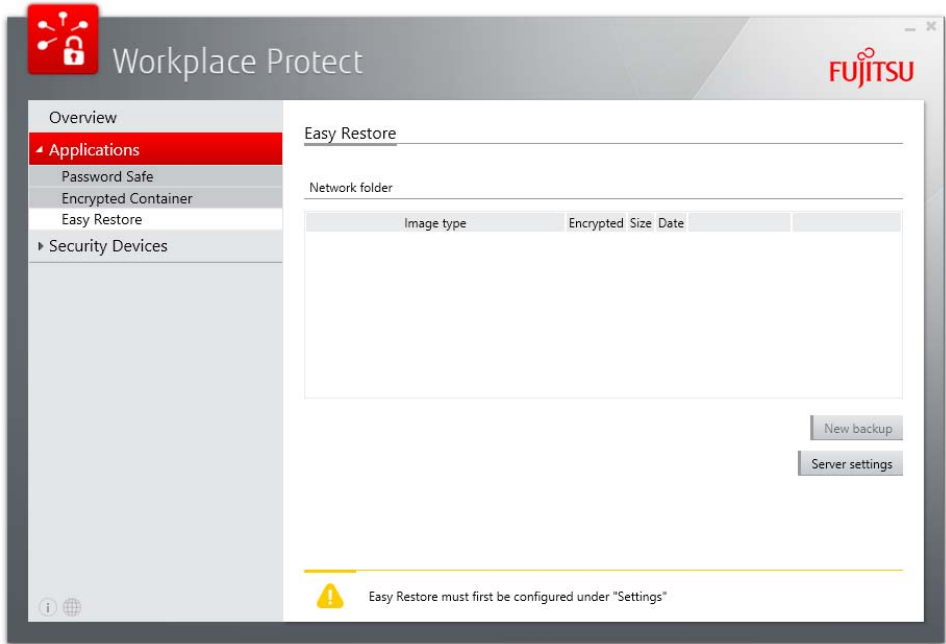
It is not possible for the license to be issued later on.

i The function is only shown in managed mode of *Workplace Protect* if it has been enabled by the administrator in *Workplace Manager* and the system has the license for *Workplace Embedded Tools* at its disposal.



Start Easy Restore

- In the menu bar, click on *Applications - Easy Restore*.



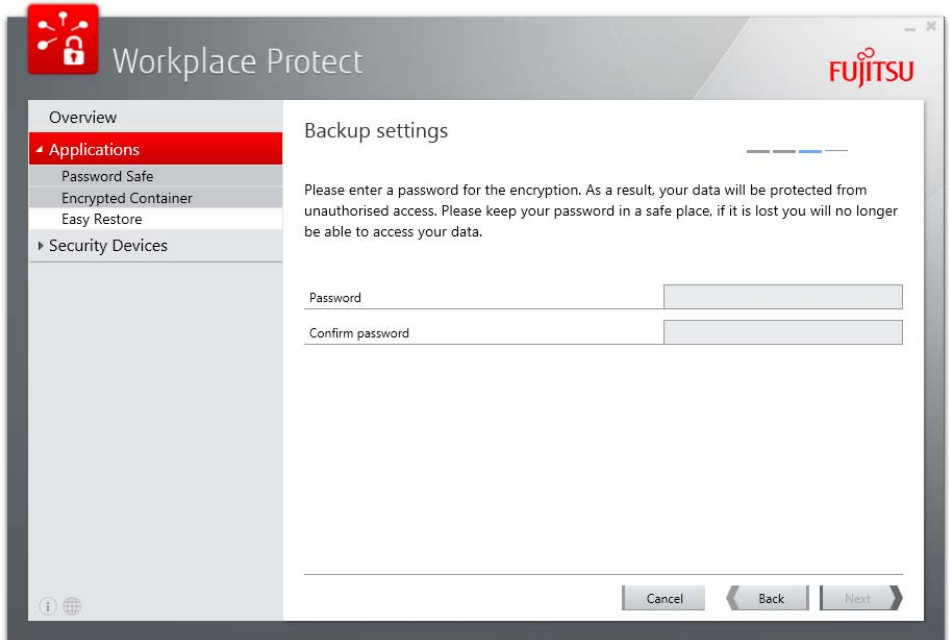
Button	Function
<i>New data backup</i>	Backs up the contents of the hard disk. A backup can be repeated at any time.
<i>Server settings</i>	During the first start of <i>Easy Restore</i> , the server on which the data will be backed up must be configured.
<i>Download</i>	During the first start, the boot image (<i>Windows PE</i>) must be downloaded from the Fujitsu Server. The image is automatically stored on the TFTP server. The button is only visible during the first start or if a new boot image (<i>Windows PE</i>) is present.

Create data backup

To create a new data backup, proceed as follows:

- ▶ Click on *New data backup*.

The following window opens:

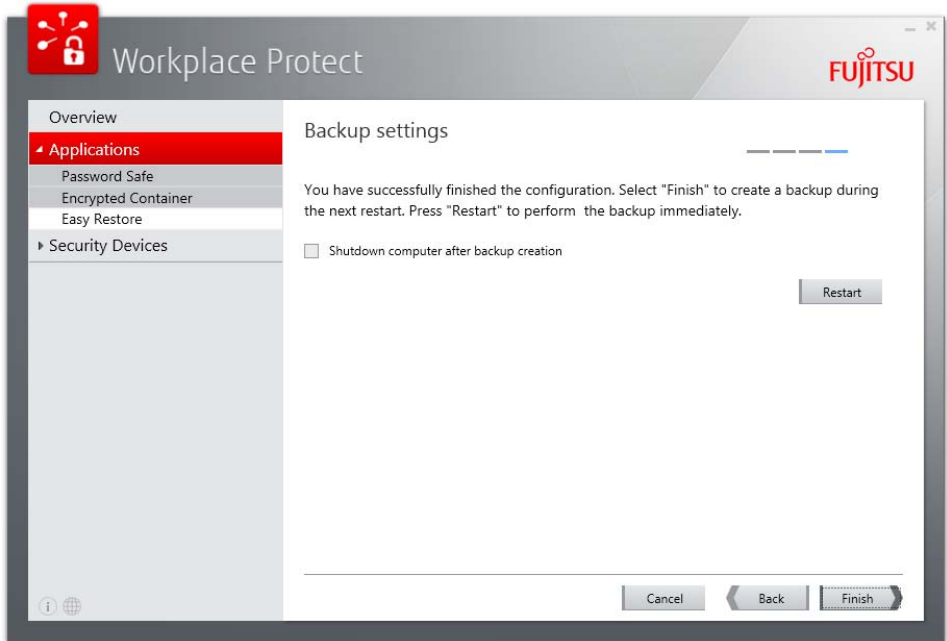


Users of *Windows 8.1* with pre-installation by Fujitsu can first choose from one of the following options:

- *Recreate delivery state*: the user data is lost during this backup.
- *User data*: only the user data is backed up.
- *Recreate previous state*: the system and the user data are reset to their last backed up state.

On all other systems, the reset is always to the last backed up state.

- ▶ Enter the required password and confirm it, to protect your backup from unauthorised access.
- ▶ Click on *Next* to complete the process.



At this point you have two options.

- ▶ Click on *Restart* to create the backup immediately.

Or

- ▶ Click on *Finish* to create the backup during the next restart of the computer.
- ▶ Select the option *Switch off the computer after the data backup* to shut down the computer when the backup has been created (e.g. when the start of the backup is at the end of the working day).

When the backup is generated, you receive the BIOS message:

Easy Restore: Starting backup. Please wait...

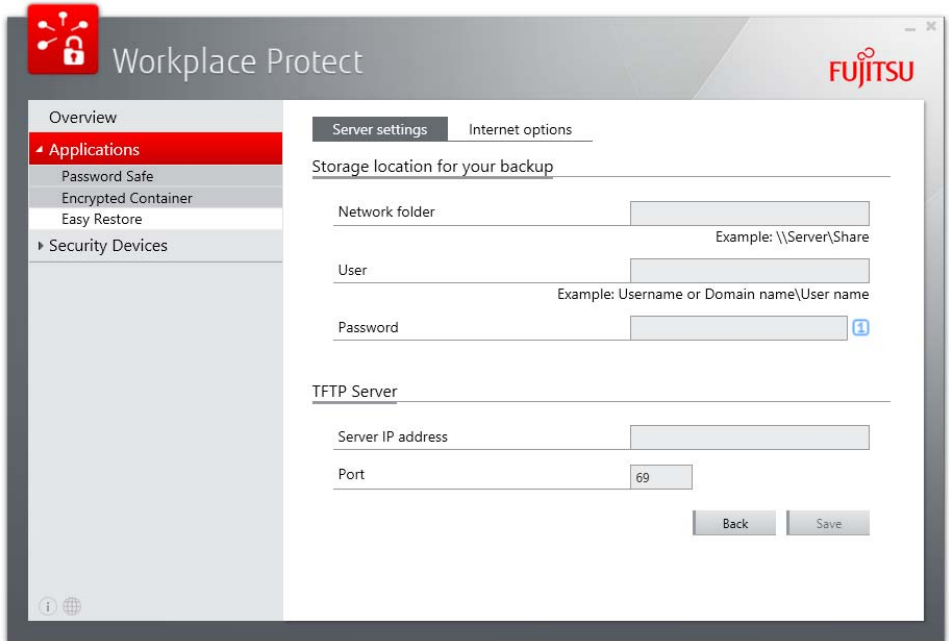
- ▶ The backup is saved on the server specified previously and is entered in the list of existing data backups.

Configure the server for backup/restore



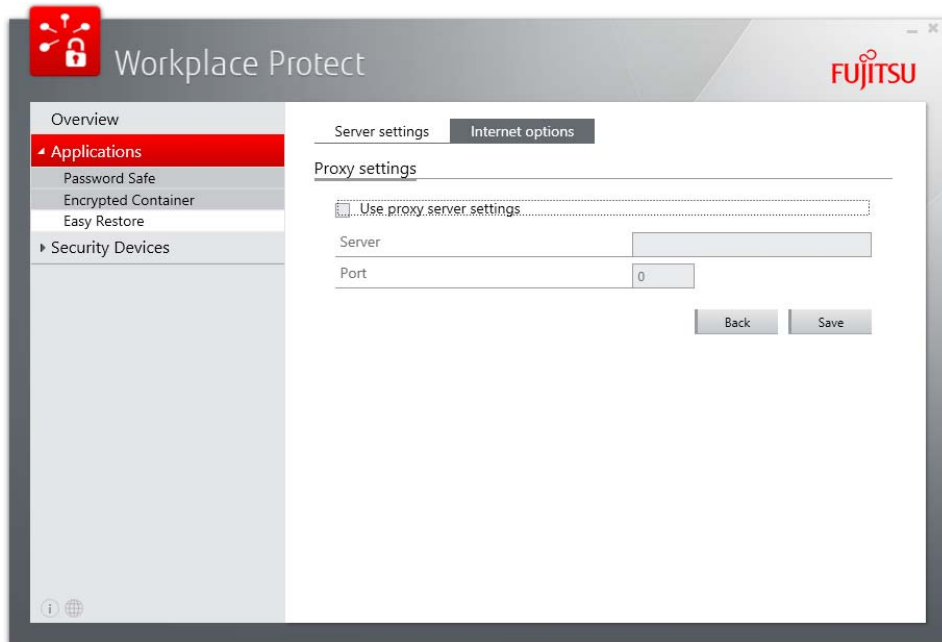
During the first start of *Easy Restore* or when there are changes in the storage location or server structure, the network folder and the TFTP server must be configured.

The settings are divided into two parts *Server settings* and *Internet options* (proxy settings).



Field	Function
<i>Server settings</i>	
<i>Network folder</i>	► Enter the path on which the backup should be saved.
<i>User</i>	► Enter your user name.
<i>Password</i>	► Enter a password.
<i>Confirm password</i>	► Confirm the password first entered (display/entry is dependent on the network configuration).
<i>Server IP address</i>	► Enter the IP address of the TFTP server on which the boot image (<i>Windows PE</i>) should be stored. You must ask your administrator for the address.
<i>Port</i>	► Enter the port. The standard port of the TFTP server is 69.
<i>Back</i>	Opens the Easy Restore start window.
<i>Save</i>	Checks and saves your entries

- ▶ If you are working with a proxy, click on the *Internet options* tab.



- ▶ Enter the *Proxy settings* that you have received from your administrator.
- ▶ This completes the requirements for saving the data.

Download boot image (Windows PE)

During the first start, the boot image must be downloaded from the Fujitsu Server.

If a new boot image is available, a message is displayed. You can then download the new image when required.

- ▶ To download the boot image, click on the button *Download* at the start of the boot process.



The button is only visible during the first start or if a new boot image is present.

The image is automatically stored on the TFTP server.

Restoring data

- ▶ To restore data, click the **F5** button during the start of the boot process:

The normal boot process is interrupted and the BIOS first displays the following message:

```
Easy Restore: Starting Restore. Please wait...
```

With a series of further displays, in which you also select the desired backup and must enter the associated password, the backup is written to the computer.

You receive a message when the restore is complete.

Using the security functions of Workplace Protect

Log on to the system again



With registration of the RFID card/RFID token, it is possible to log on at each logon screen by holding the card at the reader.

The logon method which was used last is used as the default logon method.

The available security devices are offered.

Field	Function
<i>Other users</i>	Enter user name and password
<i>Fingerprints</i>	Login with the recorded fingerprint
<i>Palm vein recognition</i>	Login with the recorded palm print
<i>Face recognition</i>	The success of face recognition depends on the light conditions.
<i>Insert the smartcard</i>	Login with smartcard

Log on to the system using a password

- ▶ Log on to the system with your user name and password, as described in the documentation for your operating system.

Log on to the system with biometric authentication options

If Multi-Factor Authentication has been set on the system, the associated additional identification must take place when selecting the security device. This will be requested automatically when the identification with the first factor has been completed.

- ▶ Click on the right-hand side on the desired logon option.

The chosen logon option is highlighted in blue.

- ▶ Follow the instructions on the screen.

Log on to the system with SmartCard



In administrator mode in *Windows 8* and *Windows 10*, it is only possible to login using the user account specified by the administrator.

If a specific user has been selected, the associated data on the smartcard will be read.

If *Other User* has been selected, all the user accounts which may be stored on the smart card will be displayed. The relevant user must then be selected.

- ▶ Click on *Fujitsu SmartCard logon*.
- ▶ Insert the SmartCard in the slot provided for it on your device.
- ▶ Enter the SmartCard PIN.

The logon data on the SmartCard is checked and used for the Windows logon.

TFTP server

TFTP (Trivial File Transfer Protocol) is a simple protocol for data transmission.

A TFTP server must be set up before *Easy PC Protection* can be used.

In doing so, any TFTP server that is compatible with RFC 1350, RFC 2347, RFC 2348 and RFC 2349 can be used. Alternatively, a Fujitsu *CELVIN NAS* with integrated TFTP server can also be used. A selection of chargeable and free TFTP servers for *Windows* is listed below:

- WinAgents TFTP server

<http://www.winagents.com/en/products/tftp-server/>

- Open TFTP server

<http://sourceforge.net/projects/tftp-server/>

- TFTP server

<http://tftpserver.codeplex.com/>

Alternatively, a Fujitsu *CELVIN NAS* with integrated TFTP server can also be used.

The following devices are thereby supported:

- *CELVIN® NAS Server Q902*
- *CELVIN® NAS Server QR802*
- *CELVIN® NAS Server Q802*
- *CELVIN® NAS Server Q800*
- *CELVIN® NAS Server Q700*

Setting up the TFTP server

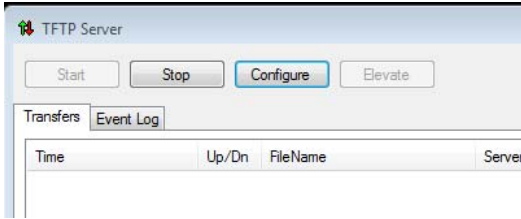


You need administrative rights for the installation.

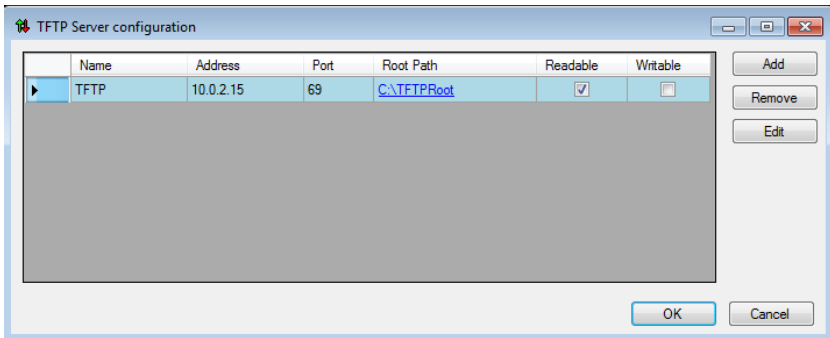
The TFTP server must be set up so that it responds on port 69 to incoming requests.

The following section describes an example of the configuration of the TFTP server from <http://tftpserver.codeplex.com/>, which also requires .NET 4.0.

- ▶ Download the required setup files from the website.
- ▶ Install the TFTP server on your server operating system.
- ▶ Start the program and click on *Configure* to set up a new TFTP server.

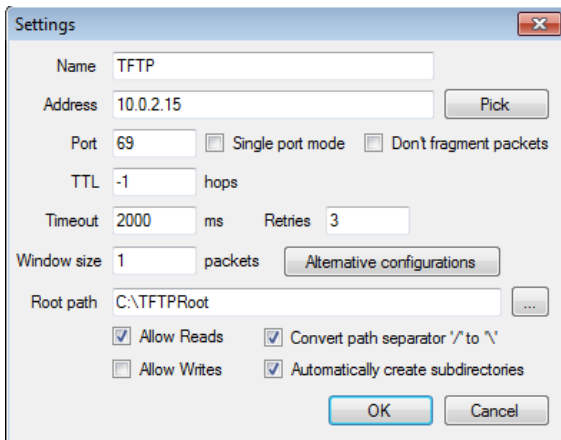


A configuration screen opens, in which you can add a new TFTP server.



- ▶ Click on *Add*.

The Settings window opens.





The IP address is an example and may differ from your system.

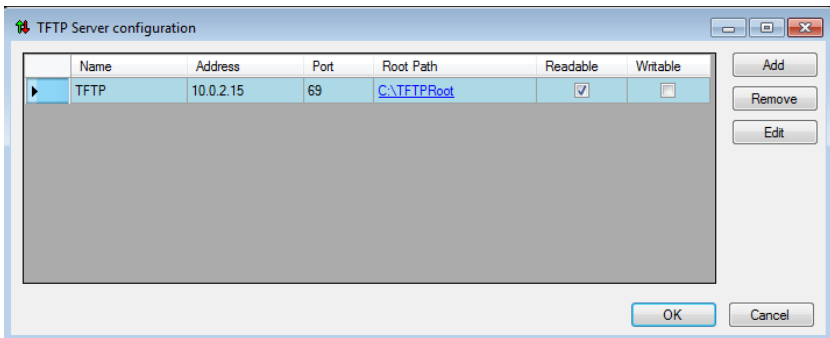
- ▶ Click on *Pick* to select the desired network interface and the matching IP address.



Please be careful to select an IPv4 address.

- ▶ Enter the root directory of the TFTP server in *Root path*.
All the files situated in the root directory can be reached using TFTP.
- ▶ Confirm your input with *OK*.

The server is shown in the configuration window.



- ▶ Confirm your input with *OK*.
- ▶ Start the server with *Start*.

The TFTP server is now available as a service via the network adapter chosen by you. All incoming and outgoing connection requests are clearly shown in the program window.

Manufacturer's notes

Open Source Software in Workplace Protect

Workplace Protect contains Open Source Software. Detailed information on this software can be found in the file `ThirdPartyLicenseReadme.txt`. This file is located in the *Workplace Protect* installation directory.