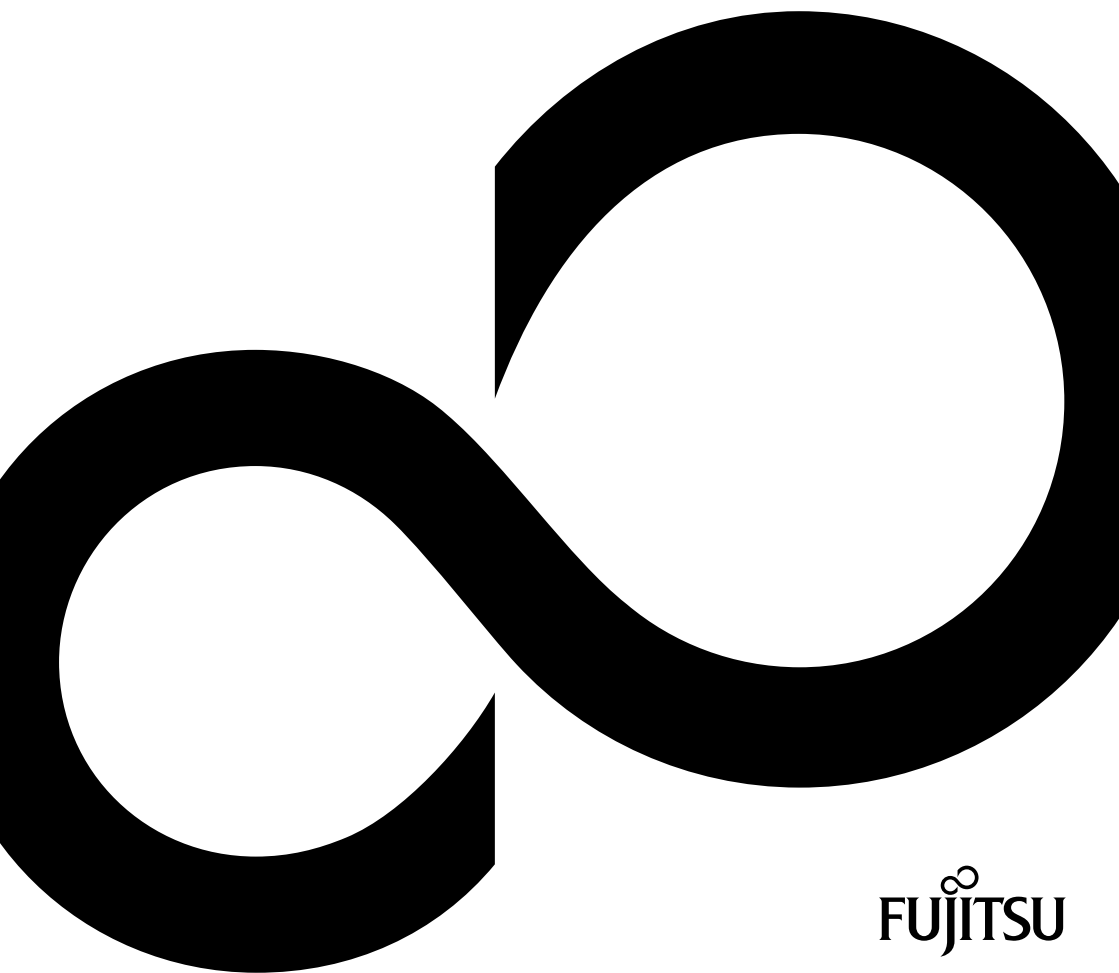


# Workplace Manager



## Congratulations on your purchase of an innovative product from Fujitsu.

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

For driver updates, go to: <http://fujitsu.com/fts/support>

If you have any technical questions, please contact:

- our Hotline/Service Desk: <http://support.ts.fujitsu.com/contact/servicedesk>
- your authorized distributor
- your sales office

We hope you enjoy working with your new Fujitsu product.



**Published by**

Fujitsu Technology Solutions GmbH  
Mies-van-der-Rohe-Straße 8  
80807 Munich, Germany

**Contact**

<http://fujitsu.com/fts>

**Copyright**

© Fujitsu Technology Solutions 2016. All rights reserved.

**Edition date**

08/2016

Edition 4

# Workplace Manager

## User Guide

<b>About this manual</b>	<b>1</b>
<b>The Workplace Manager concept</b>	<b>3</b>
<b>Overview – Components of Workplace Manager and Workplace Protect</b>	<b>5</b>
<b>Install Workplace Manager</b>	<b>6</b>
<b>Workplace Protect – install managed mode on the computers in the network</b>	<b>15</b>
<b>Start Workplace Manager</b>	<b>18</b>
<b>Configure Workplace Manager (first time)</b>	<b>20</b>
<b>SystemLock management</b>	<b>31</b>
<b>Job management</b>	<b>52</b>
<b>Workplace Manager Settings</b>	<b>83</b>
<b>Glossary</b>	<b>87</b>
<b>Index</b>	<b>91</b>

**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 and the Fujitsu logo are registered trademarks of Fujitsu Limited or its subsidiaries in the United States 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 properties 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

<b>About this manual .....</b>	<b>1</b>
Notational conventions .....	1
<b>The Workplace Manager concept .....</b>	<b>3</b>
<b>Install Workplace Manager .....</b>	<b>6</b>
Requirements .....	6
Set up the database server .....	7
Set up the database server .....	7
Install the Workplace Manager software .....	8
Install Workplace Manager Cockpit under Windows 10 .....	10
Installing Workplace Manager Cockpit .....	11
Connecting the Workplace Manager Cockpit to the server .....	11
Set firewall .....	12
Update and repair Workplace Manager .....	12
Workplace Manager versions/compatibility .....	13
Uninstall Workplace Manager .....	14
Uninstall the Workplace Manager Software .....	14
Uninstall database server .....	14
<b>Workplace Protect – install managed mode on the computers in the network .....</b>	<b>15</b>
Requirements .....	15
Workplace Manager and Workplace Protect .....	16
Install on the managed computers in the network .....	16
Workplace Protect – managed mode in Workplace Manager .....	17
Uninstall managed computers in the network .....	17
<b>Start Workplace Manager .....</b>	<b>18</b>
Required input during the first start .....	18
Overview – Workplace Manager User Interface .....	18
<b>Configure Workplace Manager (first time) .....</b>	<b>20</b>
Import computers .....	20
Group Computers – Group Management .....	21
Edit static and dynamic groups .....	22
Computer properties .....	25
Automatic update of computer details .....	25
Display computer details .....	25
Licensing .....	26
Purchase licences .....	27
Activate licences .....	28
Allocate licences to computers in the network .....	28
Handling registration problems .....	29
<b>SystemLock management .....</b>	<b>31</b>
SystemLock concept .....	31
System requirements .....	33
SmartCard .....	34
Putting SystemLock into operation and administrating .....	35
General procedure .....	35
Activation of SystemLock management in the Workplace Manager .....	36
Organisations and groups .....	37
Create organisations .....	37
Create groups .....	38

## Contents

---

Assign a computer to a SystemLock group .....	39
Import/add users .....	41
SmartCard types .....	42
Configure/write SmartCard types .....	43
SystemLock job settings (BIOS settings) .....	45
Change SystemLock settings .....	48
Uninstall SystemLock on the Computer .....	48
Unlock SmartCard PIN .....	49
Unlock SystemLock PC .....	49
<b>Job management .....</b>	<b>52</b>
Workplace Manager Versions and Job Compatibility .....	53
Setting up BIOS administration .....	53
Create/change/delete BIOS configuration list .....	55
Create BIOS configuration list from a (master) computer .....	56
Easy PC Protection .....	57
Requirements for the use of Easy PC Protection .....	57
Implementation of the Easy PC Protection function .....	58
Certificate settings .....	59
Schedule settings .....	60
Execute job .....	61
Change schedule settings .....	63
Change log in methods .....	63
Set up allowed applications .....	65
Define presence sensor settings .....	67
Auto BIOS Update .....	68
Make BIOS updates available .....	69
Allocate BIOS updates to computers .....	70
Show the user BIOS update messages .....	70
Setup Auto BIOS Update .....	71
Set BIOS password .....	72
Set BIOS user password .....	74
Set hard disk password .....	75
Password on boot settings .....	77
Advanced Face Recognition .....	78
Licences .....	78
Advanced Face Recognition licensing .....	79
Job-History / Delete jobs .....	80
<b>Workplace Manager Settings .....</b>	<b>83</b>
Set language and port .....	83
<b>TFTP Server .....</b>	<b>84</b>
Setting up the TFTP server .....	84
<b>Glossary .....</b>	<b>87</b>
<b>Index .....</b>	<b>91</b>



# About this manual

This manual is intended for all persons in your company who perform system management tasks (system administrators, service personnel).

The installation of the *Workplace Manager*, the installation of the extensions and the individual components are described in this manual.

## 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.

## Representation and spelling of command lines

The following special characters are used in command lines:

[ ]	Optional parameters
< >	Variables
{ }	Optional variables
	Parameters that can be used as alternatives

Parameters and variables are allowed in uppercase, lowercase, or a combination of both.

The values of variables can be entered with or without quotation marks.

# About Workplace Manager

*Workplace Manager* is a software which makes it easy for you to enter security settings for computers in a network.

*Workplace Manager* provides the following functions:

- Set up accesses in a network
- Centrally manage the security settings in a network.

The software and this manual are intended for network administrators in small to medium-sized networks.

*Workplace Manager* consists of the following components:

Component	Brief description
<i>Workplace Manager Cockpit</i>	The "My computer" of the administrator. Used to configure <i>Workplace Manager</i> . Is automatically installed on the Workplace Manager Server. Optional installation on a computer in the network with operating system Windows 10 is possible.
<i>Fujitsu Workplace Manager Server</i>	The server software
<i>Workplace Manager – Database</i>	Manages the computers, licences and settings in the network where <i>Workplace Manager</i> is installed
<i>Fujitsu Workplace Manager Client</i> (alternatively referred to as: <i>Workplace Protect</i> in managed mode)	Software which runs on the managed computers in the network on which <i>Workplace Manager</i> is installed

You will find a detailed description of the components below.

# The Workplace Manager concept

There are many different computers in your network, which you wish to administer using *Workplace Manager*.

You need to import these computer details into *Workplace Manager* and then group them together for administration purposes.

After the import, the *Workplace Protect - managed mode* program must be distributed to the computers in the network.

Computers in the network cannot be managed with *Workplace Manager* without licences. It is therefore necessary that you purchase licences, activate them and allocate them to computers in the network. Three test licences are available free for test purposes.

You can allocate jobs to the computer groups in the network if the *Workplace Manager* is set up accordingly:

- You can determine how your users should log in on their computers, according to the equipment on the computer e.g. by fingerprint, password or SmartCard.
- You can permit the use of a safe for passwords and the use of an encrypted data file directory.
- You can determine the actions when the user is present and when absent if a presence sensor is installed.
- You can define passwords for the hard disks and the BIOS.
- The user can also log into the system by face recognition, if additional licences are available and the computer is set up accordingly.

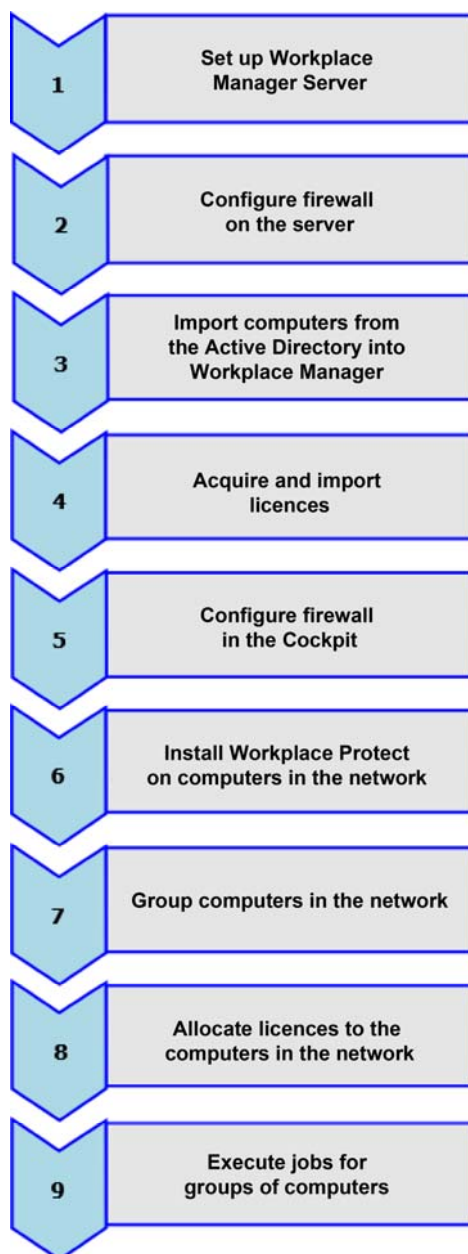
Multi-factor authentication is one of the most important main functions. It increases IT security in a network and guarantees that a user is actually the user he says he is. The more factors are used to determine the user's identity, the greater the level of security regarding genuine authenticity.

Management of the SystemLock pre-boot authentication solution, which is integrated in the BIOS (as an order option), is another main function. If *SystemLock* is activated on the computer, it can then only be booted with an initialised SmartCard (CardOS) and personal identification number (PIN). The SmartCard and PIN are checked in the BIOS during system boot, i.e. before the operating system starts.

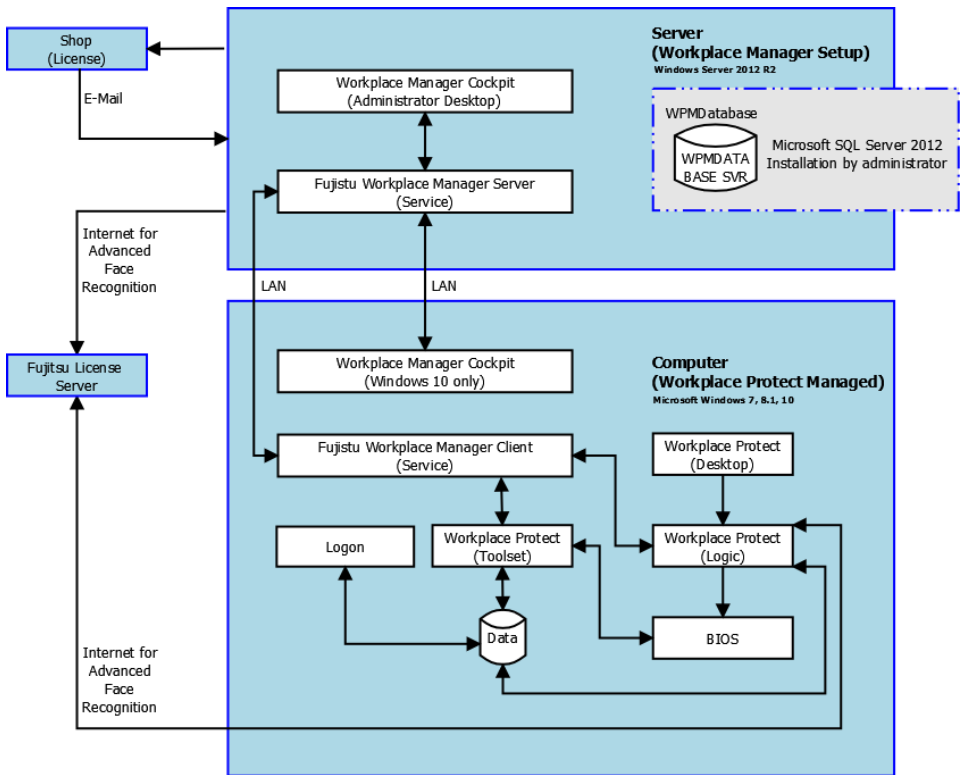
You can carry out the following tasks centrally in *SystemLock-Management*:

- Activate/deactivate the pre-boot authentication *SystemLock*-capable computers in your network.
- Determine the *SystemLock* settings
- Create access SmartCards with different authorisations
- Create and administer *SystemLock* organisations and groups
- Unlock PINs
- Unlock computers

Setting up *Workplace Manager* and working with *Workplace Manager* can be illustrated as follows:



## Overview – Components of Workplace Manager and Workplace Protect



# Install Workplace Manager

The installation proceeds in two steps:

- Set up the database server
- Install the *Workplace Manager* software

The installation package for *Workplace Manager* is found on the internet at

<http://www.fujitsu.com/fts/solutions/high-tech/solutions/workplace/security/secure/index.html>



You need administrative rights for the installation.



The database server and the *Workplace Manager* software must be installed on the same computer.

## Requirements

### Hardware

SmartCard reader, if *SystemLock* is to be worked with

### Operating system

*Windows Server® 2012 Standard R2*, 64 Bit

### Software

*Microsoft® .NET Framework 4.5* (is installed together with *Workplace Manager* if necessary)

*Microsoft® SQL Server® 2012 Service Pack 1 (SP1) Express*

You can download the software from the Microsoft Download Centre.

### Internet access

You need Internet access to activate the *Workplace Manager* licences.

## Set up the database server

A database server instance with the name **WPMDATABASESVR** must be installed. The instance must be set up with SQL authentication. The basis is the *Microsoft® SQL Server® 2012* data administration system

The password set up here will be needed later during installation of the *Workplace Manager* software.

For set up and installation, you can also adapt the sample files included in the installation package (folder **SQLPrepare**) to your environment and requirements.

The sample batch file **inst\_wpm\_dbs.bat** installs *Microsoft SQL Servers 2012 Express* and uses data from the file **ConfigurationFile\_SQL2012.ini** to set up the *Workplace Manager* data base instance with the name **WPMDATABASESVR**.

Please read the corresponding *Microsoft* documentation for additional information about installing *Microsoft SQL Server*.

### Installation directory in the file **inst\_wpm\_dbs.bat**

- In the sample batch file **inst\_wpm\_dbs.bat**, change the path to the SQL server package and remove the existing **rem** comment instructions in front of the path specification.



**Important:** In the batch file you must use the absolute path to the configuration file. Adapt the path specification according to your settings.

### Passwords in the file **ConfigurationFile\_SQL2012.ini**

- The settings from the sample file **ConfigurationFile\_SQL2012.ini** are used when setting up the server.
- Adapt the file **ConfigurationFile\_SQL2012.ini** to your environment. For instance, change the predefined password (**SAPWD=PWD1**).



**Important:** Write down all the settings, entries and the password and put these away in a safe place. You will need the password during installation of the *Workplace Manager* software or if you have to update or repair *Workplace Manager*.

## Set up the database server

- Start the set up of the database server by calling the file **inst\_wpm\_dbs.bat**.

Setting up the database server can take from 5 to 20 minutes depending on the computer system.

In the next step, the *Workplace Manager* software is installed with the administration interface (Cockpit), the server services and the database.

# Install the Workplace Manager software

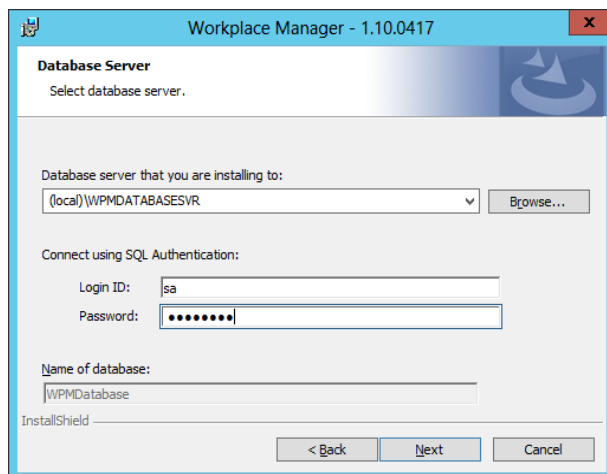
To install the *Workplace Manager* software, proceed as follows:

- ▶ Double-click on the file **WorkplaceManager\_Setup.exe**.

The wizard for installing the *Workplace Manager* is started.

- ▶ Read and accept the licence terms in the *Licence Agreement* window.

The *Database Server* window is opened, in which you enter the parameters necessary for creating a connection to the database server.



- ▶ Select the database server *(local)\WPMDATABASESVR*.
- ▶ Enter the username and associated password. You defined the password when installing the database server (see page 7).

The name of the database catalog is **WPMDatabase**. No change is possible.

- ▶ Confirm your entries with *Next*.

An error message appears if the selected database server does not exist.



The *Server-Client communication* window appears, in which you can define the ports for communication with the computers in the network on the server and configure the computers in the network.

The name of the *Workplace Manager* server on which the current installation is running is displayed.

The pre-set standard values **3298** for the **Server Port (TCP)** and the **Client Port (TCP)** can be changed if necessary.

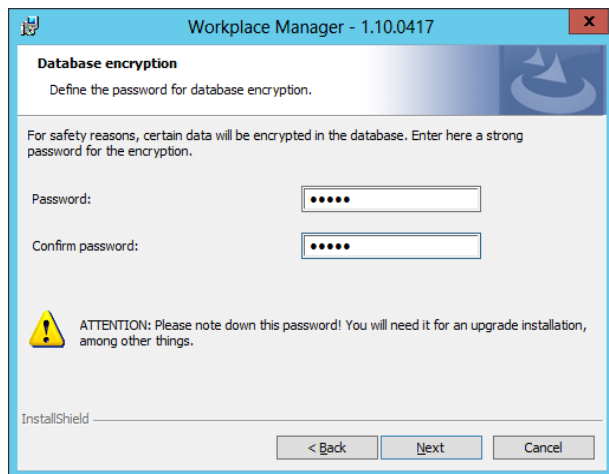


Make sure that the ports defined here have been unblocked in your installed firewall (see following section page 10).

You must specify the ports assigned here and the name of the *Workplace Manager* Server during the installation of *Workplace Protect*.

- Confirm your entries with *Next*.

Register the password for database encryption in the next window *Database Encryption*:



- ▶ Enter the password (at least 5 characters).
- ▶ Repeat the password entered to confirm it.



**Important:** Keep this password in a safe place. The password and database are encrypted.

Without the password, update or repair installation of the Workplace Manager *software* is not possible. If the password is not known, the database must possibly be reset meaning that all the settings and the information will be lost.

- ▶ Confirm your entries with *Next*.

All the required configuration data has now been specified. A window appears, in which the actual installation process is started.

- ▶ Click on *Install* to start the installation process.

A message appears when the installation process has completed successfully.

## Install Workplace Manager Cockpit under Windows 10

During installation of Workplace Manager, the graphical user interface (Workplace Manager Cockpit) is automatically installed on the server.

The Workplace Manager Cockpit can also be installed on the administrator's computer if operating system Windows 10 (64bit) is installed. With this type of installation, the network can be managed easily without switching computer workstation and without a remote connection to the server computer.

A connection to the Workplace Manager Server is established via the administrator's computer.



If several administrators are using the Cockpit at the same time, they must mutually agree the jobs. The most recently submitted job overwrites the previous jobs.

## Installing Workplace Manager Cockpit



Workplace Manager Cockpit

During installation of the server, the **WPMAdministrators** user group is set up automatically and the user, who is installing the server, is entered as a user.

The administrator, who will in future administrate *Workplace Manager* via the Cockpit on a *Windows 10* computer, should be added to this user group.



The version of the Cockpit on the *Workplace Manager Server* must be the same as the version on the computer with *Windows 10*.

To install the *Workplace Manager Cockpit* software on a computer with *Windows 10*, proceed as follows:

- ▶ Double-click on file **WorkplaceManager\_Setup.exe**, which you also used to install the server.


The wizard for installing *Workplace Manager* is started.

- ▶ Read and accept the licence terms in the *Licence Agreement* window.

Click on *Next* to start the installation and install the graphical user interface.

## Connecting the Workplace Manager Cockpit to the server

To connect the Cockpit on the *Windows 10* computer to the *Workplace Manager Server*, proceed as follows during initial start-up or following a change of server address or port.

- ▶ Start the *Workplace Manager Cockpit* using the administrator role.
- ▶ Click on  Application settings.
- ▶ Enter the server address and the port number.
- ▶ Click on OK.
- ▶ The connection to the server is established.
- ▶ In the *Login Workplace Manager Administrator* window, click on *Login*
- ▶ Enter the domain name, user name and user password.
- ▶ This user data must be stored on the server in the **WPMadministrors** user group.
- ▶ Confirm with *OK*.
- ▶ The programme is started.

### Set firewall

The following example for the *Windows* firewall shows the activation of the ports with the standard value of **3298** for the **server port** and the **client port**. Similar settings apply to other firewalls.

The example is executed in the command line in "Administrative Mode":

```
Set myport=3298
```

```
netsh advfirewall firewall add rule name="Workplace Manager incoming"  
dir=in action=allow protocol=TCP localport=%myport% remoteport=any
```

```
netsh advfirewall firewall add rule name="Workplace Manager outgoing"  
dir=out action=allow protocol=TCP localport=%myport% remoteport=any
```

### Update and repair Workplace Manager



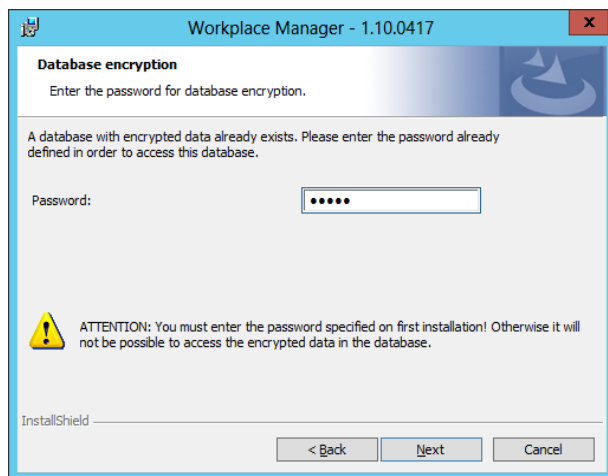
**Important:** Backup the *Workplace Manager* database before performing an update.

The installation package for *Workplace Manager* can be found on the Internet at <http://www.fujitsu.com/fts/solutions/high-tech/solutions/workplace/security/secure/index.html>

An update and repair installation is carried out much like the installation of the *Workplace Manager* software.

Assignment of the password for the database encryption is the only difference, the password cannot be reassigned.

- Follow the instructions as described above in chapter "Install the Workplace Manager software", page 8.



- Enter the database encryption password that you assigned during installation.

A message appears when the installation process has completed successfully.

## Workplace Manager versions/compatibility

The *Workplace Manager* modules (features) are continuously being further developed. Therefore, during installations and job creation, you must always note which module is possible with the *Workplace Manager* versions or feature set.

The following table provides an overview:

Function	<i>Workplace Manager 1.10/Feature set</i>	<i>Workplace Manager 1.11/Feature set</i>	<i>Workplace Manager 1.21/Feature set</i>
Easy PC Protection	-	2	2
Login methods	1	2	3 (*)
Enabled applications	1	2	2
Presence sensor	1	1	1
Auto BIOS Update	-	2	2
Hard disk password	1	1	1
BIOS password	1	1	1
SystemLock	1	1	1
BIOS user password	-	1	1
Password request during boot	-	1	1

The feature set is displayed in the computer properties. This allows you to see whether the client supports a specific feature.

You must decide whether you have to update the clients.

Example:

You cannot use *Workplace Manager 1.21* to adjust the login methods on computers in the network with *Workplace Protect 1.15*.

*Workplace Protect 1.21* (feature set 3) or higher must be installed on the computers in the network or you must forego the *Workplace Manager* update.

Support of feature numbers by client versions:

1 => WPP 1.10

2 => WPP 1.11, 1.12, 1.15

3 => WPP 1.21 (login with multi-factor authentication)

# Uninstall Workplace Manager

## Uninstall the Workplace Manager Software

- Uninstall *Workplace Manager* as software using the tools of your operating system.

The data in the *Workplace Manager* database is not deleted.

If the encryption password is known, you can access the data again by reinstalling.



BIOS settings that you have made using *Workplace Manager* (e.g. passwords, settings, SystemLock, Auto BIOS Update, Easy PC Protection) will not be reset during the uninstall.

## Uninstall database server



You can remove the database when you ensure that *SystemLock* is no longer activated on the computers in the network.

- Uninstall the *Workplace Manager* database using your operating system tools or *Microsoft® SQL Server® 2012*.

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

After installation of the *Workplace Manager* software and import of the computers (see page 20) the *Workplace Protect - managed mode* program must be distributed to the computers in the network. Depending on the operating system, use the 32 bit or the 64 bit version of the software.



Ensure that all computers that should be managed are visible in the group *All computers* (see chapter "Import computers", page 20).

The installation requires administrative rights.

## Requirements



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

### Hardware

Fujitsu computer, see FeatureFinder on the Internet at <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 patches for the operating system.

### Fujitsu drivers

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 licences for face recognition.

# Workplace Manager and Workplace Protect

This manual describes the current version of *Workplace Manager*.

If you have used a previous version, you should upgrade the computers in the network to the latest version of *Workplace Protect*. You will find details concerning this in the release notes for Workplace Manager and Workplace Protect. In Group Management you will find a group which provides you with a list of the Workplace Protect computers in the network which need updating.

## Install on the managed computers in the network

i

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 *Picture Password* (Windows 8 and Windows 10) and *PIN Password* (Windows 8) login methods are deactivated.

- 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.

i

If you have already installed a previous version of Workplace Protect, you can also use the upper command line for the update.

Please note that the ports are configured as with the predecessor installation.





Register the computer at *Fujitsu Workplace Manager Server* if the software on the computer is installed in the network.

The computers which have been registered on the server are displayed after an import of the computers (see page 20) in the working area *Group Management* (see page 21).

Computers with which there are problems when registering on the server are recorded in the *Registration Problems* list (see page 29).

This completes the installation of the managed computers in the network.



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 as a local version 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 their use is not ruled out by the administrator). You will find more information about these functions in the *Workplace Protect* 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 managed computers in the network



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

# Start Workplace Manager

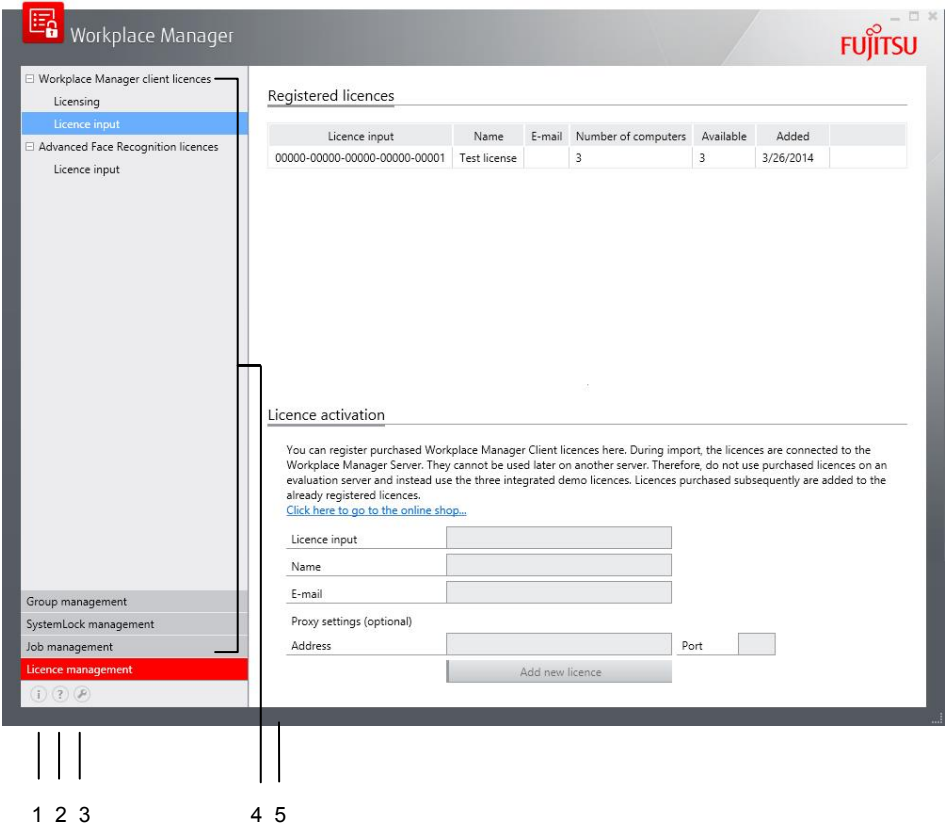
## Required input during the first start

You will be asked for the domain, user and password during the first start.




If a user different from the one who created the database should also be able to use *Workplace Manager*, this user must be added to the *WPM Administrators* group. This user can also login with their own user data.

## Overview – Workplace Manager User Interface

The windows in the *Workplace Manager* are always set up in a similar way:



- 1 Information about the current version and instructions about the Open Source licences used.
- 2 Access to the online manual
- 3 Settings
- 4 Navigation area
- 5 Working area

Area/Symbol	Description
Navigation area	Consists of 2 to 3 areas in which you navigate or select job and management tasks
Working area	Displays information and contains functions for the option selected in the navigation area.
	Displays the current software version
	Online manual
	Settings (See "Workplace Manager Settings", page 83)

# Configure Workplace Manager (first time)

You have set up the *Fujitsu Workplace Manager Server* (see page 7), installed the *Workplace Manager* software (see page 8) and distributed the software program *Workplace Protect – managed mode* to the computers (see page 21).


The following describes which steps are necessary to configure *Workplace Manager* for first time use.

## Import computers

There are a number of different computers in your network which you wish to administer using *Workplace Manager*.

You must import these computers:

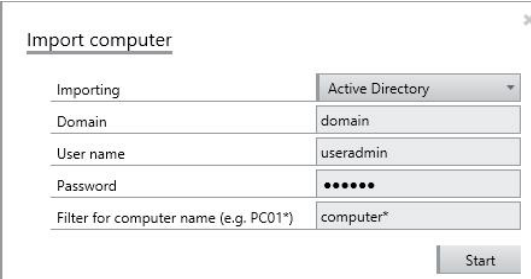
- for the first work with *Workplace Manager*
- always, when new computers are added to your network.

 Computers which experienced problems with registration on the server are recorded in the list of "Registration Problems" (see page 29).

- ▶ Select the option *Group Management* in the lower navigation area.
- ▶ Start the import with the context menu *Import computers* under the entry *System Groups* in the upper navigation area or with the *Import* button in the working area.

The *Import computers* window is opened.

- ▶ Select the option *Active Directory*.



- ▶ Enter the required information (login information of the user who is allowed to read the Active Directory) and click on the button *Start*.

If you do not wish to select all the computers from the Active Directory, you can enter the starting characters of the name or the desired name exactly at *Filter for computer name*. You can use "\*" as a wildcard (e.g. enter PC12\* to find all computers whose names start with PC12).

Computers which are deactivated in the Active Directory are not selected.

The imported computers are displayed in the group *All Computers*.

## Group Computers – Group Management

The imported computers in your network are displayed with the option *Group Management/All Computers* in the working area.



Groups can be created and changed only in *Group Management*. The groups are also visible in *Job Management* but cannot be edited there.

Group names must be unique.

You can sort the computers by clicking once in the column heading (e.g. with *Added*, by the date on which they were imported).

**Workplace Manager**

**Computer overview**

Computer to update (registered)



Licence	Version	Feature set	Computer name	Fully-qualified name	Registered
00000-00000-00000-00000-00001	1.10	1	WIN7X64-110-5	WIN7X64-110-5.poc.local	Yes
00000-00000-00000-00000-00001	1.10	1	WIN7X64-110-6	WIN7X64-110-6.poc.local	Yes
00000-00000-00000-00000-00001	1.10	1	WIN7X64-110-4	WIN7X64-110-4.poc.local	Yes
rKhV2-8HW80-p58cU-5Xa76-nOC5k-Dv24v	1.10	1	WIN7X64-110-14	WIN7X64-110-14.poc.local	Yes
rKhV2-8HW80-p58cU-5Xa76-nOC5k-Dv24v	1.10	1	WIN7X64-110-11	WIN7X64-110-11.poc.local	Yes
rKhV2-8HW80-p58cU-5Xa76-nOC5k-Dv24v	1.10	1	WIN7X64-110-10	WIN7X64-110-10.poc.local	Yes
rKhV2-8HW80-p58cU-5Xa76-nOC5k-Dv24v	1.10	1	WIN7X64-110-15	WIN7X64-110-15.poc.local	Yes
rKhV2-8HW80-p58cU-5Xa76-nOC5k-Dv24v	1.10	1	WIN7X64-110-12	WIN7X64-110-12.poc.local	Yes
rKhV2-8HW80-p58cU-5Xa76-nOC5k-Dv24v	1.10	1	WIN7X64-110-1	WIN7X64-110-1.poc.local	Yes
rKhV2-8HW80-p58cU-5Xa76-nOC5k-Dv24v	1.10	1	WIN7X64-110-13	WIN7X64-110-13.poc.local	Yes
rKhV2-8HW80-p58cU-5Xa76-nOC5k-Dv24v	1.10	1	WIN7X64-110-3	WIN7X64-110-3.poc.local	Yes
rKhV2-8HW80-p58cU-5Xa76-nOC5k-Dv24v	1.10	1	WIN7X64-110-2	WIN7X64-110-2.poc.local	Yes
rKhV2-8HW80-p58cU-5Xa76-nOC5k-Dv24v	1.10	1	WIN7X64-110-9	WIN7X64-110-9.poc.local	Yes
rKhV2-8HW80-p58cU-5Xa76-nOC5k-Dv24v	1.10	1	WIN7X64-110-8	WIN7X64-110-8.poc.local	Yes
rKhV2-8HW80-p58cU-5Xa76-nOC5k-Dv24v	1.10	1	WIN7X64-110-7	WIN7X64-110-7.poc.local	Yes

**Group management**

- SystemLock management
- Job management
- Licence management

You can use the corresponding functions in the navigation area to display the imported computers in the following groups:

System groups	The computers in the network are automatically allocated to the following fixed groups. You cannot change the allocation.	
	<i>Registered</i>	Computers which have been registered with the Workplace Manager
	<i>Licensed</i>	Computers for which <i>Workplace Manager Client</i> licences were assigned.
	<i>Unlicensed</i>	Computers on which no jobs can be executed since they are not licensed.

	Computers to update	Computers on which the previous version of Workplace Protect is installed and which therefore must be updated.
Static groups		You can group computers according to specific organisational criteria, e.g. all computers in a certain building or in a certain user group.  Jobs for these groups will be of a more organisational nature.
Dynamic groups		You can filter computers in the network according to certain equipment features and group them together, e.g. all computers with finger sensor.  Jobs for these groups will be system-dependent, e.g. login methods
SystemLock groups		Reference to the grouping for <i>SystemLock</i> is made in chapter "Create groups", page 38.

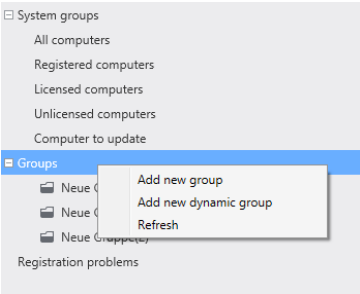


To execute a job with *Workplace Manager*, the computers must be allocated to a static or dynamic group. Group the individual computers according to particular criteria, e.g. location, model or equipment features.  
Group names must be unique.

## Edit static and dynamic groups

### How to create a static or dynamic group

- ▶ Mark the Groups entry in the display area and call up the context menu.



- ▶ Select Add new dynamic group or Add new group and enter the name you wish to give to the group.

### How to group the computers in your network

- ▶ Mark the entry *Groups* in the display area and call up the context menu.
- ▶ Select *Add new group* and enter the name you wish to give to the group.
- ▶ Mark the desired computers and drag these into a system group or a group created by you.

### How to arrange the computers into different groups

- ▶ Mark the desired computer in another group
- ▶ Drag the computer into the desired group.

The computer is copied and is now available in the different groups.

### How to allocate a computer to a new group

- ▶ Mark the desired computers and call up the context menu.
- ▶ Select Add to new group.

A new group is created, to which the marked computer is added.

- ▶ Enter a meaningful name for the group.

### How to copy a group

- ▶ Mark the group which you want to copy and call up the context menu.
- ▶ Select *Copy* and enter the desired name.

### How to rename a group

- ▶ Mark the group which you want to rename and call up the context menu.
- ▶ Select *Rename* and enter the desired name.

### How to delete a group

- ▶ Mark the group which you want to delete and call up the context menu.
- ▶ Select Delete from group and confirm with OK.

The computer is deleted from the group.

### How to delete a computer from the system



*SystemLock* must be deactivated.

- ▶ Mark the computer which you want to delete from the desired group and call up the context menu.
- ▶ Select Delete from system and confirm with OK.

The computer is removed from the *Workplace Manager* administration.

# Define and change filters for dynamic groups

## How to create filters for dynamic groups

Filters allow you to group together computers which share certain equipment features, e.g. a specific BIOS version.

The following filters are available:

- And/or

You can specify one or more criteria which must occur or which can occur as alternatives.
- Inventory property

Equipment feature that a computer must possess (e.g. BIOS version, hardware equipment)
- Operator

Defines whether or not the defined value must be fulfilled (equal to or not equal to)
- Value

Values that can be fulfilled (e.g. Manufacturer Fujitsu) are displayed according to the selected *Inventory property*.
- ✕

Deletes the filter element.

- ▶ Select the dynamic group whose filter you want to define.
- ▶ Define the filter criteria that a computer must meet in order to be displayed in the dynamic group.

Filter

And / or	Inventory property	Operator	Value		
	PalmVeinSensor	EQUALS	internal	✕	
AND	BiosVersion	CONTAINS	1.05	✕	

Save filter and apply

- ▶ Click on Save filter and apply.
- ▶ The computers that match the filter criteria are displayed in the work area.

## How to add new filter criteria


- ▶ Select the dynamic group whose filter you want to change.
- ▶ Double-click in the last blank row.
- ▶ The already defined criteria are displayed.
- ▶ Add the desired criteria.
- ▶ Click on Save filter and apply.
- ▶ The computers that match the filter criteria are displayed in the work area.



## How to change a filter criterion

- ▶ Select the dynamic group whose filter you want to change.
- ▶ Double-click on the line of the filter criterion you want to change.
- ▶ The already defined criteria are displayed.
- ▶ Change this criterion.
- ▶ Click on Save filter and apply.
- ▶ The computers that match the filter criteria are displayed in the work area.

## How to delete a filter criterion

- ▶ To delete a filter criterion, click on the symbol in the filter criterion line. 
- ▶ The line is deleted.
- ▶ Click on Save filter and apply.
- ▶ The computers that match the filter criteria are displayed in the work area.



### Applying filters

If a dynamic group is open, the filters are automatically updated when a computer in the network sends updated data.

If you click on Save filter and apply, the computers in the network are filtered again and displayed in the work area.

# Computer properties

## Automatic update of computer details

If a computer is registered in the *Workplace Manager*, the computer regularly synchronises its properties with the properties saved on the server. If something has been changed on the computer, e.g. BIOS Update, the new data is sent to the server and saved.

## Display computer details

If you require more detailed information about a computer on the network, you can have this information displayed.

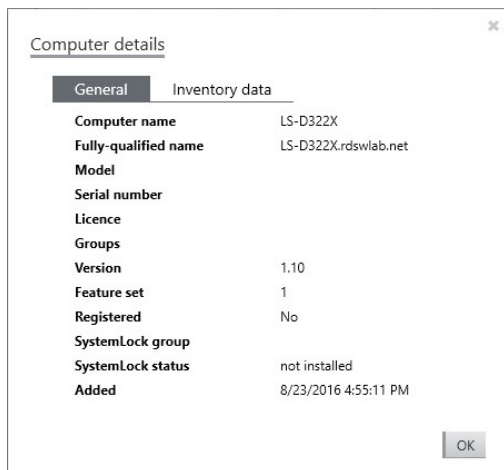
- ▶ Click on the group you want in *Group management*.

The computers of the group are displayed in the working area.

- ▶ Click on the computer you want in the *Computer overview* list.

A window will open displaying the details of the selected computer.

The assigned passwords are displayed on the *Inventory data* tab.



The screenshot shows a 'Computer details' dialog box with a close button (X) in the top right corner. It has two tabs: 'General' (selected) and 'Inventory data'. The 'General' tab contains the following information:

Computer name	LS-D322X
Fully-qualified name	LS-D322X.rdswwab.net
Model	
Serial number	
Licence	
Groups	
Version	1.10
Feature set	1
Registered	No
SystemLock group	
SystemLock status	not installed
Added	8/23/2016 4:55:11 PM

An 'OK' button is located at the bottom right of the dialog box.

## Licensing

A licence authorises the administration of a computer in the network with *Workplace Manager*. It is therefore necessary that you purchase licences, activate them and allocate them to computers in the network.



Please use the three test licences delivered to test the administration with *Workplace Manager*. These can be assigned once for test purposes.

The licence keys acquired and the allocation of licences to computers in the network are administrated using licence management (Option *Licence Management* in the navigation area).

Only computers on which the software *Workplace Protect – managed Mode* is installed and have been registered at *Fujitsu Workplace Manager Server* after installation can be licensed (see page 21).



In order to activate licences, it is necessary that the server can access the Internet.

A specified licence can no longer be deleted and used in another *Workplace Manager* installation.

## Purchase licences

Workplace Manager

**Licensing**

- Workplace Manager client licences
  - Licensing
    - Licence input**
  - Advanced Face Recognition licences
    - Licence input

**Registered licences**

Licence input	Name	E-mail	Number of computers	Available	Add
00000-00000-00000-00000-00001	Test license		3	3	26.03..

**Licence activation**

You can register purchased Workplace Manager Client licences here. During import, the licences are c Workplace Manager Server. They cannot be used later on another server. Therefore, do not use purch an evaluation server and instead use the three integrated demo licences. Licences purchased subsequ to the already registered licences.

[Click here to go to the online shop...](#)

Licence input

Name

E-mail

Proxy settings (optional)

Address  Port

► Purchase the necessary licences from your service partner.

Or

► Open the link *Click here to go to the online shop* and follow the instructions on the screen.



If you have purchased a licence, you will receive an email with an activation code at the email address specified.

Save the email in a secure place.

### Activate licences

You must activate the purchased licences in the working area *Licence activation*.

- ▶ Enter the activation code which you have received by email.
- ▶ Identify yourself with the name and email address which you gave during purchase.
- ▶ If necessary you must specify the proxy settings.
- ▶ Finalise your entries by clicking on the button *Add new licence*.

The licence codes purchased and activated are displayed in the working area under *Registered licences*.

### Allocate licences to computers in the network



The licences are linked to the server. This means that the licences or serial numbers of the computers which are processed on the server cannot simply be used on another server.

**Tip:** After each licensing save the LIC file (in the installation directory of *Workplace Manager* under **\License\WorkplaceManager.lic**). An existing LIC file is taken into account during a reinstallation of the server on the same computer with the matching serial number.



Please use the included 3 test licences to test the administration with *Workplace Manager*. These can be assigned once for test purposes.



Since version 1.11, licences which have been assigned once can be assigned again if the earlier already licenced system no longer exists in the network.

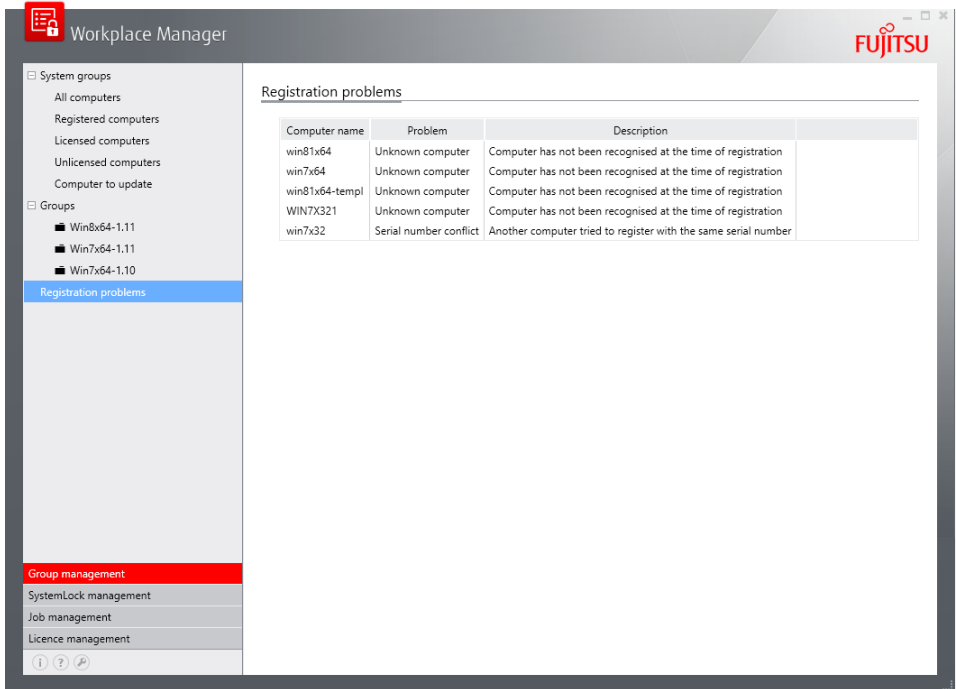
During deletion of the already licenced system, the licence is released again and is available for licensing of new computers in the network.

- ▶ Select the option Licence management / Licensing in the navigation area.
- ▶ In the list of unlicensed computers, mark those which you want to licence.
- ▶ Click on the Licensing button.

The selected computers are licenced.

## Handling registration problems

- In the lower navigation area, select the option *Registration problems*.



Workplace Manager

Registration problems

Computer name	Problem	Description
win81x64	Unknown computer	Computer has not been recognised at the time of registration
win7x64	Unknown computer	Computer has not been recognised at the time of registration
win81x64-templ	Unknown computer	Computer has not been recognised at the time of registration
WIN7X321	Unknown computer	Computer has not been recognised at the time of registration
win7x32	Serial number conflict	Another computer tried to register with the same serial number

Computers with which conflicts have occurred during registration are displayed in the working area.

Computers are recorded in the problem list for the following reasons:

- During registration, the computer has reported a serial number which is already in use by another registered computer.
  - Possible cause: The computer was renamed in the Active Directory and the registration was restarted.
  - **Important:** If the computer which had used the serial number was already licensed, its licence will be allocated to the new computer when it is approved.
- An already registered computer reports with a different serial number.
  - Possible cause: Hardware was changed in the computer and the registration was restarted.
  - If an already licenced computer is recorded in the problem list due to a serial number conflict (new registration of the computer with the same computer name, but different serial numbers) and if it is authorised for re-registration, its licensing is invalid. The computer must be licenced again for further administration.

- Computer models which are locked for administration with *Workplace Manager* (unsupported model).
- A computer which has not yet been imported has tried to log in.
  - Possible cause: The computer tries to log in before it was imported by the Active Directory.
  - Possible cause: A known computer was renamed in the Active Directory and the registration was restarted, but the computer has not yet been imported into the *Workplace Manager*. As a result the computer is not recognised by the system (fully qualified name is not known).

### To resolve the problem

You have two ways of handling problematic computers:

- ▶ *Allow*: The computer is prepared for re-registration and a re-registration is initiated on the computer. The serial number, registration status, model and if necessary licensing (only with serial number conflict) are reset when preparing the computer.
- ▶ *Deny*: The problematic computer is removed from the problem list, but will be re-entered into the list if it tries to register itself again.

# SystemLock management

*SystemLock* is the pre-boot authentication solution from Fujitsu, which is integrated into BIOS (as an order option). If *SystemLock* is activated on a computer, it can then only be booted with an initialised SmartCard (CardOS) and personal identification number (PIN). The SmartCard and PIN are checked in the BIOS during system boot, i.e. before the operating system starts.

You can carry out the following tasks centrally on the administrator console in *SystemLock Management*:

- Activate/deactivate the pre-boot authentication *SystemLock*-capable computers in your network.
- Determine the *SystemLock* settings
- Create access SmartCards with different authorisations
- Create and administrate *SystemLock Organisations* and *SystemLock Groups*



With incorrect settings and in some circumstances, you can irrevocably lock individual computers or networks in *SystemLock*.

Please read the following description closely and follow the instructions described.

## SystemLock concept

You can define access rights with *SystemLock* and write on SmartCards which enable or deny user access to particular computers in your network.

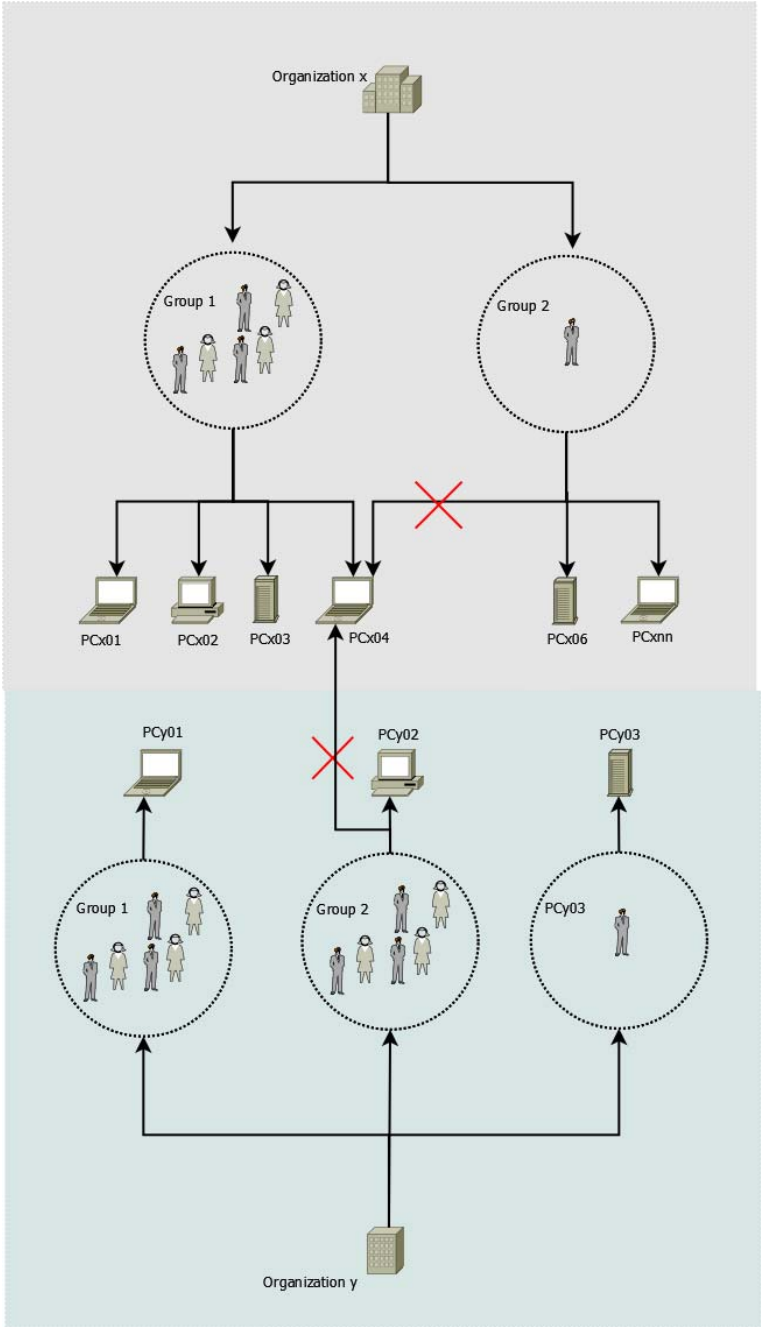
The individual computers are allocated to an organisation, in which different groups are defined.

A computer can only be allocated to one group of this organisation.

A user who has the SmartCard for this group has access to all computers which are in this group.

You can also allocate a single computer just to its own "Group". A "Single Group" is referred to when allocating a computer just to its own group. In that case, the name of the computer must also be the name of this single group. You create a personal computer in the literal sense with individual groups, with which an individual user has access to "their own" PC with the right SmartCard. If you duplicate this SmartCard and pass it on to other users, you can also create a scenario in which several users share just one computer.

If a computer is allocated to a group which is not an individual group, there are normally several computers which belong to this group. All users who possess a SmartCard for this group can access any computer of this group. Hence for example, five users can share three computers or one user can access just five computers.





# System requirements

**Computer:**

The *SystemLock* must have been requested with the computer otherwise the functions are not included in the BIOS of the computer.

Please contact your Fujitsu contact person to check whether a subsequent acquisition of *SystemLock* is possible on your systems.

**SmartCard:**

The following SmartCards are supported by the *SystemLock* manager:

- Smartcard CardOS V 4.4 and SIEMENS ® Smartcard CardOS V 4.3b

Only SmartCards which have been purchased from and initialised by Fujitsu Technology Solutions are supported.

**SmartCard reader:**

The following SmartCard readers are supported:

- SCR USB2.0 Intern
- Dual Smartcard Reader D321
- SCR USB Solo 3
- CLOUD 2700R
- SCR 3500
- SCA Express card
- Readers integrated in LIFEBOOK

**Keyboards with integrated SmartCard readers:**

The following keyboards with SmartCard readers are supported:

- KB SCR (K528)
- KB SCR eSIG (K529)
- KB SCR2 (K538)
- KB SCR2 eSIG (K539)
- KB SCR Pro (K328, K329)

If necessary, refer to the documentation included with your SmartCard reader for instructions on driver installation.

### SmartCard

A SmartCard is used to save security-related data. Basically, it consists of memory which records data and an upstream micro-controller which monitors access to this data. Access to the security-relevant data is protected by a PIN (Personal Identification Number). A locked SmartCard can be unlocked again using the PUK (Personal Unlock Key).

#### Important notes for handling SmartCards

To ensure the security of your access protection, you should observe the following:

- The first time you use your SmartCard, you must enter the preset PIN disclosed to you by the SmartCard manufacturer or your system administrator.
- When delivered, the preset PIN and PUK numbers for the above-mentioned supported SmartCards are "12345678". For security reasons, we strongly recommend that the particular user changes the PIN and PUK immediately, provided authorisation to do so has been granted by the administrator.
- Both secret numbers must have a minimum of four and a maximum of eight digits. Do not use combinations that are easy to guess, such as number sequences (e.g. 2345...) or repetitions (e.g. 4444).
- The SmartCard can only be used with a PIN, so protection is maintained even if the SmartCard is lost.
- If the PIN is entered incorrectly three times, the SmartCard is locked and can no longer be used. It must be unlocked with the PUK.
- If the PUK is entered incorrectly ten times, the SmartCard is locked and can no longer be used.
- In general, it is advisable to create backup copies of SmartCards, and especially of Administrator SmartCards.
- Always keep one of the SmartCards in a safe place if you are carrying the other SmartCard with you. Think of the SmartCard in the same way as your car keys, of which you also have a spare set that you normally keep in a safe place.

#### SmartCard reader

There is either a SmartCard reader integrated in your computer or you have connected a SmartCard reader.

With the appropriate SmartCards and the associated software, you can also use your SmartCard reader for the digital signature, e-mail encryption or for home banking.

##### Insert the SmartCard



Do not use force when inserting and removing the SmartCard.

Make sure that foreign objects do not fall into the SmartCard reader.

# Putting SystemLock into operation and administrating

## General procedure

If you want to use *SystemLock* in your network, you must first enable it in *Workplace Manager*. For this purpose, you need a SmartCard which then automatically becomes the *Database Administrator SmartCard*.



You will need the *Database Administrator SmartCard* from this time on, to be able to operate the *Workplace Manager Cockpit*. This also applies to *Workplace Manager* tasks which are not associated with *SystemLock*.

For security reasons, create one or more additional *Database Administrator SmartCards*, so that you will continue to have access to the database if the first card is lost.

You configure the cards which you need in your company in the database using the *Database Administrator SmartCard*.

For this purpose, you must set up at least one organisation (see page 37) and at least one group (see page 38) within this organisation.

You allocate a computer to the group. A computer can only be allocated to one group.

Afterwards you assign the necessary rights for each individual computer/user.

At first, all your information is only stored in the database.

If required you can also write to the necessary SmartCards immediately after configuration.



The PIN and PUK are automatically generated during configuration.

You can also notify the user in your company that a SmartCard was prepared and that they can collect this from a central office. The central office accesses the configuration stored in the database with the *Personalisation SmartCard* and issues the SmartCard for the user.

If you are sure that all users have their SmartCards, you can switch on the *SystemLock* functionality in the BIOS of the systems on those computers in the network which are equipped with the *SystemLock* function.

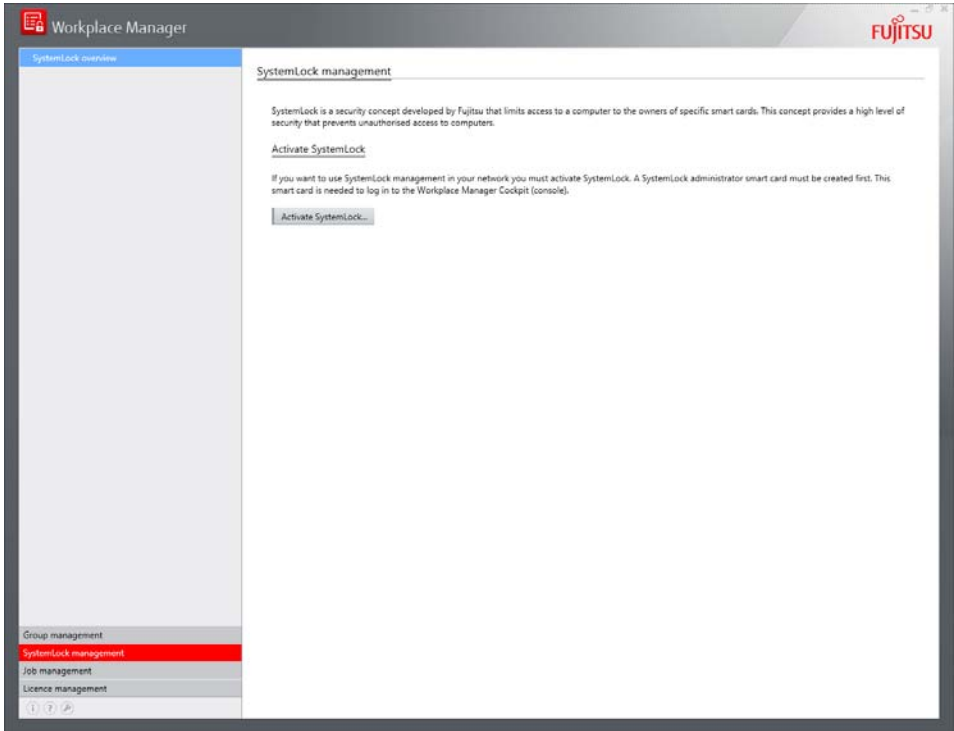
Activation occurs via the *SystemLock job* in Job Management in the *Workplace Manager*.

# Activation of SystemLock management in the Workplace Manager



Make certain that there is no SmartCard still in the reader.

- Select the option *SystemLock management* in the lower navigation area.



- Click on the *Activate SystemLock* button.

The following window opens:



- Insert an empty SmartCard into the reader.

The reader will automatically be recognised.



A PUK must contain 4 to 8 digits.

- Enter the PUK and confirm your entry with *OK*.

You will need to know the PUK assigned to the SmartCard if you want to use an already initialised SmartCard.

A new SmartCard has the number sequence 12345678 as PIN and PUK.



The first SmartCard automatically becomes the *Database Administrator SmartCard*.

## Organisations and groups

To be able to execute a *SystemLock* job, computers must be assigned to organisations and groups. With this mapping you can portray the access concepts with corresponding access rights in your company (see page 42).

The name of an organisation and group must be unique.

## Create organisations

- Select the option *Organisations and SystemLock Groups* in the upper navigation area and select the entry *Set up SystemLock Organisation* in the context menu.

The following window opens:

New organisation

Name

Unlock password

Password confirmation

If you want to generate an unlock code for Fujitsu support, you must specify a password here.

OK Cancel



The password is optional. With the help of Fujitsu Support you can activate the computer with activated *SystemLock* using the password, see the following section.

- Enter a unique name for the organisation.
- If you want to access Fujitsu Support, assign a password and confirm it.
- Confirm the entries with *OK*.

### Password for Service Activation

In an emergency, (e.g. faulty card, incorrect code entered several times), Fujitsu Service can activate your computer (see chapter "Unlock SystemLock PC", page 49).

**Requirement:** On creating a new organisation, you assign a password which will be requested during activation.

- ▶ If you do not want activation by Fujitsu Service, leave the input field *Unlock password* empty.
- ▶ If you wish to allow activation by Fujitsu Service, enter the password.
- ▶ The password is accepted with the button *OK*.
- ▶ The password is saved in the BIOS and the dialogue window closes.



Keep this password in a safe place.

### Create groups

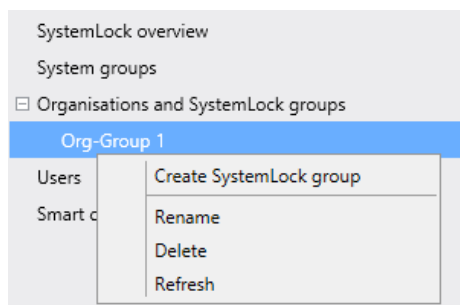
The creation of the *SystemLock* groups is similar to processes in *Group Management*. A computer can be assigned to a single *SystemLock* group in contrast to the *SystemManager* groups.



A distinction is made between the following *SystemLock* groups:

- a group to which several computers can be assigned.
- a single group to which just one computer is assigned. This group must have the same name as the computer. This group can also not be assigned to any additional computer later on.

The number of groups is limited to 65,534.



### How to create a group within an organisation

- ▶ Mark the desired organisation in the working area and call up the context menu.
- ▶ Select *Create SystemLock Group* and enter the desired name for the group.

### How to rename a group



A group can only be renamed if no computer is allocated to it.

- ▶ Mark the group which you want to rename and call up the context menu.
- ▶ Select *Rename* and enter the desired name.

### How to delete a group



A group can only be deleted when no computers are allocated to it.

A computer is deleted from the group via the *SystemLock Job Uninstalling SystemLock* (see page 40).

- ▶ Mark the group which you want to delete and call up the context menu.
- ▶ Select *Delete* and confirm with *OK*.

The group is deleted.

### How to update the view in the work area

- ▶ Select *Refresh*.

The changes made by you in the *SystemLock Groups* are displayed in the working area.

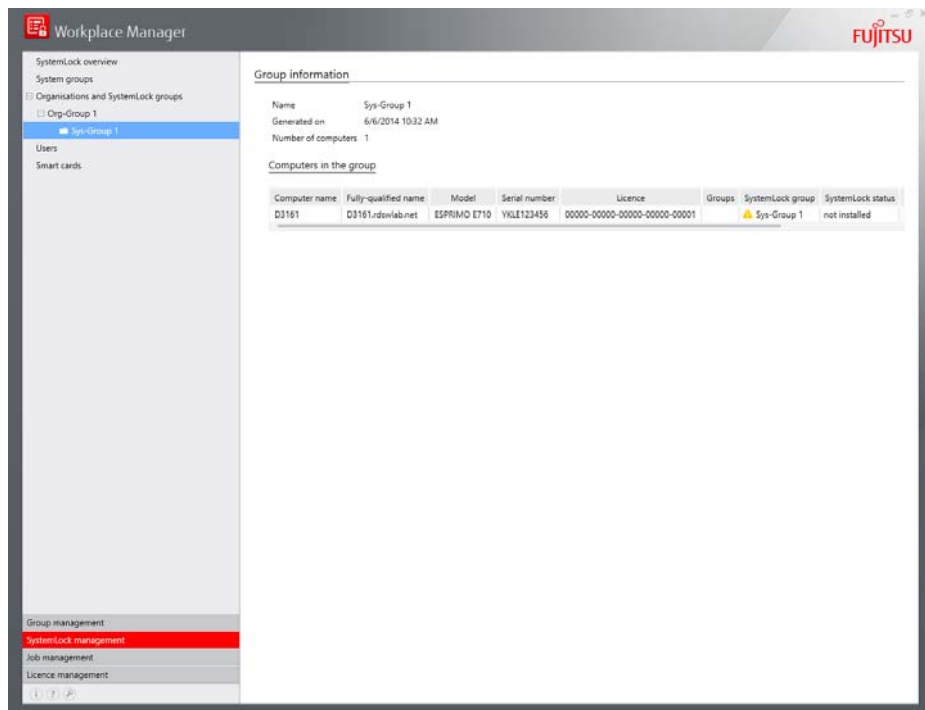
## Assign a computer to a SystemLock group



When you assign a computer to an organisation, a *SystemLock* single group is generated for this computer. Therefore the users of an organisation have access to just one computer in the organisation with their SmartCard.

When you assign a computer to a group, the "Group Members" have access to all computers in the group with their SmartCard.

Moving computers between groups is not possible.



## How to create a single group within an organisation

- ▶ Mark the desired computers in the system groups and drag these into the organisation created.

A yellow triangle appears in front of the computer name, provided *SystemLock* is not activated on the computer.

## How to assign a computer to a group

- ▶ Mark the desired computer and drag it into the group created.

A yellow triangle appears in front of the computer name, provided *SystemLock* is not activated on the computer.

## How to delete a computer from a group



The deletion of computers from *SystemLock* groups is only possible if *SystemLock* is not installed and no *SystemLock Job* is open.

Computers on which the *SystemLock* is installed are automatically deleted if the *Uninstall SystemLock Job* was carried out successfully.

- ▶ Mark the computer which you want to delete from the desired group and call up the context menu.
- ▶ Select *Delete* and confirm with *OK*.

The computer is deleted from the group.



## Import/add users

SmartCards are assigned to users (except for the initialisation SmartCard during enabling of *SystemLock*). This is why it is necessary to create or import the users.

### How to import users

- ▶ In the navigation area, right-click with the mouse on the Users entry to open the context menu.
- ▶ Select the Import user entry.
- ▶ In the following dialogue window, enter the Domain, User name and Password.
- ▶ Click on Start to import the users

### How to add single users

- ▶ In the navigation area, right-click with the mouse on the Add user entry to open the context menu.
- ▶ Select the Add user entry.
- ▶ In the following dialogue window, enter the user's full name, the user name and e-mail address.
- ▶ Click on Save & Close to create the user and complete the process.

or

- ▶ Click on Save & New to create the user and to add another user.

or

- ▶ Click on Cancel to close the window without any changes.

### How to rename a group



A group can only be renamed if no computer is allocated to it.

- ▶ Mark the group which you want to rename and call up the context menu.
- ▶ Select *Rename* and enter the desired name.

### How to delete a group



A group can only be deleted when no computers are allocated to it.

A computer is deleted from the group via the *SystemLock Job Uninstalling SystemLock* (see page 40).

- ▶ Mark the group which you want to delete and call up the context menu.
- ▶ Select *Delete* and confirm with *OK*.

The group is deleted.

### How to update the view in the working area

- ▶ Select *Refresh*.

The changes made by you in the *SystemLock Groups* are displayed in the working area.

### SmartCard types

A new SmartCard initially only has a preset PIN and PUK. Access rights and the individual PIN and PUK are only assigned when the SmartCard is initialised.

You can create different types of SmartCards with *Workplace Manager*:

- Cards for administering the *SystemLock* environment in the network.
- Cards which control access to the systems at organisational and group level and allow or block particular functions (e.g. BIOS, system start).

The following SmartCards are used in *Workplace Manager*:

- The *Database Administrator SmartCard* is initially created during the activation of *SystemLock*. The card is necessary:
  - to define the *SystemLock* network environment with organisations, groups, users and SmartCards
  - to create SmartCards and administer the *SystemLock* function in the BIOS of computers via *Workplace Manager*
- *Personalisation SmartCard* allows the generation of SmartCards in accordance with the guidelines defined by the database administrator.

The following SmartCards control access to the computers in the network:

- Access within the associated *SystemLock* group (on site):
  - *Administrator SmartCard* (Administrator via the allocated *SystemLock* group, uninstalling *SystemLock*)
  - *Service SmartCard* (BIOS settings)
  - *Superuser SmartCard* (BIOS settings, system start)
  - *User SmartCard* (system start)
- Access within all groups of an organisation (on site):
  - *Organisations Service SmartCard* (service SmartCard for all groups of an organisation, BIOS)
  - *Organisation Administrator SmartCard* (Administrator SmartCard at organisation level. necessary for example for the local administration of single groups)

All these SmartCards can change their PIN and unblock a blocked SmartCard with knowledge of the PUK and authorisation of the administrator.

	User SmartCard		SuperUser SmartCard		Service SmartCard		Admin SmartCard	
	PIN	PUK	PIN	PUK	PIN	PUK	PIN	PUK
System start	x		x				x	
Call <i>BIOS Setup</i>			x		x		x	
Change own PIN	x		x		x		x	
Unlock own blocked SmartCards via the software		x		x		x		x
Unlock own blocked SmartCards in BIOS		x*		x*		x*		x
<i>SystemLock</i> activate/uninstall							x**	

\* Configured in BIOS setup (designation of the BIOS setting: Unlock SmartCard)

\*\* If allowed in BIOS Setup

## Configure/write SmartCard types

### Warning



Please be aware you carry a great responsibility when configuring and writing SmartCards. An incorrect procedure can permanently lock individual computers, groups of computers or in extreme cases all computers.



When configuring SmartCard types your settings are initially entered only in the database. Your settings are written onto the SmartCard and saved in the database when writing.

### Database Administrator SmartCard



When first switching on *SystemLock* the first SmartCard becomes the Database Administrator SmartCard. With this card you have access to the database in which you enter organisations and groups and assign the computers in the network.



Keep this SmartCard safe, since you have no access to the database without it.

Additional SmartCard types

- ▶ In the working area, select the computer for which you want to configure the SmartCard.
- ▶ Select the option *SmartCards* in the navigation area and open the context menu.
- ▶ Select *SmartCard configuration*.

The following window opens:

Smart card configuration

Smart card configuration

Current step1/1

UserTester

Smart card typeUser

SystemLock groupLab1

☐ Enables SystemLock activation on following computer

Computer name:

☐ Generating PIN and PUK for new smart cards

Save

Generate

Skip

- ▶ Select your desired *SmartCard type*:

SmartCard type	Description
Administrator	Boot system, make changes in BIOS Setup, change PIN, uninstall <i>SystemLock</i> , initialise SmartCards, unlock SmartCards
Database Administrator	Only access to the database
Personalisation service	Generating SmartCards according to the database administrator definitions
Organisation administrator	Administration within a <i>SystemLock</i> organisation
Organisation service	Service SmartCard for all groups of an organisation, BIOS settings.
Service	Changes in the BIOS setup
Superuser	Boot system, make changes in BIOS Setup, change PIN
User	Boot system, change PIN

- ▶ Select the desired *SystemLock group* which you previously created
- ▶ When you mark the option *Enable SystemLock activation on the following computer*, an input field appears where you have to specify the name of the computer.
- ▶ When you mark the option *Generate PIN and PUK for new SmartCards*, the PIN and PUK are automatically generated and entered into the database.



A new SmartCard has the digit sequence 12345678 as standard PIN and standard PUK.

If the option *Generate PIN and PUK for new SmartCards* is not selected and the standard PUK was not changed, the standard PIN is written in the database.

The PUK is requested if the PIN and PUK were already changed. This is written in the database. In this case the PIN remains unchanged.

The entries on the SmartCard can be displayed with *SystemLock Management/SmartCards*.

The order is entered into Job Management.

## SystemLock job settings (BIOS settings)



*SystemLock* jobs can only be executed on computers which are allocated to a *SystemLock* group.

► Select *Jobs/SystemLock* in the navigation area.




The computers for which SmartCard types are defined are displayed in the upper navigation area.


### Symbol overview - navigation area

	Refers to groups of computers for which SystemLock jobs are still pending
	SystemLock computer
	SystemLock change has not yet been carried out for client
	SystemLock organisation
	Refers to SystemLock organisations for which SystemLock jobs are still pending
	SystemLock group
	Refers to SystemLock groups for which SystemLock jobs are still pending
	The exclamation mark indicates that changes are pending



- Select the desired settings as follows:

Setting	Description
<i>Action</i>	
<i>Install SystemLock</i>	<p><i>SystemLock</i> is installed on the computer. Activation is carried out by the user by switching on the computer and inserting the SmartCard generated for them.</p> <p> Test whether the computer is actually intended for installation.</p>
<i>Activate immediately</i>	<p>Immediately activates <i>SystemLock</i> on the selected computer in the network</p> <p> Ensure that the user already possesses a functioning SmartCard which grants access to the computer.</p>
<i>Change settings</i>	Allows change of the settings already entered into the database.
<i>Uninstall SystemLock</i>	<p>Uninstalls <i>SystemLock</i> on the selected computer in the network.</p> <p> Test whether the computers are actually intended for uninstalling.</p>

Setting	Description
<i>Request for SmartCard and PIN</i>	
<i>Request PIN during every boot</i>	Requires PIN entry on each restart
<i>Allow Wake on LAN without PIN</i>	<p>Allows system changes via the network.</p> <p> This permission represents a security risk, since an unauthorised user can gain access to the computer with this setting.</p>

Setting	Description
<i>Support for Single Sign-On (SSO)</i>	Authentication information is forwarded to the operating system to automate the login. Additional software is required for this. Please find out more from your specialised dealer.
<i>Users can reset PIN</i>	Allows the unblocking of the PIN
<i>BIOS changes are allowed</i>	Allows changes in BIOS

- ▶ Click on the *Execute* button to write the changed BIOS settings into the BIOS.

The settings are written into the BIOS upon activating the computer in the network.

### Change SystemLock settings

- ▶ Insert the Admin SmartCard into the reader.
- ▶ Enter the PIN and confirm the entry with *OK*.
- ▶ Select the desired *SystemLock* group.
- ▶ In the working area, select the computer from which you want to uninstall *SystemLock*.
- ▶ Select *Job/SystemLock* in the navigation area.
- ▶ Click on the action *Change settings*.

Change the desired settings as described above (see chapter "SystemLock job settings (BIOS settings)" Page 45)

- ▶ Assign a job name and click on *Execute*.

The *SystemLock* data is changed in BIOS.

The settings are written into the BIOS upon activating the computer in the network.

### Uninstall SystemLock on the Computer

- ▶ Insert the Admin SmartCard into the reader.
- ▶ Enter the PIN and confirm the entry with *OK*.
- ▶ Select the desired *SystemLock* group.
- ▶ In the working area, select the computer from which you want to uninstall *SystemLock*.
- ▶ Select *Job/SystemLock* in the navigation area.
- ▶ Click on *Uninstall SystemLock*.
- ▶ Assign a job name and click on *Execute*.

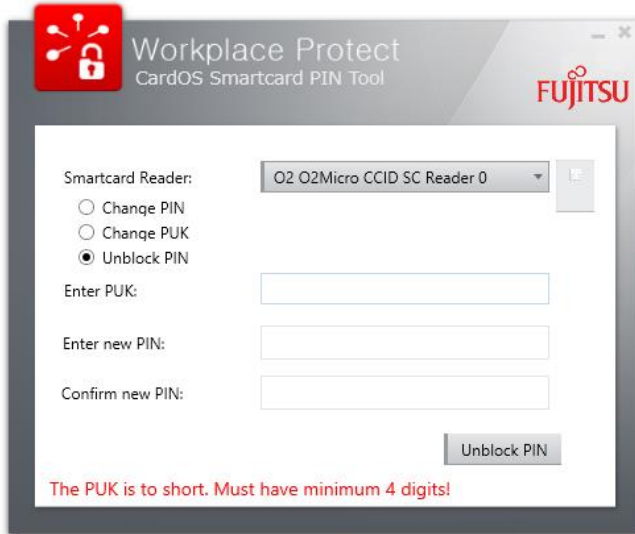
The *SystemLock* data is changed in BIOS.

The settings are written into the BIOS upon activating the computer in the network. *SystemLock* is uninstalled.



## Unlock SmartCard PIN

If a user has locked their SmartCard you can unlock it with the tool *Workplace Protect – CardOS SmartCard PIN Tool*. For this purpose, you must know the PUK of the SmartCard.



*Workplace Protect – CardOS SmartCard PIN Tool* is installed with the *Workplace Manager* setup in the folder `%programfiles%\Fujitsu\Workplace Manager\Admin\Tools`.

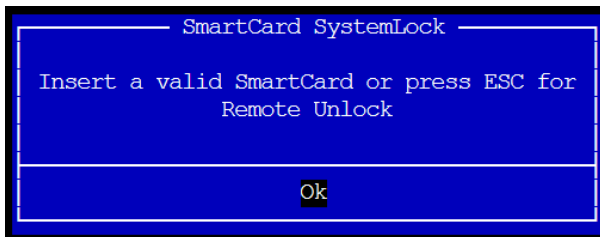
## Unlock SystemLock PC



You need the password which was issued on creation of an organisation (see section "Create organisations", page 37).

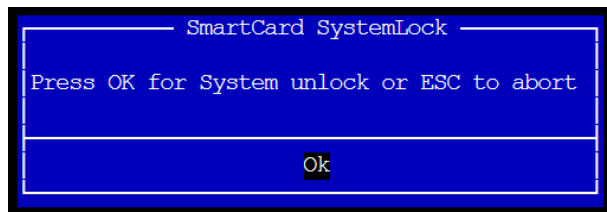
- Start the locked computer without inserting a SmartCard.

The following BIOS dialog is displayed:



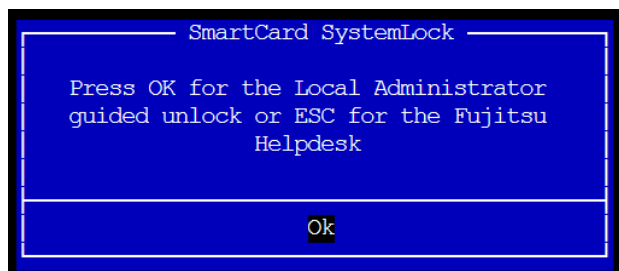
- ▶ You (or the user) should press the *ESC* key.

The following window appears:

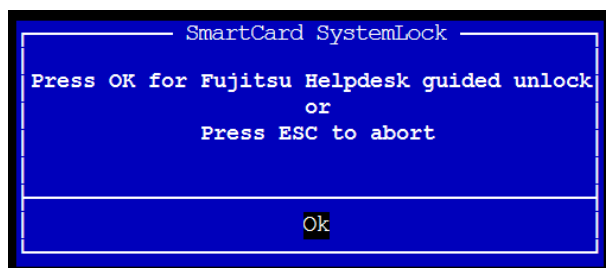


- ▶ Click on *ESC* to unlock through Fujitsu Service.

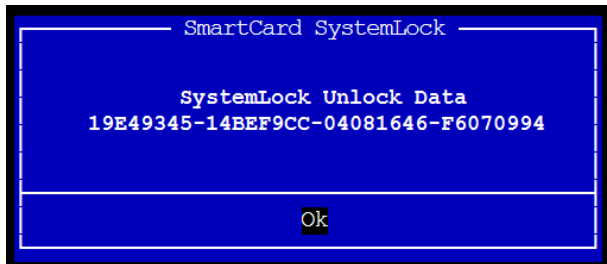
Unlocking by the administrator is not implemented.



- ▶ Click on *OK* in the following window:



The unlock data is displayed, which was generated once for this specific unlocking procedure:



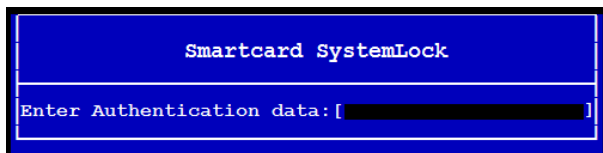
- Contact your Service Centre. Service will guide you through the next steps.



You need the password which you assigned when setting up an organisation (see Password for Service Activation, page 38).

- When you are asked to do so, close the dialogue shown above on the locked computer by clicking *OK*.

An input screen appears:



- Enter the unlocking code which you have received from Fujitsu Service into the BIOS dialog shown above.



*SystemLock* is uninstalled.

The system starts, or opens BIOS if the *F2* key was pressed at the start of the boot process.

The PC is unlocked.

# Job management

All orders which can be sent to the computer in your network are found in *Job management* of the *Workplace Manager*.

Two main groups are distinguished:

- *BIOS-Jobs*: Changes to the BIOS settings of the computers in the network.
- *Licensing jobs*: Licensing of add-on functions, e.g. face recognition.

Jobs can only be executed successfully if the computers have been registered in *Workplace Manager* and you have allocated a *Workplace Manager* client licence to the computers in Licence Management.

A job consists of:

- a number of parameters or settings which you have selected for the particular order.
- a selection of computers which you have combined into groups in group management.

A meaningful name makes it easier to recognise a job in the job history log.

With the command *Start Job*, the order is sent to the computer in the network and executed.

If a computer is not reached because it is switched off or not located in the network, the job is executed as soon as the computer can be reached. The completion of a job can be delayed through this.

The processing status of the job can be checked in the job history log. You recognise the jobs by the names you gave them, see section "Job-History / Delete jobs", page 78.

## Workplace Manager Versions and Job Compatibility

The *Workplace Manager* modules (features) are continuously being further developed.

Therefore, it may not be possible to execute a job with a previous version of *Workplace Manager*. You will receive a notification from the program in this case.

The following table provides an overview of the functions and required feature sets in the different versions:

Function	<i>Workplace Manager</i> 1.10/Feature set	<i>Workplace Manager</i> 1.11/Feature set	<i>Workplace Manager</i> 1.21/Feature set
Easy PC Protection	-	2	2
Login methods	1	2	3
Enabled applications	1	2	2
Presence sensor	1	1	1
Auto BIOS Update	-	2	2
Hard disk password	1	1	1
BIOS password	1	1	1
SystemLock	1	1	1
BIOS user password	-	1	1
Password request during boot	-	1	1

If necessary, update *Workplace Manager* (see chapter Update and repair Workplace Manager, page 12), to be able to use a desired feature.

## Setting up BIOS administration

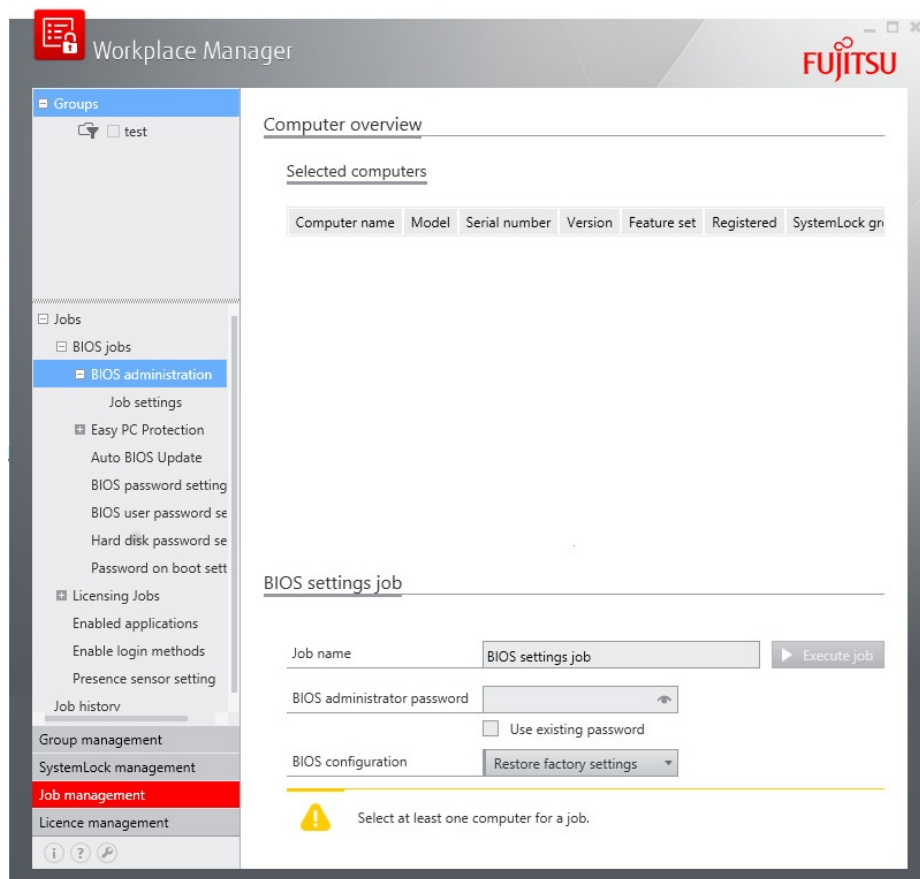
BIOS administration offers you the option of defining the BIOS settings for different groups of computers on the network and setting those computers on the network via a job.

The BIOS configurations can be saved and used again.

You can also extract the settings of an existing computer using this function. You can also record this extraction in *Workplace Protect* as an example configuration file to then distribute these settings to the computer you want on the network.

You can also reset the computers on the network to predefined BIOS settings using BIOS administration.

- In the navigation area, select *Jobs/BIOS jobs/BIOS administration*.



The groups of computers and individual computers are shown in the upper navigation area.

- ▶ Select the desired group or individual computers within the groups.

The selected groups and computers are shown in the working area.

- ▶ Assign a meaningful job name.
- ▶ Enter the BIOS administrator password or use the password saved in the database



### BIOS configuration

A *Factory settings* configuration is available as standard, enabling you to reset the computers to the BIOS standard configuration. This file cannot be deleted or changed.

You can create your own configurations as files (see the section below).

- ▶ Choose the configuration you want to use on your computers from the *BIOS configuration* list.
- ▶ Click on *Execute job* to send the job.

Individual tasks are created for each configuration setting for each computer selected. If no parameters have been set in the configuration list for a BIOS setting, no task will be created.

If errors occur when executing jobs, these are displayed in the job history referring to the tasks.

## Create/change/delete BIOS configuration list

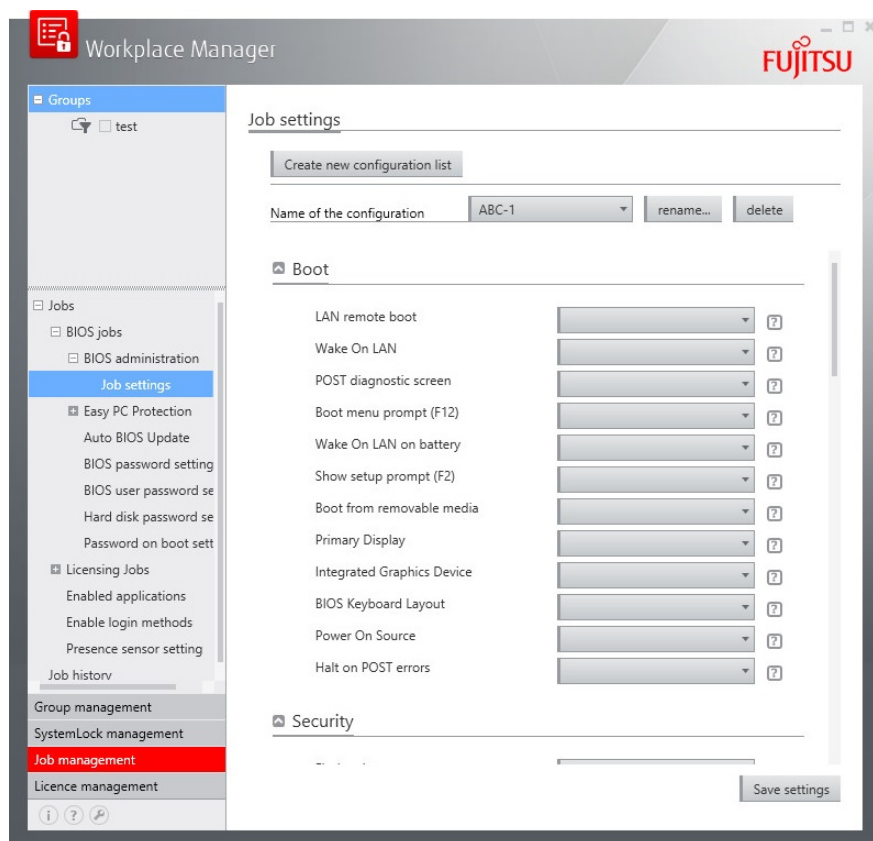
The *Workplace Manager* settings described below offer you all settings on all computer models with the different BIOS versions. Therefore, with regard to a specific computer on the network, settings are also possible which are not available on this model.

Incorrect settings in the configuration result in errors that are displayed in the job history.

It is therefore recommended that you create a suitable configuration for each computer model.

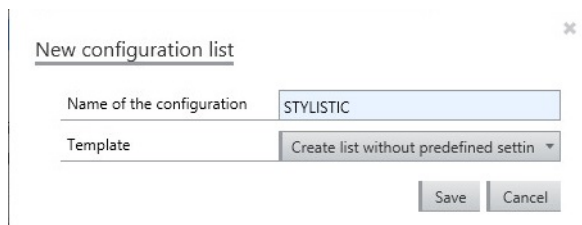
The range of values of a BIOS setting has also been changed at times throughout the computer generations. Therefore make sure that the supported setting is always selected for each computer model.

- In the navigation area, select *Jobs/BIOS jobs/BIOS administration/Job settings*.



### New configuration list

- ▶ To create a new configuration, click on *Create new configuration list*.



- ▶ Enter the name you want to use in the *Name of configuration* field.
- ▶ Choose the configuration you want to use as a basis from the *Template* selection list.
- ▶ Click on *Save* to create the list.

### Change configuration list



Always change the configuration using this function. Changes made directly in the associated file can result in errors.

- ▶ Choose the configuration you want to change from the *Name of configuration* selection list.
- ▶ Choose the BIOS settings you want from the selection lists. Settings you do not choose (=empty selection field) are not changed on the target computers.
- ▶ Save your settings by clicking on the *Save settings* button.

### Rename/delete configuration list

- ▶ You can rename or delete existing configuration lists using the *Rename* or *Delete* buttons.

### Create BIOS configuration list from a (master) computer

You can extract the settings of an existing computer. You can record this extraction in *Workplace Manager* as a configuration file.

You need the DeskView Client product for this, which is currently available on the Fujitsu download sites for free.

- ▶ Open the BIOS (press F2 button when starting the system) on the computer on which you want to create a BIOS extraction.
- ▶ Set the BIOS to match your requirements.
- ▶ Create an archive of the BIOS settings (see DeskView Client user manual, command-line command BIOSSET using /AR parameter).
- ▶ Give the archive a meaningful name.



- Copy the archive to the Workplace Manager Server in the directory:  
%AppData%\Roaming\Fujitsu\WorkplaceManager\BiosSettings\

The next time you call up the *Configuration list*, this archive is made available to you as a predefined configuration file.

## Easy PC Protection

The aim in a network environment is to protect the computers in the company against unauthorized access. Despite the protective measures necessary as a result, the employees should have access to their computers without any great effort on their part.

The computers of different user groups (e.g. night shift, day shift, production, management, etc.) are usually logged into the network at certain times.

*Easy PC Protection* is a function with which the request for a set BIOS password during system boot can be suppressed at specified standard times in a secure company network environment.

The basis for this function is a TFTP server (see section Setting up the TFTP server, page 84), which makes available a time profile file in CSV format and an associated signature file in the company network.

The time profile file contains data records which begin with a profile name. Using these names, the computers in the network can identify those entries which contain the time periods relevant to them.

The times for each weekday are presented after the profile name.

To exclude any falsification of the data, a cryptographic checksum about the file is calculated for every change in the file. This is signed and saved in the attached signature file.

The computer in the network attempts to find the server. If the server cannot be reached, the signature does not match or the signature file is not present, the PC ignores the time profile file and requests the BIOS password as usual.

## Requirements for the use of Easy PC Protection

- TFTP Server



For information on setting up the TFTP server, please refer to this manual, TFTP Server, page 84.

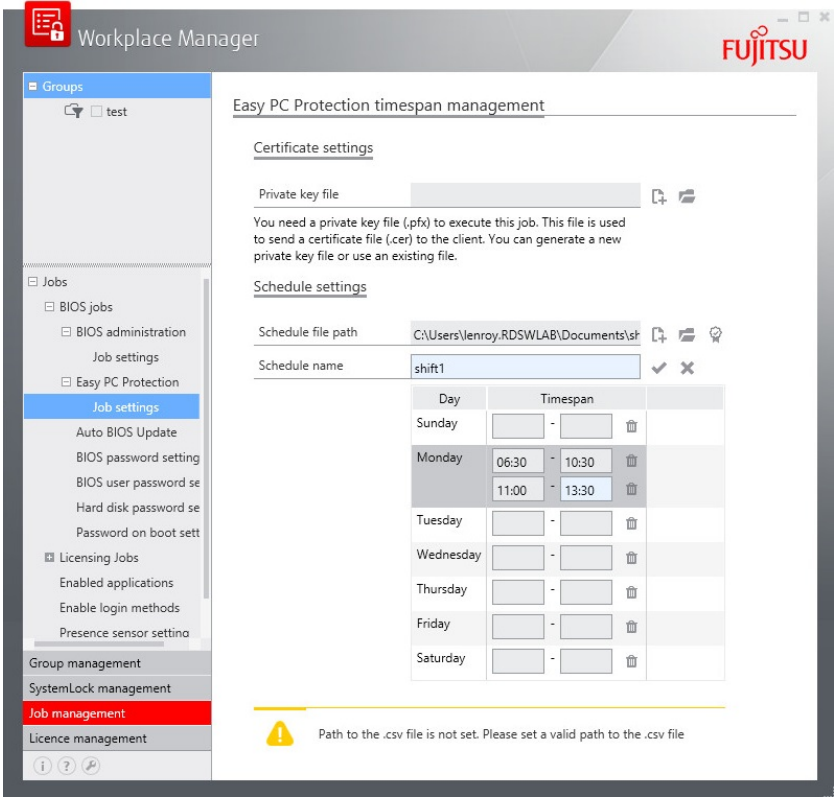
- Network with DHCP support
- *Easy PC Protection* can only be installed on selected systems from Fujitsu.
- *Easy PC Protection* requires appropriate BIOS support by the devices.
- To be able to use the *Easy PC Protection* function, the licence for *Workplace Embedded Tools* (order number S26361-F2542-E437) must be ordered at the same time that the system is ordered.

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

- If computers in the network are protected by *SystemLock*, *Easy PC Protection* cannot be used.

# Implementation of the Easy PC Protection function

► In the navigation area, select *Jobs / BIOS Jobs / Easy PC Protection / Job settings*.



## Symbol overview

Symbol	Function
+	Inserting a new schedule
	Opens a dialogue window below
	Opens an explorer window for selecting a file
	Signs the schedule file
	Switches to edit mode to edit the schedule file
	Deletes the selected schedule



All settings and changes, both during *Certificate settings* and also during *Schedule settings* must always be concluded with the *Sign* button.


To exclude any falsification of the data, a cryptographic checksum about a file is calculated for every change in the file. This is signed and saved in the attached signature file.

The networked computer checks this signature. If the signature is not found or the signature does not match, the computer ignores the time profile file and requests the BIOS password as usual.

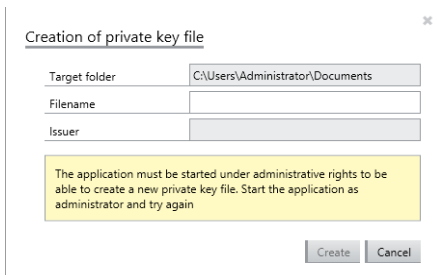
## Certificate settings

A private key file is required for the job execution. This file is used to create a file from it with the matching public key. In the job, this is then sent to the computers in the network.

### Create new private key file

► To create a new private key file, click on the  symbol in the Certificate settings area.

The following window opens:




All the entries are required.

- Configure the target folder using Explorer.
- Enter the file name of the private key file to be created.
- Enter the name of the issuer.
- Assign a password.

Once you have made all the necessary entries, the *Create* button becomes enabled.

- Click on the *Create* button.

A private key file with the file extension *.pfx* and with the name specified is created in the path specified.

Open existing private key file

- ▶ To open an existing private key file, click on the *Open* button.
- You can set the file you require in the Explorer window which then opens.
- ▶ Configure the path.
- ▶ Enter the associated password.
- ▶ Click on the *OK* button which has now become enabled.

The private key file is opened.

Schedule settings

The computers of different user groups (e.g. night shift, day shift, production, management, etc.) are usually logged into the network at certain times.

During these standard times, the users should be able to log into the network without the BIOS password.

In order to determine the times for the computers of different user groups in your network, you need a file called a schedule file.

i




TIP

Mount the TFTP server as a network drive in your system and select the root directory of the TFTP server as the path for the schedule file.

Schedule settings



Schedule file path









C:\Users\lenroy.RDSWLAB\Documents\sh




Schedule name


shift1




Day	Timespan		
Sunday		-	
Monday	06:30	- 10:30	
	11:00	- 13:30	
Tuesday	06:30	- 10:30	
Wednesday		-	
Thursday		-	
Friday		-	
Saturday		-	

- ▶ To create a new schedule file, click on the  symbol in the Schedule settings working area.
- ▶ In the subsequent dialog window, enter the path and the file name of the file to be created.
- ▶ Click on the *OK* button which is now enabled.


A schedule file with the file extension .csv and with the name specified is created in the path specified.

- ▶ To open an existing schedule file, click on the  symbol.
- ▶ Select the required file in Explorer.



The file with the file extension .csv with the corresponding path is shown in the Schedule file field.

- ▶ Use the  symbol to create a new schedule. The name of the schedule is shown in the *Schedule* name field.

Or

- ▶ Change an existing schedule with the  symbol. The name of the schedule is shown in the Schedule name field.

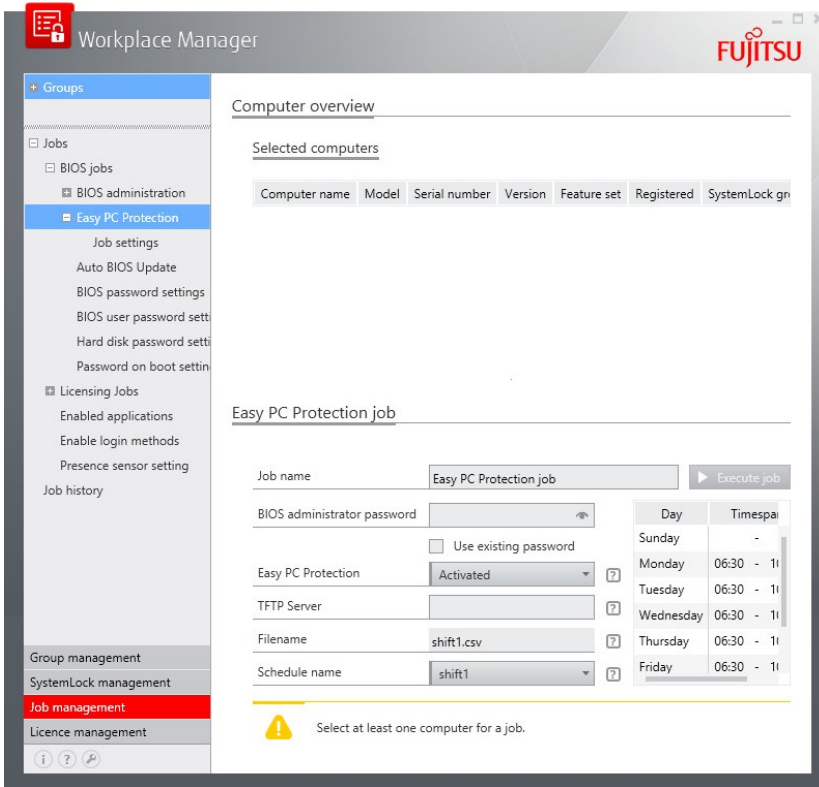
Or

- ▶ Delete an existing schedule with the  symbol.
- ▶ In the days table, enter the times during which the selected computers are normally accessible.
- ▶ Click on the  symbol to sign the changes in the schedule file.

## Execute job

- ▶ Before you create the job, make sure that the schedule file (csv) and the associated signature file (sig) are stored in the root directory of the TFTP server. The signature file \*.sig must have the same name as the schedule file (\*.csv).
- ▶ In the navigation area, select Jobs / BIOS Jobs / Easy PC Protection.

A new working area opens, in which you create the job.



The groups of computers and individual computers are shown in the upper navigation area.

- ▶ Select the desired group or individual computers within the group.

The selected groups and computers are shown in the working area.

- ▶ Assign a meaningful job name.
- ▶ In the Easy PC Protection selection list, choose whether the function should be activated or deactivated.
- ▶ Enter the address of the server in the TFTP Server input field.
- ▶ The previously chosen file name of the schedule file in the root directory of the TFTP server is displayed in the File name field.
- ▶ In the Schedule name selection list, choose the schedule that you have created in Jobs BIOS Jobs / Easy PC Protection / Job settings / Schedule.

An overview of the selected schedules is superimposed.

- ▶ Click on the Execute job button to dispatch the job.

## Change schedule settings

If the computers in the network are set up for the TFTP server, signature file and schedule file, you can change the times within a schedule at any time on the TFTP server.

Requirement: You must use the same certificate for saving the file. If the server address, file name, schedule or certificate change, the job must be executed again with the changed parameters.



A change to the schedule file must not be made directly with an editor, because otherwise the signature file (sig) will not be matched.

## Change log in methods

The login methods secure access to the computers in the network. You can increase this security by combining several login methods with each other.

With this multi-factor authentication, you can protect the computers in the network significantly more effectively against unauthorised access. The more factors are used for authentication at the computer, the greater the security regarding the genuine identity of a user.

For multi-factor authentication, the following factors can be combined:

- Something that the user knows – Password or PIN (secret)
- Something that the user possesses – SmartCard
- Something that the user is – Biometrics, e.g. a fingerprint



Please note that incorrect settings for "Log in" can lock out the user from the system.

This means that, if you configure only devices which are not present on the PC (e.g. fingerprint), the user has no way in which they can use their system.



If you wish to change a previously permitted login method for a user, notify the relevant user in good time. The change will cause the biometric data to be deleted.

Ensure that the user can adapt to the change. For example, allow Windows login as a login method for a short time.



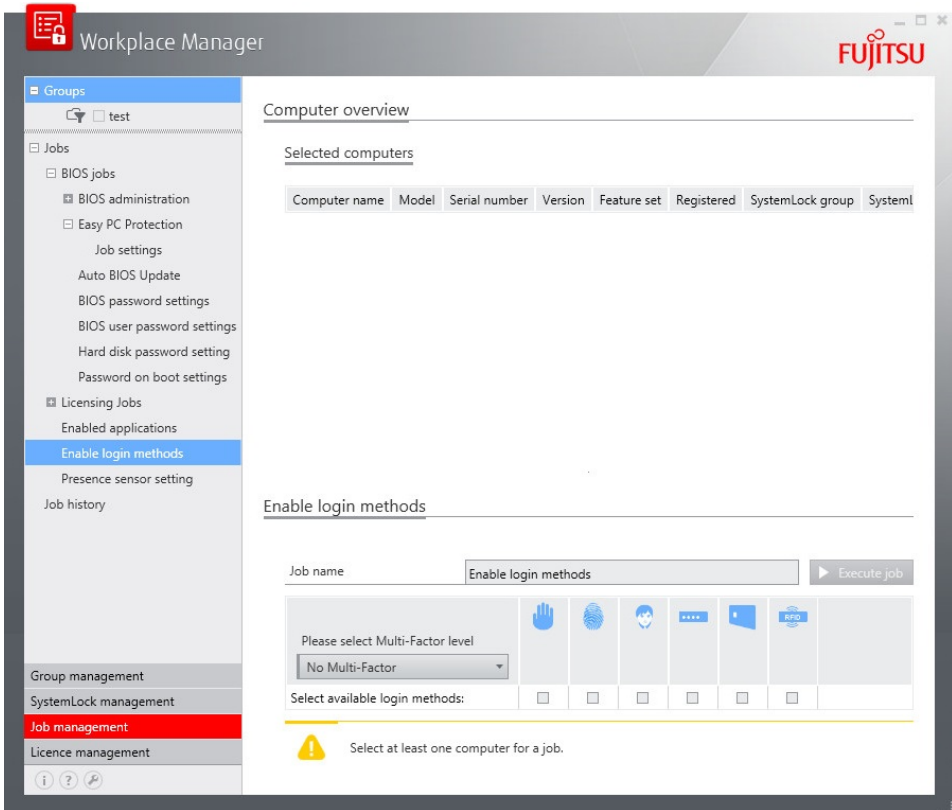
Information about face recognition: An *Advanced Face Recognition* licence must be installed on the computer before the face recognition can be used as a registration method.

Apart from that, ensure that the user has already recorded his or her face in *Workplace Protect*, since no recording of the face can be carried out in "Log In", in contrast to fingerprint and palm recognition.

- ▶ Select *Allow jobs/registration methods* in the navigation area.
- ▶ In the following window, select the security level you wish to assign to the user.

Symbol / Security level	Function
? / Single factor	Login with password, SmartCard, etc.
? / Multi-factor (Template on Card)	Login with biometric data, which is saved on the SmartCard
? / Multi-factor (Secret)	Login with biometric data and a password, which must be entered by the user

Depending on the selected security level, the individual login methods or additionally possible login options will be displayed.



The groups of computers and individual computers are displayed in the upper navigation area.

- Select the desired group or individual computers within the groups.

**i** Of those computers that you wish to assign, select only the ones that are equipped with the "Log in" function.

The selected groups and computers are displayed in the working area.

- Assign a meaningful job name.



- ▶ Mark one or several login methods or the additional log-in options, which are applicable to the selected computers:

Methods	Login
Palm recognition	Login using the palm sensor
Fingerprint	Login by fingerprint
Facial recognition	Login by matching the face of the user with a photo of the face taken previously in <i>Workplace Protect</i> (Licence required)
Password	Login with password
SmartCard	Login with SmartCard and PIN
RFID	Login with RFID

- ▶ Define where the biometric data should be saved (on the computer or on a SmartCard).



The face recognition data cannot be saved on the SmartCard.

- ▶ Click on the *Execute job* button to dispatch the job.



The settings must be performed again when reinstalling a computer.

## Set up allowed applications

You can use this job to enable additional security applications for the user.



Before activating the application, check the operating system on the computer for which the job has been created, is compatible with the application.



If the users were already working with Password Safe before version 1.21, the existing database must be updated. To do this, users will required Internet access.

If Internet access is not possible, provide the users with the following files.

Link to converter:

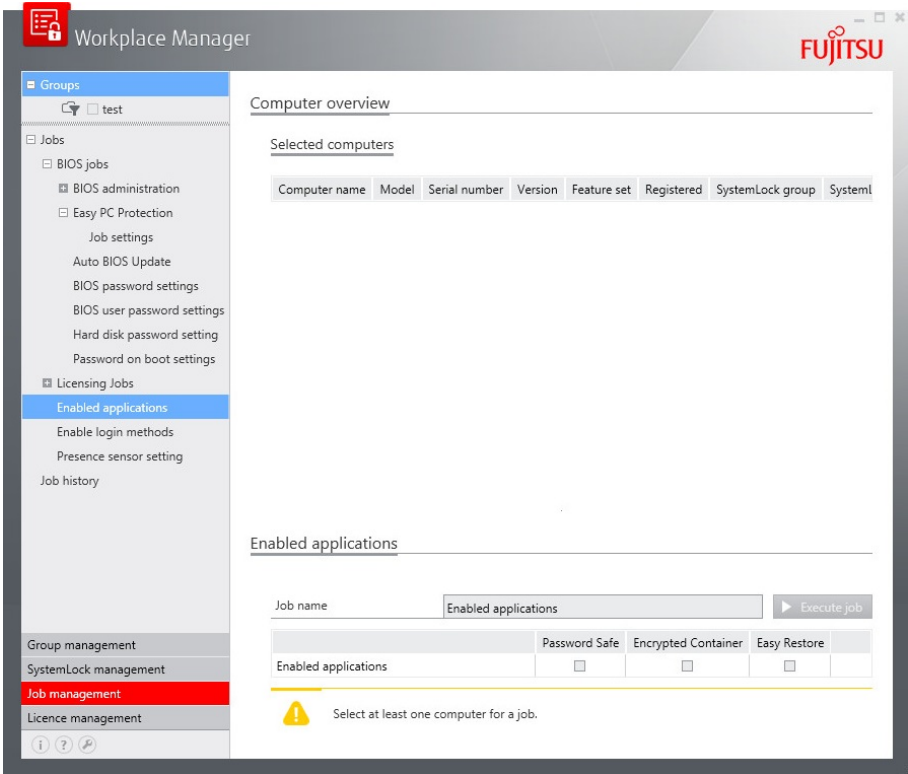
<http://support.ts.fujitsu.com/download/Permalink.asp?ID=3F72249D-1527-4677-9FC1-E2DA44473294>

Link to licence:

<http://support.ts.fujitsu.com/download/Permalink.asp?ID=7BBDF9AB-1EB1-4845-B997-3AEAECB411D>

Ensure that the users can save the required files on their computers in the %programdata%\fujitsu\KPConverter directory.

Select *Jobs/allowed applications* in the navigation area.



The groups of computers and individual computers are displayed in the upper navigation area.

- ▶ Select the desired group or individual computers within the groups.

The selected groups and computers are displayed in the working area.

- ▶ Assign a meaningful job name.
- ▶ Mark the application which you want to enable for the selected computers in Workplace Protect:

Application	Description
<i>Password Safe</i>	Safe for saving passwords
<i>Encrypted Container</i>	Encrypted data area on the hard disk
<i>Easy Restore</i>	Allow restore to delivery status or backup of networked computers. If this function is to be enabled, as administrator you must make a TFTP server available. (see manual: Workplace Protect)

- ▶ Click on the *Execute job* button to dispatch the job.



After the installation of *Workplace Protect* (managed mode), the applications are enabled, so that the end users could already have these in use when you lock the applications. In this case, you should inform your end users in advance about switching off the applications.

## Define presence sensor settings



This function requires a presence sensor on the computers. This can for instance be ordered as an order option together with the computer models ESPRIMO X913 or ESPRIMO X923.

With the presence sensor settings, you determine which actions may be performed if the user is sitting in front of the screen, or is absent.

Select *Jobs/Presence sensor setting* in the navigation area.

The screenshot shows the Workplace Manager application window. The left sidebar contains a navigation menu with the following items: FTS, LS-S935FP, Jobs, BIOS jobs, BIOS administration, Easy PC Protection, Job settings, Auto BIOS Update, BIOS password settings, BIOS user password settings, Hard disk password setting, Password on boot settings, Licensing Jobs, Enabled applications, Enable login methods, **Presence sensor setting** (highlighted), and Job history. Below this are sections for Group management, SystemLock management, Job management (highlighted in red), and Licence management. The main content area is titled 'Computer overview' and shows a table of 'Selected computers' with columns: Computer name, Model, Serial number, Version, Feature set, Registered, SystemLock group, and System status. The table contains one entry: LS-S935FP, with Version 1.10, Feature set 1, Registered No, and System status not in use. Below the table is the 'Presence sensor setting' section. It includes a 'Job name' field with the value 'Anwesenheitssensor Einstellungsjob' and an 'Execute job' button. There is a checkbox for 'Activate presence detection'. Under 'User is absent', there are three action configurations: Action 1, Action 2, and Action 3, each with a dropdown menu and an 'Action after' field (60, 0, and 0 seconds respectively). Under 'User Presence', there are two checkboxes: 'Turn the display on' and 'Resume the computer from sleep or hiber'.

The groups of computers and individual computers are displayed in the upper navigation area.

► Select the desired group or individual computers within the groups.

The selected groups and computers are displayed in the working area.

- ▶ Assign a meaningful job name.
- ▶ Mark the option *Activate presence detection*.

The *Presence sensor* function is activated or deactivated with this.

- ▶ Select an action which should be performed after a defined period of time if the user remains absent:

Action during absence
<i>Lock computer</i>
<i>Turn off display</i>
<i>Turn off display and lock computer</i>
<i>Energy saving</i>
<i>Hibernate</i>



Not all actions may be selectable, depending on what has already been selected.

The time set for a subsequent action must be greater than that of the previous action.

- ▶ Select an action which should be performed in the presence of the user:

Action when present
<i>Activate monitor</i>
<i>Transfer the computer from sleep or hibernate mode into normal mode</i>

- ▶ Click on the *Execute job* button to dispatch the job.

## Auto BIOS Update

You can use *Auto BIOS Update* to allow the BIOS on a group of computers to be automatically updated.

You have two options thereby:

You update to the latest BIOS directly from the official Fujitsu Download Server. (Licence not needed – Internet access needed).

Or

You place the BIOS on a TFTP server in your company. With this you can decide which BIOS version will be installed on the computers. (It is necessary to buy a licence when buying the system - Internet access is not needed)

### Requirements for the BIOS update from a company in-house server

- TFTP server (for setting up the server, please refer to this manual, TFTP Server, page 84)
- Network with DHCP support.

During the boot process, the system uses the DHCP protocol to obtain a free IP address for itself, and to receive information about the network infrastructure.

- The conditions of use must be accepted

*Auto BIOS Update* can only be installed on selected systems from Fujitsu.

To be able to use *Auto BIOS Update* in your company network, the licence for *Workplace Embedded Tools* must be ordered at the same time as the system is ordered (order number S26361-F2542-E437). *Auto BIOS Update* via the Fujitsu server is not possible without a licence.

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

## Make BIOS updates available

For each system family supported by Fujitsu and that should be supplied with BIOS updates automatically, certain files must be present. To receive the necessary files for the system being used by you, download the *Admin package* from the Fujitsu Support web site:

<http://support.ts.fujitsu.com>.

- From there, select *Drivers & Downloads*.
- Enter the serial number or identification number of the product, or select the product from the list (e.g. → ESPRIMO P → ESPRIMO P520 desktops).

Selected operating system: **OS Independent (BIOS, Firmware, etc.)** Change selected operating system >>

If your driver is not shown below, then the driver may already be part of the operating system.  
If you need more help please contact your [local Service Desk](#).

☐ Show all files

☒ Flash - BIOS

☒ BIOS Update - Admin Pack for D3220-A1x

Title	Version/Date	Size	Status	Language	PDF	Save	FileDownload
D3220-A1x - Admin package - Compressed Flash Files <a href="#">Other versions</a>	V4.6.5.4 - R1.14.0 05.02.2014	31,96 MB	✓	🌐			Download >>

☒ BIOS Update - Windows for D3220-A1x

☒ Systemboard

☒ Documentation

- As operating system, select *OS Independent (BIOS, Firmware, etc.)*.
- Download the *BIOS Update - Admin Pack*.
- If you wish to download an older version of a BIOS Update, click on *Other versions*.

The downloaded .zip file contains a directory called TFTP, which contains the files necessary for the server.

In the following example, for the BIOS Update to version 1.14.0 of the ESPRIMO P520 system, these files are included:

- D3220-A1-1-14-0.csv (control file for all BIOS versions for the ESPRIMO P520)
  - D3220-A1-1-14-0.UPC (compressed BIOS Update to version 1.14.0)
- For your present system, create an empty master file in the root directory of the TFTP server, named as follows: <Mainboardname>.csv. (e.g. D3220-A1.csv). Copy the contents of the file contained in the ZIP file (D3220-A1-1-14-0-14-0.csv in the example) into the master file. If you wish to make several BIOS versions available, transfer their contents line-by-line into the master file.
  - Copy all the associated UPC files into the root directory of the TFTP server. Customisation for several BIOS versions is necessary if a BIOS version of a specific earlier version is needed for an update. Without customisation, the highest available version available on the server is always installed automatically on the computers.
  - Repeat the steps described to add BIOS updates for other system families.



The *Flash Write Support* setting in the BIOS Setup *Security* menu must be enabled for the BIOS update to be successful. (For DeskView Client users: BIOSSET /FW ...)

## Allocate BIOS updates to computers



For each system family for which BIOS updates are distributed, a CSV control file must exist in the TFTP root directory, containing the information on the available BIOS updates for the system family.

If you wish to provide several versions of firmware for a system family (e.g. 1.5.0, 1.10.0 and 1.14.0) customization of the CSV file is required for this system family.

The control file is constructed as follows:

The first line contains the header record with the following "column names":

```
version,needed_version,filename,changelog
```

Each further line contains information about the particular firmware update.

In the example (BIOS version 1.14.0 for the ESPRIMO P520) the second line contains:

```
1.14.0,,D3220-A1-1-14-0.UPC,,
```

Another line must be inserted in the CSV file for each further BIOS version which is allocated.

You can copy the lines required from the particular CSV files of the corresponding "Admin packs".

The file for the example ESPRIMO P520 system can for instance look like this:

```
version,needed_version,filename,changelog,
```

```
1.5.0,,D3220-A1-1-5-0.UPC,,
```

```
1.10.0,,D3220-A1-1-10-0.UPC,,
```

```
1.14.0,,D3220-A1-1-14-0.UPC,,
```

## Show the user BIOS update messages

Immediately before an update, you can report text to the user by storing a `Change log` file.

The following conventions must be adhered to for an error-free description:

- Maximum of 43 characters per line
- Maximum of 14 lines
- ASCII character set (no special characters, umlauts, etc.)

Save the text file in the TFTP root directory of the server, giving it a meaningful file name (e.g. `D3220-A1-1-14-0-changes.txt`).

Insert the file name in the corresponding column for this firmware version in the csv file.

```
version,needed_version,filename,changelog
```

```
1.14.0,,D3220-A1-1-14-0.UPC,D3220-A1-1-14-0-changes.txt,
```

## Setup Auto BIOS Update

- Select Jobs / BIOS Jobs / Auto BIOS Update in the navigation area.

The screenshot shows the Workplace Manager interface. On the left is a navigation pane with a tree view containing 'Jobs', 'BIOS jobs', 'Easy PC Protection', 'Job settings', 'Auto BIOS Update' (highlighted), 'BIOS password settings', 'BIOS user password settings', 'Hard disk password setting', 'Password on boot settings', 'Licensing Jobs', 'Enabled applications', 'Enable login methods', 'Presence sensor setting', 'Job history', 'Group management', 'SystemLock management', 'Job management' (highlighted in red), and 'Licence management'. The main area is titled 'Computer overview' and shows a table of 'Selected computers' with columns: Computer name, Model, Serial number, Version, Feature set, Registered, SystemLock group, and System status. One computer, 'LS-S935FP', is listed. Below this is the 'Auto BIOS Update configuration' section with fields for 'Job name' (Auto BIOS Update configuration), 'BIOS administrator password', 'Automatic update' (monthly), 'Custom update' (never), 'Update server' (Fujitsu server), and 'Server address' (webdownloads.ts.fujitsu.com). There are checkboxes for 'Use existing password', 'Silent update', and 'Terms of Use Accepted'. An 'Execute job' button is on the right. At the bottom, a yellow warning icon and text state: 'Accept the terms of use to execute this job'.

The groups of computers and individual computers are displayed in the upper navigation area.

- Select the desired group or individual computers within the groups.

The selected groups and computers are displayed in the working area.

- Assign a meaningful job name.
- Enter the BIOS administrator password or use the password saved in the database.
- In the *Automatic Update* selection list, choose the frequency at which the BIOS should be automatically updated (e.g. monthly).
- In the *User-defined Update* selection list, choose whether or not an update should be searched for once, during the next boot of the computer.
- In the *Server for update* selection list, choose the server on which the search for the BIOS update should be performed.

With declaration of your in-company TFTP server, you can specify which of the BIOS versions that you have made available will be installed (licence needed).

- ▶ Enter the address of the server into the *Server Address* field.
- ▶ For an in-company TFTP server, enter the IPv4 address of the TFTP server in the particular network.
- ▶ If the BIOS should be updated without any messages being issued, mark the *Silent Update* option.
- ▶ Read the conditions of use and then mark the option *Accept conditions of use*.
- ▶ Click on the *Execute job* button to dispatch the job.
- ▶ The computer is now set up for Auto BIOS and at the specified times a test will be made for a new BIOS and if so it will be installed.



If you are to uninstall Workplace Protect, the settings for BIOS Update are kept.

If you do not wish to keep the settings, you must send a job which sets the *Never* option in the *Automatic Update* selection list in the BIOS Update configuration and switches off the *User-defined update*.

## Set BIOS password

You use the BIOS password to protect the BIOS from being changed. Only the administrator should have unlimited access to the BIOS.

You can assign different passwords for groups of computers.

This increases the BIOS security on your network.

So that you do not have to memorise all of these passwords, you can store them in encrypted form using the "Save password" option in the *Workplace Manager* database.

You can use saved passwords for all jobs for which the BIOS administrator password is requested. Each saved password is used for each computer.



If you need a password of an individual computer to give it to a support member, you can read it out by clicking on a computer in the *Computer overview* list (see section Computer properties).

The password should be immediately changed after the support operation.

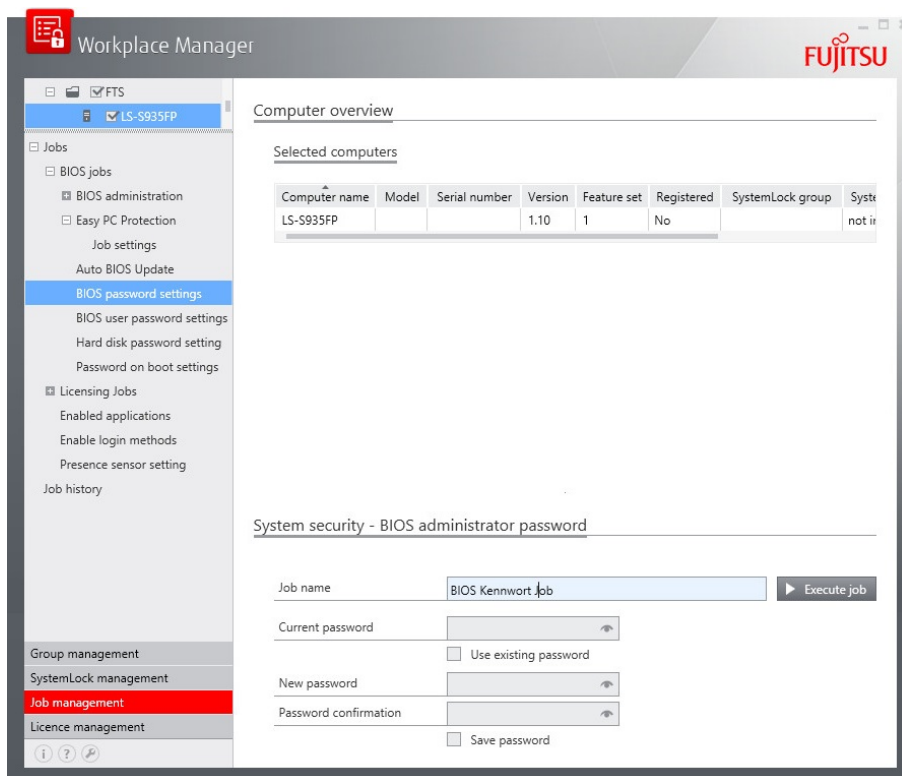


You can set and administer passwords which contain special characters. The use of special characters requires the support of BIOS for the managed systems.

When using special symbols in passwords, please note that the BIOS Setup input masks (e.g. during system boot) are based on the English keyboard layout.

- ▶ Select Jobs / BIOS Jobs / BIOS password settings in the navigation area.





The groups of computers and individual computers are displayed in the upper navigation area.

- Select the desired group or individual computers within the groups.

The selected groups and computers are displayed in the working area.

- Assign a meaningful job name.
- If a password has already been assigned, enter this in the field *current password*.
- Enter the "old" hard disk password in the field *Current Password*, if a password is already assigned.
- Enter the new password in the field *New password* and confirm it in the field *Confirm password*.
- Click on the button *Execute job* on conclusion of the entries.

The password assigned is sent to the computer.

It is checked and is immediately valid.

**i** If for example the *BIOS Administrator password* was incorrectly written, the passwords are not set.

## Set BIOS user password

You severely restrict access to the BIOS Setup with the BIOS user password.

If the users in the network should use their own BIOS user passwords for their computers, you can achieve this using this job.

You send the users a temporary password that you predefine, inform the end users of it and ask them to change the password as soon as possible using *Workplace Protect*. The end users do not need to know your BIOS Administrator password for this purpose.

You can also use this job if one of your end users has forgotten their BIOS user password.



You can set and administer passwords which contain special characters. The use of special characters requires the support of BIOS for the managed systems.

When using special symbols in passwords, please note that the BIOS Setup input masks (e.g. during system boot) are based on the English keyboard layout.

- In the navigation area, select Jobs / BIOS Jobs / BIOS user password settings.

The screenshot shows the Workplace Manager interface. On the left is a navigation pane with a tree structure. The 'Jobs' folder is expanded, showing 'BIOS jobs' which includes 'BIOS administration', 'Easy PC Protection', 'Job settings', 'Auto BIOS Update', 'BIOS password settings', and 'BIOS user password settings' (which is highlighted). Below these are 'Licensing Jobs', 'Enabled applications', 'Enable login methods', 'Presence sensor setting', and 'Job history'. At the bottom of the navigation pane are 'Group management', 'SystemLock management', 'Job management' (highlighted in red), and 'Licence management'. The main area is titled 'Computer overview' and shows a table of 'Selected computers' with columns: Computer name, Model, Serial number, Version, Feature set, Registered, SystemLock group, and System status. One computer, 'LS-S935FP', is listed. Below this is the 'BIOS user password settings job' configuration section. It includes a 'Job name' field with the value 'BIOS user password' and an 'Execute job' button. There are three password fields: 'BIOS administrator password', 'New user password', and 'Password confirmation', each with a toggle for visibility. There are checkboxes for 'Use existing password' and 'Save password'. At the bottom, a yellow warning icon and text state: 'BIOS administrator password must be set'.

**Workplace Manager**

**Computer overview**

Selected computers

Computer name	Model	Serial number	Version	Feature set	Registered	SystemLock group	System status
LS-S935FP			1.10	1	No		not in

**BIOS user password settings job**

Job name: BIOS user password ▶ Execute job

BIOS administrator password 👁

☐ Use existing password

New user password 👁

Password confirmation 👁

☐ Save password

BIOS administrator password must be set

The groups of computers and individual computers are displayed in the upper navigation area.

- ▶ Select the desired group or individual computers within the groups.

The selected groups and computers are displayed in the working area.

- ▶ Assign a meaningful job name.



You can also have displayed the characters which you enter in the password field, by marking the *Character display* option.

- ▶ Enter the required password in the *BIOS administrator password* field.
- ▶ Enter the new user password in the field *New user password* and confirm it in the field *Confirm password*.
- ▶ Click on the button *Execute job* on conclusion of the entries.

The password assigned is sent to the computer.

It is checked and is immediately valid.



If for example the *BIOS Administrator password* was incorrectly written, the passwords are not set.

## Set hard disk password

With the hard disk password, you prevent the hard disk being used in another system without knowledge of the password.



The BIOS administrator password is only required if *SystemLock* is not activated.

You can set and administer passwords which contain special characters. The use of special characters requires the support of BIOS for the managed systems.

When using special symbols in passwords, please note that the BIOS Setup input masks (e.g. during system boot) are based on the English keyboard layout.

- ▶ Select *Jobs / BIOS Jobs / BIOS password setting* in the navigation area.

The screenshot shows the Workplace Manager application window. The left sidebar contains a navigation menu with the following items: **Jobs** (expanded), BIOS jobs, Easy PC Protection, Job settings, Auto BIOS Update, BIOS password settings, BIOS user password settings, **Hard disk password setting** (selected), Password on boot settings, Licensing Jobs, Enabled applications, Enable login methods, Presence sensor setting, Job history, Group management, SystemLock management, **Job management** (highlighted in red), and Licence management. The main area is titled 'Computer overview' and shows a table of 'Selected computers'.

Computer name	Model	Serial number	Version	Feature set	Registered	SystemLock group	System
LS-S935FP			1.10	1	No		not in

Below the table, the 'System security - Hard disk drive (HDD) password' configuration screen is visible. It includes the following fields and controls:

- Job name:** Hard disk password
- Execute job:** Button
- BIOS administrator password:** Field with a help icon (?)
- ☐ Use existing password
- Current password:** Field with an eye icon
- New password:** Field with an eye icon
- Password confirmation:** Field with an eye icon
- ☐ Save password

The groups of computers and individual computers are displayed in the upper navigation area.

- Select the desired group or individual computers within the groups.

The selected groups and computers are displayed in the working area.

Assign a meaningful job name.

- If no SystemLock is set up, enter the BIOS administrator password or use the password saved in the database.
- If a password has already been assigned, enter this in the field *current password*.
- Enter the new password and confirm this.
- Click on the button *Execute job* on conclusion of the entries.

The password assigned is sent to the computer.

The next time the computer is booted, an attempt is made to write the password onto all hard disks. These hard disks must not have any password assigned, or these hard disks were protected up to now with the same "old" password.

The passwords specified are checked or set during the next boot.



If for example the *BIOS Administrator password* was incorrectly written, the passwords are not set.

## Password on boot settings

*Password on boot settings* specifies whether the user of the selected computer in the network must enter the user password during booting.

- In the navigation area, select Jobs / BIOS Jobs / Request password during boot.

**Workplace Manager**

**Computer overview**

**Selected computers**

Computer name	Model	Serial number	Version	Feature set	Registered	SystemLock group	Sys
LS-S935FP			1.10	1	No		not

**System security - password request**

Job name: Password request during start ▶ Execute job

BIOS administrator password:  🔍

☐ Use existing password

Password request during start: Deactivated ▼

BIOS administrator password must be set

The groups of computers and individual computers are displayed in the upper navigation area.

- Select the desired group or individual computers within the groups.

The selected groups and computers are displayed in the working area.

- Assign a meaningful job name.
- Enter the required password in the *BIOS administrator password* field.

- ▶ In the *User password during start* list, select the option *Activate* or *Deactivate* to switch the password request on or off.
- ▶ Click on the button *Execute job* on conclusion of the entries.

# Advanced Face Recognition

## Licences

Without special licences for face recognition, computers in the network cannot use *Advanced Face Recognition*. It is therefore necessary that you purchase licences, activate them and allocate them to computers in the network.

Licence management (the *Licence management* option in the navigation area) is used to administrate the purchased licence key and the allocation of licences to computers in the network.

## Purchase licences

- ▶ Select Job management / Licensing jobs / Licensing facial recognition licence input.
- ▶ Open the link *Click here to go to the online shop* and follow the instructions on the screen.



The name and email address which you must provide at purchase are requested during activation of the licence.

If you have purchased a licence, you will receive an email with an activation code, sent to the email address given.

Save the email in a secure place.

## Enter licences

You must activate the licences acquired in the working area *Advanced Face Recognition key registration*.

Enter the licence or read it from the file with the function *Read from file*.

- ▶ Identify yourself with the name and email address which you gave during purchase.

Enter the activation code which you have received by email.



Licences once assigned cannot be assigned again.

## Advanced Face Recognition licensing



Ensure that the computers to which you are sending a job have an Internet connection.

In the navigation area, select *Job management / Licensing Jobs / Face Recognition licensing*.

The screenshot shows the 'Workplace Manager' application window. The left sidebar contains a navigation menu with the following items: Groups, Jobs, BIOS jobs (with sub-items: BIOS administration, Easy PC Protection, Auto BIOS Update, BIOS password settings, BIOS user password settings, Hard disk password setting, Password on boot settings), Licensing Jobs (with sub-items: Face Recognition licensing, Enabled applications, Enable login methods, Presence sensor setting, Job history), Group management, SystemLock management, Job management (highlighted in red), and Licence management. The main area is titled 'Computer overview' and shows a table of 'Selected computers' with columns: Computer name, Model, Serial number, Version, Feature set, Registered, SystemLock group, and SystemLock status. The table contains one row: LS-S935FP, , , 1.10, 1, No, , not installed. Below this, the 'Licensing of Advanced Face Recognition functions' section is visible, featuring a 'Job name' field with the value 'Advanced Face Recognition licence', an 'Execute job' button, and proxy settings (Address, Port) which are currently empty. A yellow warning box at the bottom states: 'Computers must have an Internet connection for this job.'

The groups of computers and individual computers are displayed in the upper navigation area.

- Select the desired group or individual computers within the groups.

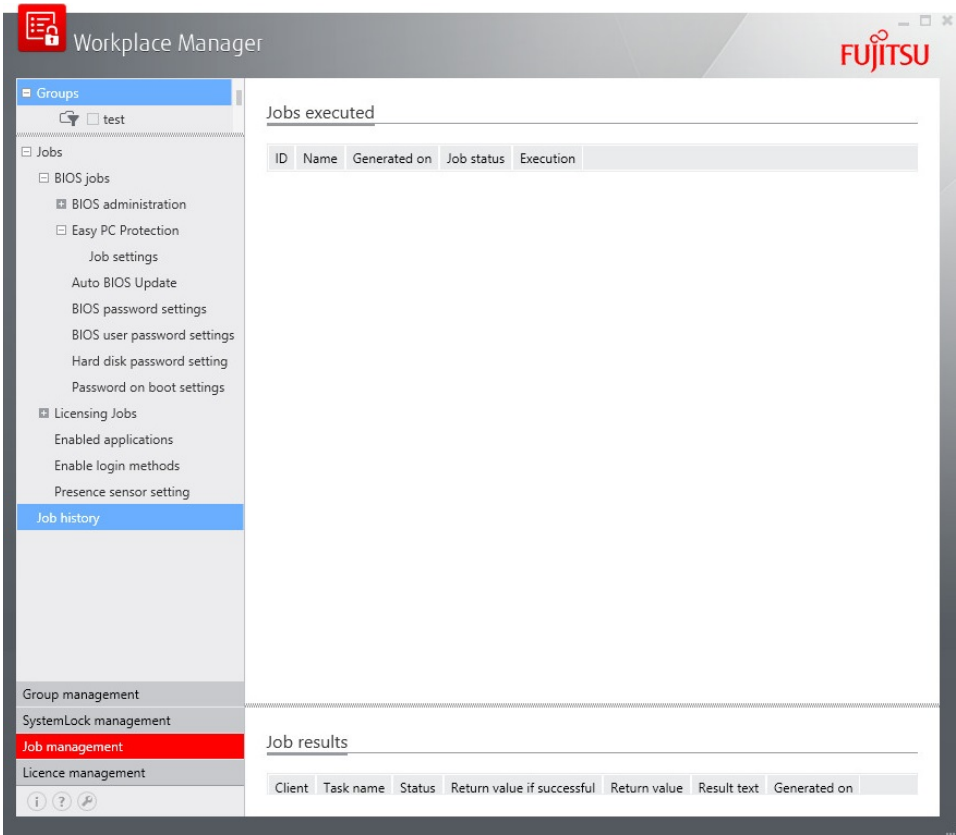
The selected groups and computers are displayed in the working area.

- Assign a meaningful job name.
- If necessary specify the address and port for the server.
- Click on *Execute Job* to send the job.

# Job-History / Delete jobs

You can check whether and how a job was carried out in the job history.

Via the context menu, you can sort according to any column and delete individual jobs or groups of jobs (e.g. delayed jobs).





## Deleting jobs



Please note that you can also delete jobs created by a different administrator. Therefore, please only delete jobs that you yourself have created or which you know can definitely be deleted.

- ▶ Sort the desired column.
- ▶ Select the jobs that you want to delete.
- ▶ In the context menu, select the entry Delete jobs.
- ▶ The selected jobs are deleted.

### Details about the jobs carried out

Job status	Description	Action
<i>Successful</i>	The job was successfully carried out on all computers in the network.	-
<i>Partial success</i>	The job was still not carried out on all computers. Or The job was incorrectly carried out on some computers.	<ul style="list-style-type: none"> <li>▶ Check whether the computers are reachable.</li> <li>Or</li> <li>▶ Check which error is present.</li> </ul>
<i>Failed</i>	Error during execution	<ul style="list-style-type: none"> <li>▶ Check which error is present.</li> </ul>
<i>Not known</i>	The job was just started and there is no feedback.	<ul style="list-style-type: none"> <li>▶ Check the status again at a later time.</li> </ul>

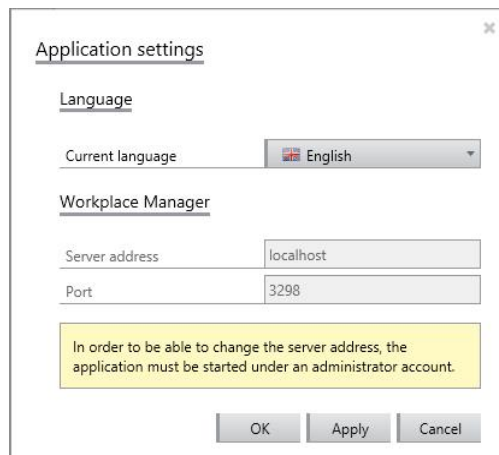
Execution	Description	Action
<i>Delayed</i>	The execution is delayed, for instance because a computer cannot be reached.	<ul style="list-style-type: none"> <li>▶ If necessary cancel the execution by calling up the context menu with the right mouse key (<i>Cancel job</i>).</li> </ul>
<i>Immediately</i>	The job was carried out and ended.	-

### Information about the job results

Status	Description	Action
<i>Not known</i>	Job is currently initialised.	-
<i>Sent</i>	The job was sent to the computers in the network.	-
<i>Completed</i>	The computer in the network has returned a result.	► If the <i>return value</i> expected on completion does not match the actual <i>return value</i> , check what error has occurred.
<i>Failed to send to computer</i>	The computer could not be reached (e.g. firewall blocking communication, computer switched off).	► Check why the computer is not reachable.
<i>Unlicensed</i>	Computer cannot be managed, since it is not licensed.	► Licence your computer.
<i>Not registered</i>	Computer cannot be managed, since it is not registered.	Import the computer again or test the cause with the option <i>Group management / Registration problems</i>
<i>Unsupported</i>	The job cannot be executed in the current configuration (e.g. when an uninstall job is still pending and an install job was just sent).	► If necessary cancel the execution by calling up the context menu with the right mouse key ( <i>Cancel job</i> ).

# Workplace Manager Settings

## Set language and port



Application settings

Language

Current language: English

Workplace Manager

Server address: localhost

Port: 3298

In order to be able to change the server address, the application must be started under an administrator account.

OK Apply Cancel

- ▶ Click on the *Spanner* symbol in the navigation area.
- ▶ Select the desired language.

**i** You should not change the settings under *Workplace Manager* for the server address and port. They describe the address of the server if the administrator console is not installed on the server (not supported in the current version).

- ▶ Confirm your entries with *OK*.

# 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* or *Auto BIOS Update* can be used in your company network.

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.

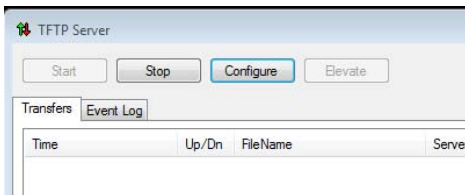
## Setting up the TFTP server

 You require administrative rights for the installation.

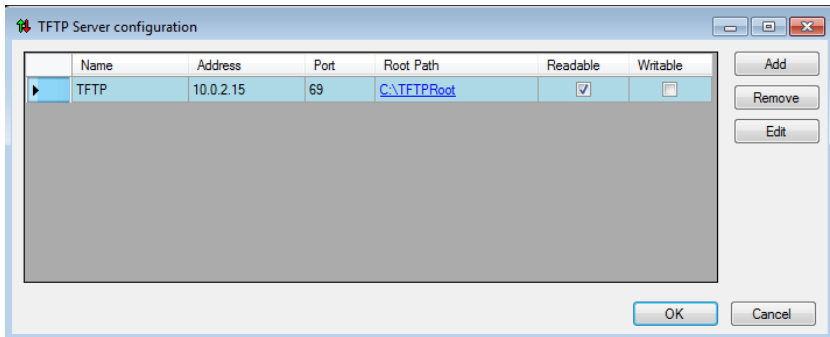
The TFTP server must be set up so that it responds on port 69 to incoming requests.

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.

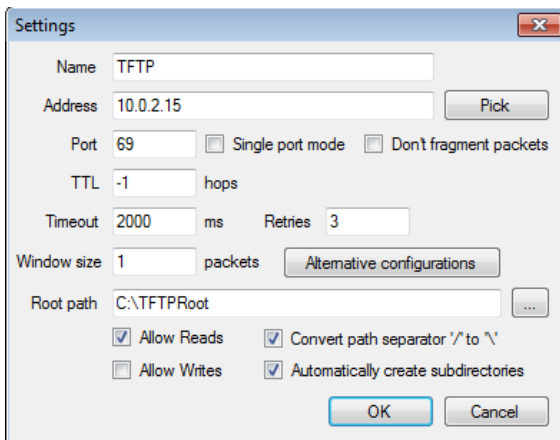


A configuration screen opens, in which you can add a new TFTP server.



- Click on *Add*.

The Settings window opens.



**i**

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

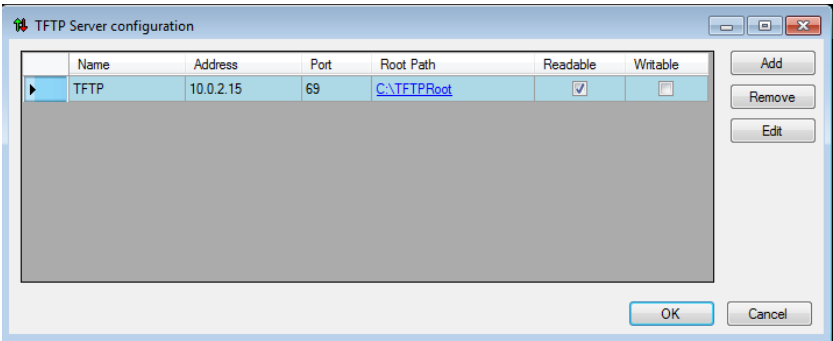
- Click on *Pick* to select the desired network interface and the matching IP address.

**i**

Please be careful to select an IPv4 address.

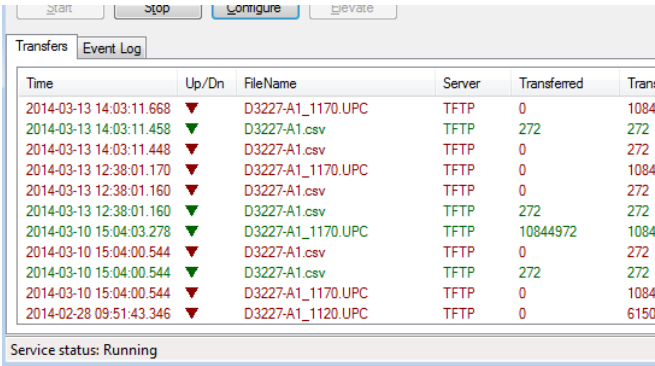
- Enter the root directory of the TFTP server in *Root path*.  
All the files situated in the root directory can be reached using TFTP.
- Confirm your input with *OK*.

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.



# Glossary

## A

### Active Directory

Active directory is a directory service of *Microsoft Windows Server*, with which a network in a company can be structured. It manages the various objects in a network, e.g. computers, servers or users.

### Admin SmartCard

Card type of *SystemLock*.

- Allows the system to be started,
- changes in BIOS Setup, PIN changes,
- deinstallation of *SystemLock*,
- initialisation of Smartcards,
- unlocking Smartcards

### Advanced Face Recognition

Function of the Software *Workplace Protect*

### Auto BIOS Update

This function can be used to update the BIOS of computers automatically via the Fujitsu Download Server or a company in-house TFTP server.

## C

### Clients

The computers in the network which are managed by *Workplace Manager*.

### Cockpit

Graphical user interface on the server or optionally on a *Windows 10* computer, with which the administrator can manage the computers in *Workplace Manager*.

## E

### Easy PC Protection

Easy PC Protection is a function with which the request for a set BIOS password during system boot can be suppressed at specified standard times in a secure company network environment.

### Easy Restore

The hard disk of a computer is automatically and regularly backed up under Windows. In an emergency, a restore of the data and system images can be started via the BIOS at the press of a button.

### **Encrypted Container**

Encrypted data area on the hard disk

## F

### **Featureset**

Level of a software module (function) in a *Workplace Manager* version

## G

### **Groups**

Number of computers with a name, which the administrator has created for the job management.

see also System groups / *SystemLock* Groups

## J

### **Job**

At least one task is carried out on a group of computers.

## M

### **Manager SmartCard**

Card type of *SystemLock*

### **Master admin SmartCard**

Card type of *SystemLock*

### **Multi-factor authentication**

A combination of several logon methods. The more factors that are used for authentication at the computer, the greater the security concerning the real identity of a user.

## O

### **Organisation admin SmartCard**

Card type of *SystemLock*

### **Organisation service SmartCard**

Card type of *SystemLock*

## P

### **Password Safe**

Safe for saving passwords



**PIN**

Personal Identification Number

**PUK**

Personal Unblock Key

**R****RFID**

Radio Frequency Identification - identification takes place via electromagnetic waves.

**S****Service SmartCard**

Card type of *SystemLock*. Allows changes in BIOS Setup.

**SmartCard**

A SmartCard is used to save security-related data. Basically, it consists of memory which records data and an upstream micro-controller which monitors access to this data. Access to the security-relevant data is protected by a PIN (Personal Identification Number). A locked SmartCard can be unlocked again using the PUK (Personal Unlock Key).

**Superuser SmartCard**

Card type of *SystemLock*. Allows system boot, change to BIOS Setup and change PIN.

**System groups**

Groups which are already defined in the *Workplace Manager* (registered computers, licensed computers and unlicensed computers).

**SystemLock Administrator**

Has the following rights within a *SystemLock* group: Boot the system, change the BIOS Setup, change PIN, uninstall *SystemLock*, initialise SmartCards, unblock SmartCards.

**SystemLock User**

Has the following rights within a *SystemLock* group: System boot, change PIN

**SystemLock Database Administrator**

Has the right to change settings or entries in the database in *SystemLock* management.

**SystemLock groups**

Number of computers with a name which the administrator has prepared for the *SystemLock* management.

**SystemLock organisation administrator**

Has administration rights within a *SystemLock* organisation.

### **SystemLock Service**

Has the following rights within a *SystemLock* group: Changes in the BIOS setup.

### **SystemLock Superuser**

Has the following rights within a *SystemLock* group: Boot system, changes in BIOS Setup, change PIN.

## T

### **Task**

Executable command

## U

### **USB - Universal Serial Bus**

USB is a bus system for connecting a computer with peripheral devices, such as a mouse or a printer.

### **User SmartCard**

Card type of *SystemLock*. Allows system boot and change PIN.

## W

### **Workgroup**

Group of computers in a network

### **Workplace Manager Cockpit**

The software *Workplace Manager* is managed in the cockpit.

### **Workplace Manager Database**

The licences, SmartCards, users and computers are managed in the database.

### **Workplace Protect – administrated mode**

Software on the computer in the network.

# Index

## A

- Activate SystemLock
  - Database Administrator SmartCard • 43
- Advanced Face Recognition
  - Licensing • 79, 81
- Applications
  - Easy Restore • 65
- Auto BIOS Update
  - settings • 69

## B

- BIOS password
  - settings • 73, 75, 78

## C

- Computer
  - display details • 25
- Computers
  - allocate licences • 28
  - group • 21
  - import • 20
  - registration problems • 29
- Concept
  - Workplace Manager • 3

## D

- Database server
  - set up • 7

## E

- Easy PC Protection
  - Function • 57

## H

- Hard disk password
  - Setting • 77
- Hardware • 6, 15

## I

- Install
  - Workplace Manager • 6
- Installation
  - Components • 8
  - prepare • 12
  - server • 7
  - WorkplaceManager clients • 15
  - WorkplaceProtect • 15
- Interface • 2
- Internet access • 6, 15

## J

- Job
  - Delete • 82
- Job history • 82

## O

- Operating system • 6, 15

## P

- Presence sensor
  - settings • 67

## R

- Requirement
  - Internet • 6, 15
  - operating system • 6, 15
  - software • 6
- Requirements
  - hardware • 15
  - hardware • 6, 15

## S

- Security applications
  - Encrypted Container • 65
  - Password Safe • 65
- Service Activation
  - Password • 38
- Set up
  - database server • 7
- SmartCard
  - access rights • 42
  - handling • 34
  - reader • 34
- SmartCard • 34
- SmartCard
  - Access concepts • 42
- SmartCard
  - Types • 42
- SmartCard
  - configure • 43
- SmartCard
  - write • 43
- Software • 6
- SystemLock
  - Activation • 36
  - BIOS • 45
  - Change settings • 48
  - Settings • 45
  - uninstall • 48
- SystemLock Management
  - assign computer • 39
  - Groups • 38
  - Organisations • 37
  - users • 41

### T

- TFTP server
  - setting up • 86
- TFTP Server • 86

### U

- Uninstall
  - WorkplaceManager • 14
- Unlock
  - computer • 49
- Update
  - WorkplaceManager • 12

### V

- Version
  - WorkplaceManager • 13, 53

### W

- Windows 10
  - WorkplaceManager • 10
- Workplace Manager
  - Concept • 3
- Workplace Manager • 2
- Workplace Manager
  - User Interface • 18
- Workplace Manager
  - configure • 20
- Workplace Manager
  - Licensing • 26
- WorkplaceManager
  - Uninstall • 14
  - Update • 12
  - Version • 13, 53
  - Windows 10 • 10