

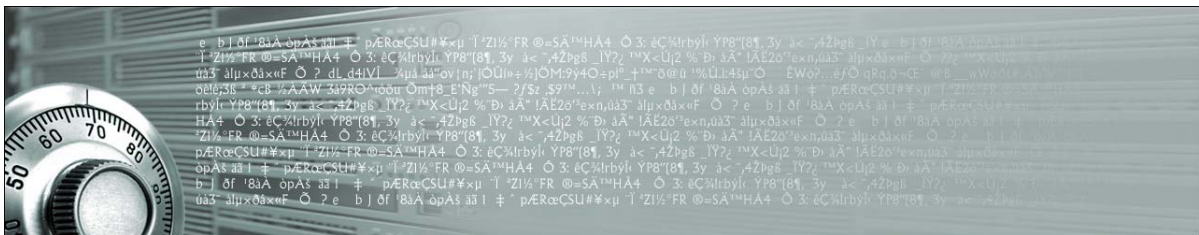
CERTUS ♦ LATEO

Realtime communication encryption layer system

User Manual

Program - Version 4.8.9

Manual Release 091126



Copyright © 2009 by Barclay Technologies (Switzerland) AG. All rights reserved.

Table of Contents

1. Introduction.....	5
Preface	5
What is Certus Lateo?	5
Introduction	5
How it works.....	5
Methods of encryption	6
Performance and security	6
Features.....	6
Components of Certus Lateo.....	7
2. Installation.....	8
Preparation	8
Updater	8
Local installation of Certus Lateo	8
Local installation via CMD console (Command line)	9
Installation of Certus Lateo™ MMC Admin Console.....	9
Installation Certus Lateo™ Admin Panel	9
Network Installation.....	10
Installation of updates	10
3. Certus Lateo™ MMC Admin Console	11
Launching the MMC Admin Console	11
Panels in the MMC Admin Console.....	11
Root	11
Overview.....	11
Actions.....	12
Functions.....	12
Add Group (Create new groups)	12
Refresh Groups (Update list of groups)	12
Refresh Computers (Update list of computers)	12
Show License Information	12
Refresh License Information.....	12
Rename (of a group)	12
Move (Assign a computer to a group).....	12
Delete (Computer)	12
Edit (setting up a group).....	13
4. Certus Lateo™ Admin Panel.....	15
Start.....	15
Configurations.....	15
Protocol	17
List.....	17
Config	17
IP and Port Settings.....	18
5. Annex	19
System Requirements.....	19
Other conditions	19
Annex A: Enduser License Agreement.....	20

1. INTRODUCTION

PREFACE

The theft or leakage of sensitive data from companies or authorities is a frequent subject in the news and can severely damage the image of this organisation or result in economic costs. But attacks by external hackers are only a minor part of the problem, mistakes, neglect or even criminal behaviour of employees are far worse.

That comes as no surprise seen how many people need access to relevant data for their usual work.

Memory media are easily lost and its simple to copy files on a CD, DVD or USB-Stick and hand it over to a third-person.

For companies several kinds of data can play a key role: customer data, project relevant files, strategies or software source code. In many cases this is at the core of a business. Protecting these data from illegal users is one of the greatest challenges businesses face today.

Among the best measures to protect data are encryption and data loss prevention (DLP) systems The downside is that these systems are complicated to use, are time consuming and need a lot of passwords which have to be kept secure too. What's more the encrypted data can't be used immediately and have to be decrypted first. Once decrypted they offer again all options for illegal use.

Surveillance software is helpful to find out who accessed which files, but it does not prevent data theft. It cannot really distinguish between an authorised access and an unauthorised access for making an illegal backup.

But even those who can fully rely on their employees are not absolutely safe from data theft. Even today hackers and other people find a way to infiltrate company networks and get access to confidential data.

The Certus Lateo system is highly secure and efficient but works virtually unnoticed from the user. It prevents unintentional as well as wilful data leaking and man-in-the-middle attacks on data transmissions.

WHAT IS CERTUS LATEO?

INTRODUCTION

Certus Lateo™ efficiently protects sensitive data from companies or organisations from unauthorized access without interrupting your usual workflows.

This is achieved by the complete isolation of a computer, which can only communicate with system having installed Certus Lateo with the same access level.

HOW IT WORKS

A Certus Lateo user works with an environment encoded for his installation, thus enabling only those devices he has prepared and on which Certus Lateo is installed to access the encrypted data.

Certus Lateo™ is used as a driver discreetly in the background of the operating system and encrypts and decrypts all incoming and outgoing data of the whole system.

The user doesn't need to start complicated encryption or decryption procedures with a separate software.

METHODS OF ENCRYPTION

Certus Lateo uses its own, completely new and innovative high-security encryption technology.

Variable and dynamic algorithms generate and apply for every data package an entirely new key with the same size as the data package itself before transmitting the data over a network connection.

It's not necessary to transmit the key, too. The receiver rather gets the necessary information to reproduce the Decryption algorithm for this data-package via dynamically embedded indicators.

By using a one-time key with the same length as the encrypted data an absolutely secure encryption is generated which cannot be mathematically reconstructed.

Another advantage of this method is the marginal use of processor power necessary for encryption as the amount of data to process is very small compared to the encryption of whole files thus allowing for real-time encryption.

PERFORMANCE AND SECURITY

Comparing leading technologies (Twofish, AES, Caesar) and Certus Lateo

	Standard	CL
Key length	128, 192 or 256	1024 and higher
Performance (encrypted symbols per ms) (Standard Workstation)	20'000	80'000
Necessary computer time to crack. (Optimised Workstation)	from a few days	not possible
Algorithms	public	variable
Market launch	from 1998	2009

FEATURES

Encryption and blocking features:

- Network Connections (Ethernet)
- Firewire (IEEE 1394)
- USB Devices
- CD / DVD discs (Blocking)
- Bluetooth
- Memory sticks
- External hard disc drives
- Memory Cards
- RS232

COMPONENTS OF CERTUS LATEO

Certus Lateo™ is made of the system software, which includes drivers and services, and is installed on each computer, as well as the separate administration panel for configuring the devices for the system.

CERTUS LATEO™

Certus Lateo™ encrypts network connections of a system. This makes it impossible for unauthorized intruders to establish a connection over a network or to steal and read data. A secured Certus Lateo™ system or network is invisible for external devices as the communication necessary for identification takes place in encrypted form.

Certus Lateo™ protects both Ethernet and Firewire connections.

Certus Lateo™ also locks or encrypts the communication with peripheral devices. Thus making it impossible to use data outside the authorized environment, as these are directly encrypted when leaving the system.

For example, if data is copied on a USB memory stick it is automatically encrypted and unreadable on a system without Certus Lateo™. Only when accessing through a legitimate device, the data is available immediately and can be decrypted without any further action.

Certus Lateo™ protects USB ports, CD / DVD drives (customized), floppy drives, Bluetooth connections, memory sticks, RS 232 interfaces, as well as other external data storage such as hard drives or memory cards.

2. INSTALLATION

When installing the components of Certus Lateo™ you have to be logged in with administrator privileges. A reboot of the system is necessary afterwards.

After installing and rebooting, the system is still unprotected and can be used as before, until the desired configuration is set up by a Certus Lateo™ administrator with the Certus Lateo™ admin panel.

This allows for a coordinated migration of all computers on a given time.

PREPARATION

Before installation and activation of Certus Lateo some aspects have to be considered:

- User may not have administrator privileges. An administrator has far reaching privileges on system level and may use them to manipulate the functionality of Certus Lateo Certus Lateo™.
- Make a plan how you would like to configure your system. Which workstations have certain privileges and which Ports and IP addresses should be open for unencrypted communication (e.g. network printers, data base servers etc.)
- Make sure you have taken all necessary complimentary security measures for protecting your data against threats, Certus Lateo cannot cover. (e.g. hardware theft)

UPDATER

Certus Lateo is continuously developed. The most recent version can be downloaded via the Certus Lateo Updater.

These updates improve handling, performance and compatibility with new system and work environments.

After downloading the existing setup files on the USB dongle are automatically replaced with their newer versions.

LOCAL INSTALLATION OF CERTUS LATEO

Certus Lateo™ will be installed through the regular install setup.

It requires no user input.

The relevant driver files are installed automatically and the necessary registrations made.

After the installation, reboot the system.

Important:

In Windows Vista and Windows 7, the setup has to be made with administrator rights.

To install .msi package as an administrator in these operating systems it might be necessary to use the CMD console.

LOCAL INSTALLATION VIA CMD CONSOLE (COMMAND LINE)

For local installation in Windows Vista (and Windows 7) you have to run .msi setup as an administrator, in order to have the necessary privileges for driver installation. Unlike .exe-files these cannot directly be started as an administrator but have to be started with the CMD Console (command line).

1. Open the CMD console in the Start-menu from the folder programs/accessories by clicking with the right button the menu entry "As an Administrator".
2. Then switch to the drive with the Certus Lateo .msi-setup
(Enter the letter of the drive, then ":" and confirm with "Enter". e.g. F: [enter])
3. Open if necessary the folder with the necessary setup-file.
(e.g.: cd *programme/certuslateo/setup* [enter])
4. Start setup by typing the file name and confirming with "Enter".
(e.g. setup.msi [enter])

The same privileges as for the CMD console are now also available for the .msi install file.

Hint: After entering the first letters you can use the TAB-key to see all available files in the directory one after the other.

After the installation, reboot the system.

INSTALLATION OF CERTUS LATEO™ MMC ADMIN CONSOLE

Before installation of the Certus Lateo™ admin panel Certus Lateo™ should be installed on the respective computers already.

1. Start to install the setup file and follow the instructions.

Setup will install an icon inside the Windows® Start Menu and on the desktop called „Certus MMC Admin“ which allows you to start the administration application.

The Certus Lateo™ MMC Admin Console can also be loaded as a Snap-In inside the Windows Microsoft Management Console.

INSTALLATION CERTUS LATEO™ ADMIN PANEL

Before installing of the Certus Lateo™ admin panel Certus Lateo™ should be installed on the respective computers already.

1. Start to install the setup file and follow the instructions.
2. During installation, you are prompted for an administrator password to be defined. You will need it later to open the admin panel. The password protects the admin panel from unauthorized manipulations.

After the installation, reboot the system.

For the correct operation of the admin panel, it can be necessary to configure your local firewall.

NETWORK INSTALLATION

On common systems Certus Lateo .msi setup files may be distributed and installed via a network. Make sure all required privileges for the distribution and installation of drivers are set.

INSTALLATION OF UPDATES

To update Certus Lateo just install the new version over the existing one.

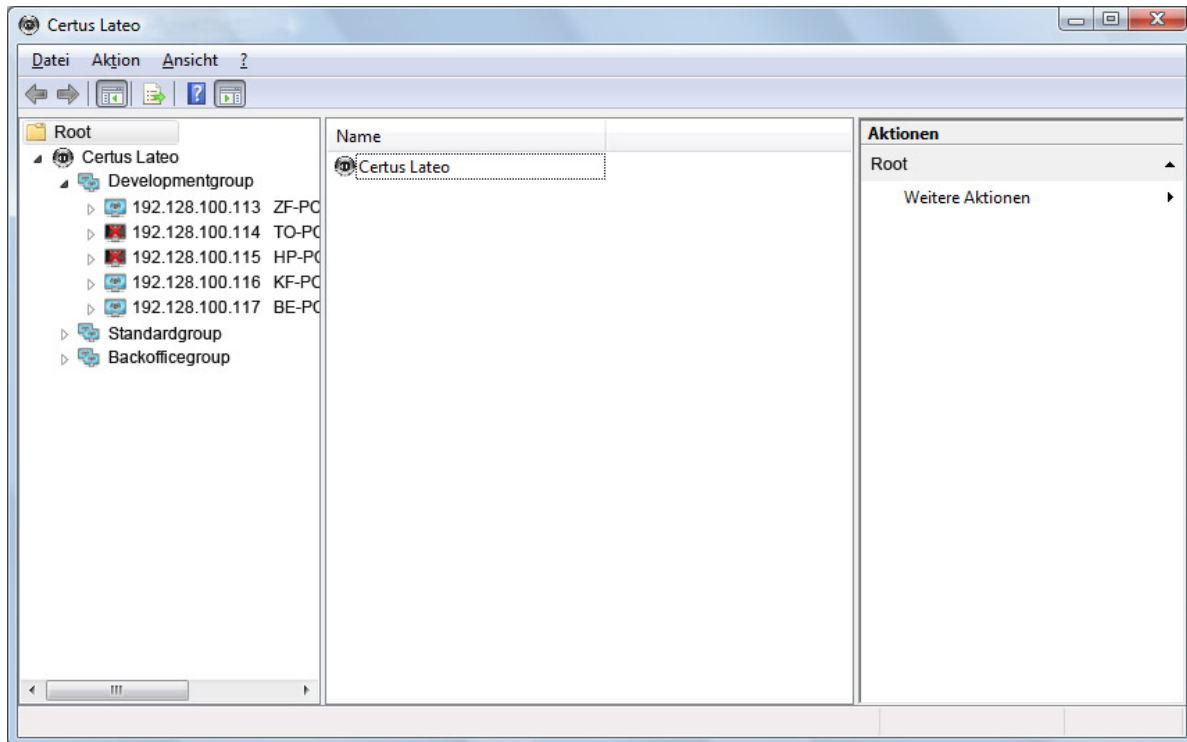
As soon as a new version is available it can be downloaded with the "Certus Lateo Updater" application on the USB dongle. After the download the old setup-file on the USB Stick is automatically replaced with the new one.

Updates have to be downloaded for each USB dongle separately.

For installation of the corresponding components follow the instructions above. During installation the message "Files in Use" might pop-up. You can simply skip it.

3. CERTUS LATEO™ MMC ADMIN CONSOLE

With the MMC Admin Console the Certus Lateo administrator administrates the system configuration. He creates groups with the required settings and assigns the devices inside the Certus Lateo network to these groups.



LAUNCHING THE MMC ADMIN CONSOLE

The MMC Admin Console can be started by clicking on the links at *START/Programs/Barclay Technologies*.

Afterwards you are requested to insert your Certus Lateo™ USB Dongle. The dongle comes with the Certus Lateo™ Setup and allows a unequivocal identification of the legitimate administrator.

Keep it safe!

PANELS IN THE MMC ADMIN CONSOLE

ROOT

In the Root in the left window of the MMC Admin Console the groups installed under „Certus Lateo“ are shown.

„DefaultGroup“ is set by the system and can't neither be deleted nor renamed. It contains all computers which haven't yet been assigned to a group.

OVERVIEW

In the middle section of the MMC Admin Console detailed information for the entry selected in the Root is shown. Either the available groups are shown or the computers contained in a group.

On the left side of the listed computers an icon shows the connection status of this device.



Device is online



Device is offline

ACTIONS

On the right side of the MMC Admin Console you will find the column „actions“ which lists all available functions. These depend from the entry selected in the overview.

FUNCTIONS

ADD GROUP (CREATE NEW GROUPS)

To create a new group select the entry “Certus Lateo” inside the Root.

Inside the „Actions“ panel click on „Add Group“ and enter a name for the new group.

REFRESH GROUPS (UPDATE LIST OF GROUPS)

This function refreshes all available groups and the assigned computers.

REFRESH COMPUTERS (UPDATE LIST OF COMPUTERS)

If new computers were started inside the network or group assignments were changed it might be necessary to refresh the list of computers.

All computers in all groups are refreshed.

SHOW LICENSE INFORMATION

This function opens a window with up-to-date licence information. This means the licence ID, the used and the maximum number of computers for this licence and the expiration date of this licence.

REFRESH LICENSE INFORMATION

When your dealer has extended or renewed your licence you have to refresh it with this command for your system.

RENAME (OF A GROUP)

1. To change a group’s name choose the entry “Certus Lateo” in the Root. The Overview window will show you all available groups.
2. Click on the group you want to rename.
3. In the „Actions“ panel you will find now the „Rename“ command.

MOVE (ASSIGN A COMPUTER TO A GROUP)

1. Open in the directory tree the group containing the computer you want to assign.
2. Choose the device and click on the „Move“ function inside the actions panel.
3. Choose your group among the groups listed and confirm with „Accept“.

The computer is now assigned to the new group and is automatically set-up with the group settings.

DELETE (COMPUTER)

To remove a computer from the system use the “Delete” command. This will just remove it from the list and unblock its licence for another computer.

EDIT (SETTING UP A GROUP)

Choose the group you want to edit. Then open the configuration window with the "Edit"-button from the "Actions" panel.

The window for group configurations:

- Basic settings
- Port and IP entry
- Overview window for existing Port and IP entries

MASS STORAGE DEVICES

Here you configure the settings for mass storage devices like USB sticks.

Open:

Mass storage devices can be used without restrictions.

Locked:

Mass storage devices are locked.

Crypted:

Data may only be written in encrypted form to a pre-defined Folder on the Mass storage device.

IMPORTANT NOTES:

Please note, that changes for a USB Mass storage devices do not apply while the device is active. That means plugged-in and in use.

In order to read encrypted data (Data at rest) again you need a computer with the same, valid licence of Certus Lateo, which was used during the storage process!

Additional (secondary) internal SATA discs must be configured in BIOS as „enhanced system disc“. Otherwise the operating system might treat them as mass storage devices.

COMPACT DISC'S

Permissions for the use of CD and DVD burners are administrated here.

Open:

Devices can be used without restrictions.

Locked:

Writing on CD and DVD drives is blocked by deactivating the internal write function of Windows.

Changes in the writing permissions of CD and DVD drives are only active after a restart of the system.

Important:

In order to efficiently prevent writing on CD and DVD drives no other applications for burning CD or DVD must be installed as these applications normally come with their own drivers.

NETWORK

Here you activate encryption of the entire network communication.

Open:

Network encryption is deactivated.

Crypted:

Network encryption is activated. The system can exchange data in encrypted form with computers inside the same Certus Lateo Network, as well as unencrypted via defined Ports and IP addresses.

SHOW STARTUP SPLASHSCREEN

The Startup Splashscreen is shown on start of the operating system informing the user about the installed Certus Lateo™ Software.

Activate this window with „true“ or deactivate it by selecting „false“.

SHOW TRAYICON

With the setting „true“ the tray icon is shown on the right in the task bar informing the user about the installed Certus Lateo™ Software. Deactivate it by selecting „false“.

PORT AND IP DEFINITIONS

Normally Certus Lateo encrypts the whole network communication. In some cases it might be necessary to use certain ports and IP addresses or address ranges for unencrypted communication if the other side does not support the required Certus Lateo™ installation. (e.g. network printers, external systems, other OS's etc.)

For this purpose single Ports, Port ranges, single IP addresses and IP address ranges may be defined, which allow unencrypted communication.

Editing Port and IP Definitions:

To add new entries fill in the values in the corresponding fields and add them with „Add“ to the list.

Delete entries by selecting them and clicking „Delete Selected“ then.

With „Accept“ all settings are activated.

Those computer which are not connected with the system during configuration changes will be updated with the new settings on their next access to the Certus Lateo network.

INTERNET AND EMAIL

On many workplaces access to the Internet (Port 80) is a must. Nevertheless, if you open this port, you have to be aware there is an open door in your network, which allows transmission of all kind of data. (Via an Upload Script for instance).

The same is true for E-Mail-Traffic: Data may be transmitted freely to others.

Make sure to log all these activities with your infrastructure and inform users, that these activities are monitored.

4. CERTUS LATEO™ ADMIN PANEL

The Admin Panel is an administration tool especially used on smaller networks. Compared to MMC Admin Console it offers no functionality to configure groups of computers. It rather treats each computer as an individual device. For this purpose the Admin Panel can be installed and used on every system, which is part of the Certus Lateo™ environment.

START

The configuration of the Certus Lateo™ environment done with the Admin Panel requires a particularly good access protection.

Both the correct administrator password and a hardware and software product identification (dongle) is used to start the application. This dongle cannot be copied and identifies the owner as a legitimate administrator.

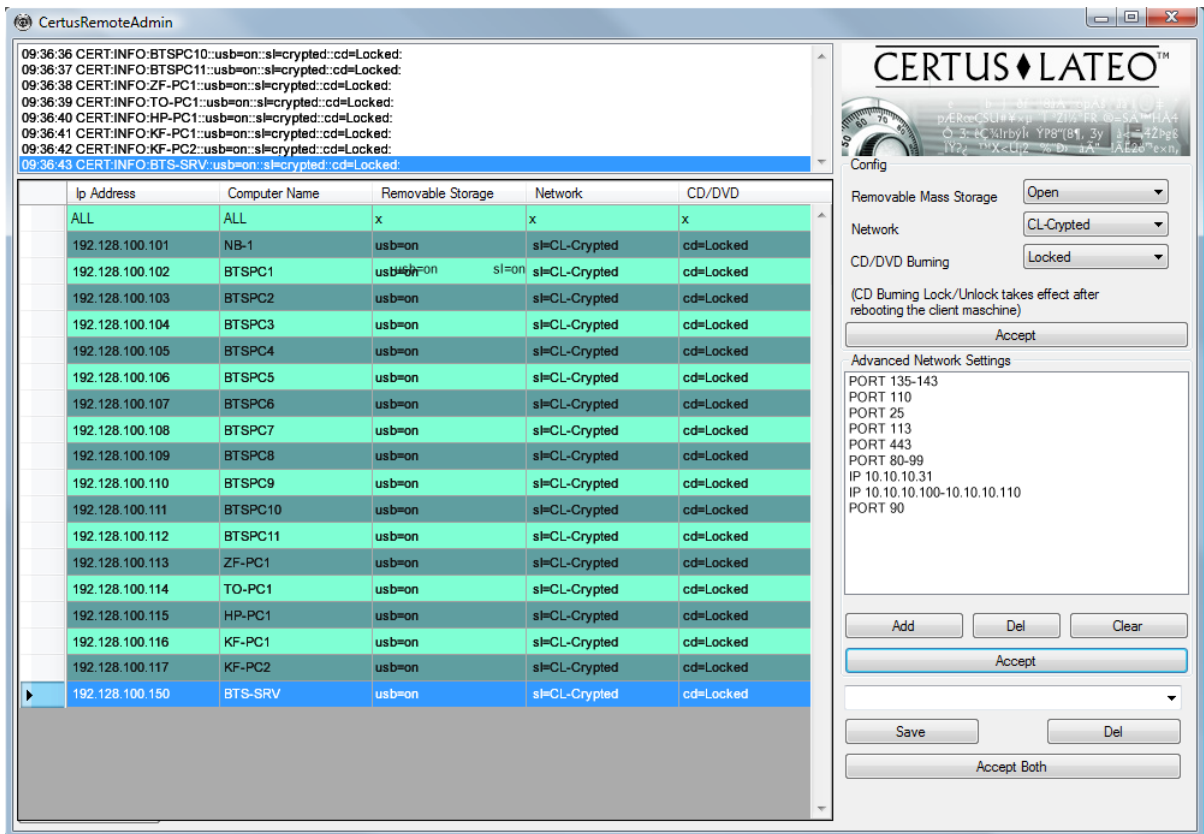
After entering the administrator password, the dongle (USB stick) has to be connected with the device within a maximum of 60 seconds. Otherwise, the start-up process quits.

For systems with a disabled USB port this port will be temporarily unlocked for the duration of that time.

CONFIGURATIONS

After the program starts, the list of the systems belonging to this Certus Lateo™ environment is loaded. This is done by the "Computer Update List".

The time to generate this list depends on size and speed of the network.



PROTOCOL

The system log shows major events while working with the administration panel.

Pressing the right mouse button opens a dialog which allows to export the log to a text file.

LIST

Here all devices belonging to the Certus Lateo™ network and their respective configurations are displayed.

The list includes information on:

- IP Address
- Computer name
- Current configuration of a USB memory, SD and MMC cards, http (port 80), network connection as well as CD- / DVD-drives.

CONFIG

Once a device in the list has been selected the "Config" area the respective settings are shown. They can be modified here with the selection lists and activated by clicking on "Accept".

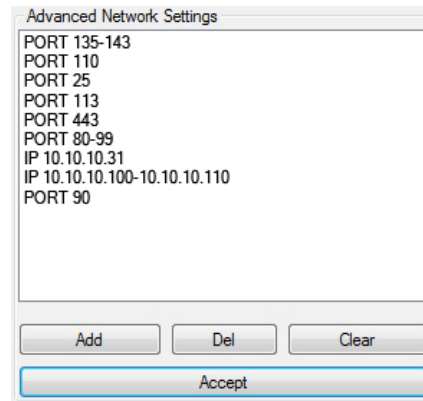
It might take some time until all settings are applied on the devices.

Important: USB sticks have to be removed before changing the configuration in order to apply the new settings.

IP AND PORT SETTINGS

The IP and port settings allow you to define individual IP addresses, IP areas, individual ports and port areas on which the system can communicate **unencrypted**.

These are entered line by line, as a single number (for example. "80") or with "from / to" definitions (e.g. "811 - 827")



The configurations you have made can be named in the list and saved by clicking "Save". So they're available for further configuration procedures.

With "Accept", the displayed settings are applied for the selected device.

Note:

After selecting a device, the current configurations do not appear.

5. ANNEX

SYSTEM REQUIREMENTS

Certus Lateo runs with every 32- or 64-bit Windows OS. The newest Service Pack is always required. Certus Lateo™ has been tested on these systems:

- Windows XP (Home, Professional)
- Windows 2003 Server
- Windows 2008 Server
- Windows Vista
- Windows 7

OTHER CONDITIONS

There are myriads of possible different hardware configurations which we couldn't test all. But there shouldn't be any errors caused by the system if the Hardware corresponds with good common standards

EXHIBIT A: BTSAG ENDUSER LICENSE AGREEMENT

LICENSE RIGHTS END USER LICENSE AGREEMENT FOR CERTUS LATEO™ - applications
SOFTWARE PACKAGE IN ACCORDANCE WITH APPLICATIONS PARTS PACKAGE

IMPORTANT - PLEASE READ CAREFULLY:

This BARCLAY TECHNOLOGIES (SWITZERLAND) AG (BTSAG) End User License Agreement ("EULA BTSAG-ELV") is a legal agreement between you (either an individual or legal person) and BTSAG.

This BTSAG-ELV governs your use of the CERTUS LATEO™ - Software and the Software related components, including but not limited to, CERTUS LATEO™ - SL, CERTUS LATEO™ - PL, CERTUS LATEO™ - WL, CERTUS LATEO™ - AL and CERTUS LATEO™ - DK. The Software may include associated media and printed materials, and Documentation in the "online" or electronic format. By using the SOFTWARE PRODUCT is installed, copy or otherwise use you agree to all provisions of this EULA, BTSAG to be bound. If the provisions of this EULA, do not BTSAG agree, you are not entitled to the SOFTWARE PRODUCT to install or use.

The SOFTWARE PRODUCT is protected by copyright laws and international copyright treaties, as well as other Laws and agreements on intellectual property. The SOFTWARE PRODUCT is licensed, not sold.

1. LICENSE GRANT.

The SOFTWARE PRODUCT is licensed as follows:

- Use and copying of "CERTUS LATEO™": Barclay Technologies grants you the right to make copies of the SOFTWARE PRODUCT CERTUS LATEO™ on exactly solved in the license number of defined computers, worldwide, on the valid licensed copies of that operating system, for which the SOFTWARE PRODUCT has been developed [eg Windows ® 7, XP, Vista, etc.], to install and use.

- Use and copying of "CERTUS LATEO™ SL (Socket Layer) and PL (Periphery Layer)": BTSAG grants you the right to make copies of the SOFTWARE PRODUCT CERTUS LATEO™ - SL and PL in exactly in the License Number dissolved defined computers, worldwide, on the valid licensed copies of that operating system, for which the SOFTWARE PRODUCT has been developed [e.g. Windows 7, Windows VISTA / Windows XP ®,], to install and use.

- Use and copying of "CERTUS LATEO™ - WF (Web Front)": BTSAG grants you the right to make copies of the SOFTWARE PRODUCT CERTUS LATEO™ - WL for the license referred to web application Servers on which valid licensed copies of that operating system, for which the SOFTWARE PRODUCT has been developed [e.g. ®, Windows Server 2000 -2008], to install and use.

- Use and copying of "CERTUS LATEO™ - AL (Application Layer)": BTSAG grants you the right to make copies of the SOFTWARE PRODUCT CERTUS LATEO™ - AL for which the license application to install and implement and use.

- Backing: You are also entitled to for backup and archival purposes necessary copies called SOFTWARE PRODUCTS records.

2. DESCRIPTION OF OTHER RIGHTS AND LIMITATIONS.

Preliminary version software

If a component of the SOFTWARE PRODUCT as a "pre-release" or "beta" tag, this component of the SOFTWARE PRODUCT Pre-release code and will possibly appear before the Final-Release fundamentally changed. You are not entitled to such a component in a live operating environment to use in which they are as reliable must operate as a final product delivery or when working with data is not sufficiently backed up.

Copyright Notices:

You are obliged to copyright notices on all copies of the SOFTWARE PRODUCT may be secured and will not change.

Sales:

You are not entitled to copies of the SOFTWARE PRODUCT to third parties except in accordance with Section 1 expressly authorized form.

Prohibition in relation to Back Development (Reverse Engineering), Decompilation, and Disassembly.

You may not use the SOFTWARE PRODUCT reverse (Reverse Engineering), decompile or disassemble, unless because and insofar as the applicable law notwithstanding this limitation, this is explicitly permitted.

Efforts to crack when the SOFTWARE PRODUCT or the encryption used by the SOFTWARE PRODUCT encrypted data are not allowed.

Rent:

You may not use the SOFTWARE PRODUCT to rent, lend, or sell.

Transmission:

You are entitled to all of your rights under this EULA BTSAG- permanent transfer, provided the recipient agrees to the terms of this BTSAG-ELV in written form.

Support Services:

BTSAG or its Resellers /Distributors offer with support services in conjunction with the SOFTWARE PRODUCT ("Support Services"). The support services may be the BTSAG rules and programs in the User's Manual, the documentation in online format and / or other BTSAG made available materials described are used. Any supplemental software code provided to you as part of Support services will be made available, as part of the SOFTWARE PRODUCT and is subject to the provisions and BTSAG-conditions of this EULA. BTSAG is entitled to the technical data you BTSAG as part of the Support services available for business purposes, including product support and development, to be used. Agrees to such technical data only anonymous in the sense of privacy should be used.

3. OBSERVANCE OF ALL APPLICABLE LAWS

You are obliged to use the SOFTWARE PRODUCT only in accordance with all applicable domestic and international laws to use. In particular, the national regulations in relation to encryption technologies.

4. DENUNCIATION

Without prejudice to any other rights, BTSAG entitled to this BTSAG ELV to terminate if you violate the terms and conditions of this EULA-violating BTSAG. In such a case, they obliged, all copies of the SOFTWARE PRODUCT be destroyed.

5. PROPERTY

All property rights, including but not limited to copyright, in and to the SOFTWARE PRODUCT and each copy of which are BTSAG or its Suppliers. Property rights and intellectual property on and in relation to the contents, by the SOFTWARE PRODUCT is accessed, belong to the respective owners and may be appropriate copyright or other laws governing intellectual property protected.

This BTSAG-ELV gives you no rights in such content. All rights not expressly granted remain BTSAG reserved.

6. EXPORT RESTRICTIONS

Hereby you agree that this SOFTWARE PRODUCT in a country, to a person, a legal person or to end users who, of the through Switzerland imposed export restrictions, export or re-be. You hereby give the assurance and declare that neither the Swiss Office for export permits, nor any other Federal authority suspended the export permit, withdrawn or rejected.

7. WARRANTY

BTSAG expressly excludes any warranty for the SOFTWARE PRODUCT from. The SOFTWARE PRODUCT and related documentation is provided "as is" made available without warranty of any kind, either express or implied, including but not limited to implied warranties of suitability, fitness for a particular purpose or non-existence of an infringement. The entire risk arising out of the Use or performance of the SOFTWARE PRODUCT is, remains with you.

8. LIMITED LIABILITY

Until by extend permitted by applicable law, neither BTSAG nor its suppliers or its Resellers/Distributors be liable for any special, incidental incurred or indirect or consequential damages (including, but not limited to lost profits, business interruption, Loss of business information, or any other pecuniary loss) arising from the use or inability to SOFTWARE PRODUCT be used, or the performance or non performance of support services and, even if BTSAG previously to the possibility of such damages has been advised. In any case, BTSAG entire liability to the amount of EUR 00.00, or at US\$ 00.00. - limited. However, if you're with BTSAG a contract for support services completed, it will BTSAG entire liability in Relation to support services through the provisions of this Treaty.

9. MISCELLANEOUS

Because some jurisdictions allow the exclusion or limitation of liability for consequential or accidental damages not permit applies the above limitation may only act in the appropriate context. Should one or more provisions of this contract for any reason be or become invalid, it is considered the validity of the Contract as a whole is not affected. Rather, the parties undertake to replace the ineffective provisions with their economic Purpose corresponding effective scheme to be agreed. And in a way that the parts in accordance with the legally intended purpose so far as possible achieved / met.

This BTSAG-ELV is subject to Swiss and the International substantive law.

Place of performance and jurisdiction is Zürich (Switzerland)

By using the SOFTWARE PRODUCT is installed, copy or otherwise use, you agree to the contents of the Handover documentation software products / services supplied are complete and exhaustive as ordering to have received.

Zürich, January 2010

BARCLAY TECHNOLOGIES (SWITZERLAND) AG (BTSAG)

Safety precautions

Please note that all data during transmission via a secure encrypted Krypt algorithm and thus an attacker unreadable form. Only the sender and the receiver are directly addressed the necessary decryption methods known to send the data back to its original state.

Encrypted data can be licensed and / or crypto-related sentence and solely with the encryption used in the re-readable versions.

Warning

The described computer program is protected by copyright worldwide. You are not entitled to the program or parts thereof without the express permission of the manufacturer to reproduce or distribute. Adversaries can be a civil action or criminal punishment after being taken and are in accordance with the applicable law with the greatest hardship prosecuted.

This user manual is copyrighted. It may not be copied, nor in any other manner reproduced. It may not in any way, nor distributed in part or in any other language to be translated.

The content of this documentation is available with no obligation or guarantee of any kind connected. The publisher can not accept responsibility or liability for the consequences which is based on incomplete or erroneous information contained in this manual are due.

All Rights Reserved.

