Corporate Portal

Security recommendations

hilfe.hvb.de
gtb-center@unicredit.de

UniCredit

Content

GENERAL

SAFE PASSWORD

SECURITY OF THE COMPUTER

TWO FACTOR AUTHENTIFICATION

- UC MOBILE TOKEN APP
- PHOTO TAN

SINGLE SIGNATURE RIGHT

RESPONSIBLE HANDLING OF DATA AND PROGRAMS

MOBILE DEVICES

SOFTWARE DISTRIBUTION REGULATES PROGRAM INSTALLATION

HUMAN FACTOR

SPECIFIC FEATURES FOR INDIVIDUAL APPLICATIONS

- UC EBANKING GLOBAL
- UC TRADER
- UC TRADE FINANCE GATE
- COMMUNICATION SUITE

SUPPORT

GENERAL

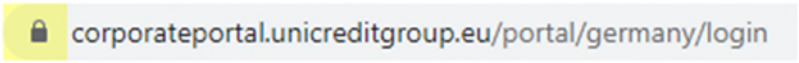
In contrast to software operated directly on your local computer UniCredit Corporate Portal is a service operated centrally at UniCredit Bank for many clients. Corporate Portal is accessed via a browser and all functionalities are displayed online. All data -with exception of a secret access key - is not stored locally within your premises.

As is generally the case, the authorization profiles for Corporate Portal and all associated applications should be regularly checked and adjusted to ensure that they are up to date (e.g., deletion of employees who have left the company, changes to signing authorizations, etc.). If you consider a particularly high level of protection to be necessary for Corporate Portal access, access should only be granted to a restricted group of people.

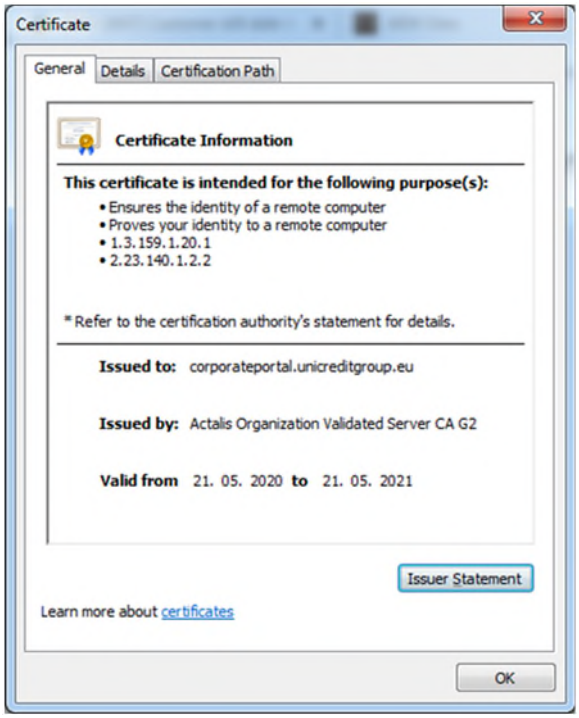
ACCESSING CORPORATE PORTAL

Data communication between customer and bank is done by a TLS encrypted communication. Most browsers signal https-secured communication by showing for example the lock-Symbol in the browser. Never enter confidential data (especially your password) without first checking the address! Below you can see an example of the Google Chrome browser.

https://corporateportal.unicreditgroup.eu/portal/germany/login



The certificate must be issued to the operator of the portal solution (in the case of Corporate Portal it is UniCredit Bank). It is signed by a trusted certification bureau. To make sure you relate to the correct address, you may check the server certificate: double click on the lock symbol in the browser address line.



There must not be any problems regarding the certificate when accessing the internet address of Corporate Portal. In such cases the browser will warn you and indicate problems with the security certificate or gives the hint that this connection is not trusted. Please contact our helpdesk via Phone +49 89 55299699 or via email gtb-center@unicredit.de if this occasion arises.

The Internet connection required to use Corporate Portal should always be established via secure Internet access. The use of unsecured or unknown WLAN access (e.g., Internet café) is strongly discouraged.

SINGLE SIGN ON

Once you successfully signed on to Corporate Portal all assigned applications are at your disposal without further log-in procedures (“Single Sign On“).

Usage of further applications (and mapping to your log-in) requires additional contractual agreements. Please contact your relation-ship manager or Cash Management/Trade Finance Specialist in this case.

If an application demands another authorization e.g., to release transactions, this is also done by means of the security method for the log-in.

AUTOMATIC LOG-OUT

For security reasons after inactivity of 5 minutes you will be logged out automatically. You can log-in again directly afterwards. The applications themselves may have a longer period until automatic log out.

SAFE PASSWORT

In general, all passwords should be sufficiently long and complex. A change of passwords is mandatory if you have suspicion of any other person having knowledge of your password. No identical passwords should be used for different purposes or applications. The passwords also should not differ only by replacement of one character.

As guideline for safe passwords please consult the recommendations of the German BSI: https://www.bsi-fuer-buerger.de/.

In places where a password is necessary, Corporate Portal or its application will require a minimum quality of the passwords. This will automatically be tested during password administration. The minimum requirements are specified by the Bank and may be changed, if necessary.

To avoid password leaks no password is to be written in plain text on the computer (e.g., in a file) or on a sticky note. Instead, a free accessible tool for password handling could be used which in general also supports safe password generation.

SECURITY OF THE COMPUTER

SECURE OPERATING SYSTEM

The operating system and other installed software e.g., PDF reader and browser must be updated regularly. The updates should be done only by means supplied by the provider e.g., Windows update or available update links within the software.

SECURE BROWSER

Only use browsers released by UniCredit Bank (see Release Notes) and perform the security updates supplied by the provider in time. Usage of additional programs in the browser should be avoided when they are not necessary. Additional programs should only be activated for trusted websites. If the browser supports mechanisms designed for Phishing and Malware Protection these should be used.

As a guideline for security settings of several browsers please also consult: www.bsi.bund.de/.

UPDATED VIRUS SCANNER

Usage of anti-virus software is mandatory. Also, this software must be updated regularly. In general, the anti-virus software includes permanent scans and automated updates in the background after every start of the computer. Additionally, the computer should undergo a complete testing by the anti-virus scanner at regular intervals.

Make sure the anti-virus software includes protection of your browser.

TWO FACTOR AUTHENTIFICATION

The two-factor-authentication means the authentication of a user by using two independent security features. This minimum two-factor-authentication could be combined of the feature “knowledge” (e.g., a password), “possession” (possession of a smartphone,

photoTAN Reader or key file) and “biometrics” (e.g., fingerprint, Face-ID).

UC MOBILE TOKEN APP

AUTHENTICATION AND AUTHORIZATION WITH A SMARTPHONE

The UC Mobile Token App is a security application which keeps at hand the required personal key for user authentication and authorization of transactions or administrative modifications and by using the smartphone is shifted to another channel of exchange with the bank. The user can only work with Corporate Portal if he is in possession of the smartphone and the associated password and/or biometric feature.

LOG-IN WITH THE UC MOBILE TOKEN APP

For access to Corporate Portal the user or administrator uses his smartphone to which the UC Mobile Token App is downloaded and installed. Corporate Portal shows an access code to the user which the user enters in the app or scans as QR-code. Now he is asked to enter a safe password (see chapter safe passwords). Another option is using biometric authentication (Face-ID or Touch-ID). Once the system has checked the code the user can safely work with Corporate Portal.

SECURITY OF THE UC MOBILE TOKEN APP

Every App of UniCredit Bank can detect modifications by “Jailbreaks” or “Root-Kits”. Should the case arise, the application will instantly delete all stored data and keys for security reasons.

Data on the UC Mobile Token App is encrypted with a device-specific characteristic. Therefore, the data is linked to the smartphone in use. When changing smartphones, the user needs to download the app to the new smartphone and authorize the new one with the old phone. A user guide for these steps is on our help site.

After entering a wrong password five times in a row the UC Mobile Token app also will delete all stored data and keys.

The UC Mobile Token App always requires a device-specific passcode or biometrical lock. Is this not the case, the app cannot be used.

DOWNLOAD OF THE UC MOBILE TOKEN APPS

Google Play Store for Android:

https://play.google.com/store/apps/details?id=de.unicredit.mobiletoken&hl=de

Apple App Store for iPhone:

https://apps.apple.com/de/app/uc-mobile-token/id1103148048

PHOTOTAN

AUTHENTICATION AND AUTHORIZATION WITH PHOTOTAN

The photoTAN method is a secure 2-factor-authentification method which requires a photoTAN generator. It can also be used when a smartphone is not available for use of the UC Mobile Token app. The user must be in possession of the photoTAN device and know the PIN code to be able to work with Corporate Portal.

Up to 8 different User IDs can be stored on one photoTAN generator. For every user an individual PIN code is assigned.

LOG-IN WITH PHOTOTAN

The device has the purpose of generating an individual TAN-code. To register a user on the photoTAN the Portal-ID, the photoTAN device and a freely chosen 4-digit PIN code are necessary. For every authorization a photoTAN graphic, a square picture with colored dots, is shown. Please scan this graphic with your photoTAN device and enter your PIN code. The data effective for this transaction is shown on the display of the photoTAN generator. After confirming, the device generates the TAN-code which is needed in Corporate Portal.

SECURITY OF THE PHOTOTAN DEVICE

The data is secured with the PIN-code. After entering a wrong PIN-code five times in a row the photoTAN device deletes the registration and the user must perform a new initialization process.

ORDERING A PHOTOTAN GENERATOR

Orders are available at http://www.hvb.de/order-phototan

SINGLE SIGNATURE RIGHT

Legally it is possible to arrange a single signature right for a bank related signature. This means that only one signature can be required to release transactions.

To enhance the security level, we strongly recommend a joint signature. Therefore, you agree with the bank on two or more signatures for authorization of transactions. The 4-eye-principle is known as effective measure against assaults, as malicious or manipulated payments (e.g., after loss or theft of the key but also after social engineering attacks) can be detected and dismissed by the user with second signature.

RESPONSIBLE HANDLING OF DATA AND SOFTWARE

Measures must be taken for information security on organizational, technical, and personal level. These measures need to include protection of access to premises and data, installation of firewalls, active management of access rights as well as monitoring and logging. Protection from malware today is essential. Furthermore, a regulated process to install software and provisions to protect the corporate network are to be implemented.

Also, in your technical environment precautionary measures need to be taken to support the included security policies for data exchange. Information and recent notes can be found at http://www.bsi.bund.de/.

MOBILE DEVICES

Daily weak spots are detected within software and operating systems of smartphones and tablets. These can be utilized by hackers and therefore pose a threat to your equipment. To protect yourself, the operating system and applications always need to be up to date with updates and versions. Keeping track of this is a challenge. The same rules as for your computer apply to your mobile device.

The biggest security risk is the loss of your smartphone. Assign a code, a password or take other protective measures to lock your phone. Then unauthorized persons cannot access your data. In the case of losing your smartphone better change all your passwords at once and use the option of remote access with a security tool to delete data on your smartphone or block the entire device.

Never leave your smartphone unattended when you are working with Corporate Portal. Also make sure no one is watching your screen when working with sensitive data. Only use your mobile device in trusted networks or via mobile internet access.

Download applications and software only from trusted sources, e.g., Apple App Store or Google Play Store. Check the security settings of every downloaded app, access rights and if necessary external assessments. If need be, restrict the security settings to your framework requirements.

Be careful with links received via SMS or email. This also applies to links hidden in QR-codes. Only follow links from trusted sources.

Always deactivate internet access, Bluetooth, Infrared and WLAN or NFC when they are not in use. This way you can hinder criminals to access your data via WLAN-spots or Bluetooth. Encrypt your data whenever possible and deactivate the device code for Bluetooth.

Secure your data with back-ups on a regular basis on a stationary computer. When selling, giving away or recycling your phone delete all data beforehand.

Every provider is offering service and security updates for their operating systems. Keep yourself informed on the webpages of your provider.

Communication between your mobile device and the Bank is very steady. System breakdowns or similar are rare. Be wary when your device acts unusual. Especially if you are facing program aborts after entering your password. When in doubt, always contact your Bank.

Do not use modifications of operating systems of your smartphone or tablet like “jailbreak”, “custom-ROMs” or “rootkit”. These modifications might contain code that enables hackers to read along data exchange of your banking apps.

SOFTWARE DISTRIBUTION REGULATES PROGRAM INSTALLATION

Installation and maintenance of software should solely be done within a regulated process (e.g., temporary administrator access rights and documentation). Especially in case of installation of banking software by service providers other than banks the technical access rights need to be restricted and deleted directly after installation. The technical access rights must be authorized by the IT-responsible of your company. To enhance the security level authorization and installation process should be concluded in 4-eye-principle and be duly documented. Workplace and access (e.g., remote access) needed for the installation should be defined and authorized beforehand.

HUMAN FACTOR

Social Engineering means an assailant is taking advantage of human characteristics to gather confidential information. In the imagination of many people internet criminals are technical masterminds programming complex codes to hack computer networks. This often is not reality. Next to classical “hacking”, meaning invading a computer by technical means such as a computer virus, there are easier ways for criminals to gain valuable information.

Why not just ask nicely?

Hard to believe but the method of “social engineering” is very promising especially in companies with above-average IT security. Assailants take advantage of human traits such as good faith, helpfulness, pride, conflict avoidance or respect for authorities to gain information using psychological tricks. A social engineering attack usually starts by gathering general information of the company which is targeted to be assailed or spied on.

Social engineering for internet criminals is a popular method to unauthorizedly gain insight on sensitive information: it is for free and overcomes even the best IT security barriers.

An organizational chart or telephone list are enough for an experienced assailant. The assailant calls the company with the knowledge of hierarchical structures. He is faking an identity to slowly give out important information using skilled questioning and psychological tricks. Often the offender takes up the role of a person of trust or authority. He collects information pieces that make him seem trustworthy in other places.

Very frequently social engineers have it in for passwords and access to banking data. The assailant fakes a problem, e.g., a hacker attack that requires immediate action to for example log-in to the banking software. The assailant presents himself sure and authoritative and imposes stress on his victim, which is chosen by psychological aspects and many times readily gives out access data.

Social engineers pretend being someone else and fake an identity. Therefore, never give out information you are not entitled to. This includes work and company organization, responsibilities, personal information of colleagues or even user data. Only give out as much information as really needed and question the requests of a caller.

Careless decisions regarding security are often taken to be polite or in situations of stress. When in doubt: security comes first, courtesy later. A process should be in place that it is not to your disadvantage to reassure with your superiors even if it means an important customer or manager may have to wait.

Never keep written notes and correspondence in plain sight on your desks but protect information from third parties. Always store sensitive data encrypted on your computer. Even from apparently unimportant information crucial conclusions can be drawn in combination with other facts. Avoid talking about business matters in public places such as trains or restaurants.

Further information and recent examples on the topic of Social Engineering can be found on our website for this purpose: http://www.hvb.de/ceo-fraud

SPECIFIC FEATURES FOR INDIVIDUAL APPLICATIONS

UC EBANKING GLOBAL

UC eBanking global is an eBanking application with which you may receive account statements and enter payments. It is subject to PSD2 directive. UC eBanking global is integrated in the Corporate Portal. Every hereunder written aspect for Corporate Portal also applies to UC eBanking global, additionally there are the following security characteristics:

AUTHORIZE PAYMENTS AND MODIFICATIONS WITH UC MOBILE TOKEN APPLICATION

To authorize payments or administrative modifications in UC eBanking global the user selects the orders or subjects he would like to release. Automatically the UC Mobile Token App shows a summary of this selection on the smartphone of the user. The user reviews the data and comfortably authorizes the proceedings by entering a passcode or by touch ID. Following UC eBanking global further processes the transaction as soon as all required signatures are added.

This process is also applicable for other installed EBICS banks.

AUTHORIZE PAYMENTS AND MODIFICATIONS WITH PHOTOTAN

To authorize payments and administrative modifications in UC eBanking global the user selects the orders or other administrative objects he would like to release. The user scans the shown picture and hence receives a summary of his selection. After reviewing the data and confirming with his PIN code a TAN code is displayed on the photoTAN reader. This TAN code is inserted in UC eBanking global. Following UC eBanking global further processes the transaction as soon as all required signatures are added.

Key Files for third banks in combination with photoTAN

In the case that other EBICS third banks should be used, an additional Keybag.dat key is to be applied, to maintain compatibility to EBICS standard.

These so-called software keys are stored within files. The keys are furthermore protected by a password. Please be aware to store it safely and protect it from unauthorized access.

When storing key files on a central storage medium other person such as system administrators could potentially have access. Removable storage containing key files can accidentally be forgotten in a public space or left in a PC.

Key files might be copied unnoticed and used by unauthorized persons. Software keys therefore should not be stored in stationary storage (e.g., local networks or company drives) but at least be stored on removable mediums which can be physically stored in a safe place.

The removable medium (e.g., USB-stick) on which the software key is stored is to be protected from abusive usage and theft. This requires safekeeping e.g., by locking it. Furthermore, we recommend safeguarding access to the security medium. This can be done by using USB sticks with a numeric keyboard and encryption hardware.

Security mediums for storing key files should only be used for this purpose and not hold any other data. Access to the removable medium and the saved software key must be secured by using a password. UC eBanking global allows access to the keys only by entering the correspondent password. Rules to set up and alter passwords should be an integrated element of your company's security guideline. Further references on the topic of password security can be found in this brochure.

After final usage of the key file the removable medium should be safely disposed of or destroyed.

Instant blocking of keys at suspicion of misuse or theft

When having a suspicion of misuse or theft of your key file it is required to immediately inform your collaborating banks of this suspicion. All access of affected users to UC eBanking global will be blocked.

It is possible to change the software key at any time. In this connection your key file will be modified, and the old version is no longer applicable.

UC TRADER

For UC Trader no automatic log out is done after 5 minutes of inactivity. Your access to Corporate Portal and other applications will still be terminated after 5 minutes of inactivity.

In case of questions regarding UC Trader please contact your Corporate Treasury Sales specialist or FX eSales Support.

UC TRADE FINANCE GATE

For UC Trade Finance Gate there is no automatic log out after 5 minutes of inactivity. Time period for automatic log out in this case amounts to 30 minutes. Your access to Corporate Portal and other applications will still be terminated after 5 minutes of inactivity. However, you can continue to work in the UC Trade Finance Gate and transfer transactions regardless of this.

The administration of user rights is handled partly by the bank (creation of users with release rights), partly by the main users nominated by the customer. Input, viewing and releasing rights are defined by the user roles according to your UC Trade Finance Gate edition. Details in this regard can be reviewed in the user manuals or by contacting your Trade Finance Sales specialist.

COMMUNICATION SUITE

Via the communication suite of the Corporate Portal, you can safely exchange messages and files in a secured channel. In contrast to email communication a transport encryption is applied. Moreover, single messages and files can be provided with a digital signature that in some cases can even replace a genuine signature on paper.

Please contact your Specialist or Relationship Manager for more information.

SUPPORT

At having the suspicion of:

- Someone having unauthorized access to your account
- Having lost access credentials by accident, theft, or unauthorized copy
- Being victim of a CyberCrime Attack

Or questions regarding data safety in general or to this brochure please contact our Helpdesk at:

gtb-center@unicredit.de