COMSUITE Portal Quick Reference

March 2025

COMSUITE
GLOBAL TRANSACTION BANKING SOLUTIONS

MUFG Bank, Ltd.
Transaction Banking Division
A member of MUFG, a global financial group

MUFG

Table of Contents

Chapter 1 Connection/Login

1-1 Check the Operating Environment of Your PC

The specified operating system, browser software, and PDF viewer software are required for using the Service.
Access the below mentioned URL and refer to "Customer Support" for the latest available Operating Environment.

URL: https://ebusiness.bk.mufg.jp/login/

1-2 Login

This service uses OTP tokens to authenticate users. OTP tokens are issued by MUFG Bank and will be necessary for login and giving approval in each service.

Have your OTP token ready.

**When logging in for the first time or logging in after resetting your password,
see "■ When logging in for the first time or logging in after resetting password" following this procedure.**

OTP Token

Enter the COMSUITE URL in your browser's address bar.

URL: https://ebusiness.bk.mufg.jp/login/

By adding the login page that is shown after accessing the mentioned URL as a favorite (bookmark), the mark appears as a favorite icon.

Login Screen

The Login screen will be displayed.

Enter your COMSUITE customer ID, COMSUITE user ID, and password in the [Customer ID] field, [User ID] field, and [Password] field, respectively.

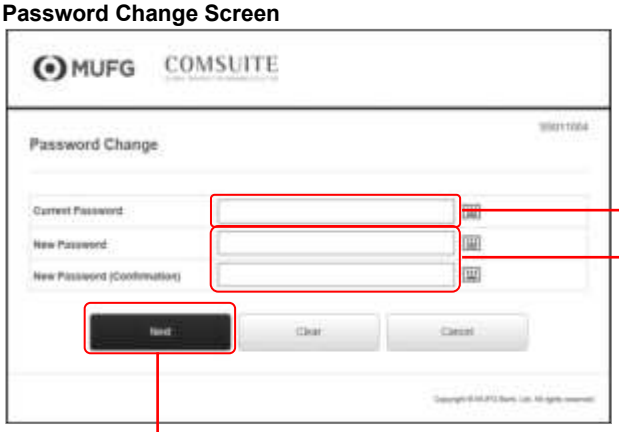
When logging in for the first time or logging in after resetting your password, see "■ When logging in for the first time or logging in after resetting password" following this procedure.

Once you enter these information, the OTP field becomes available.

Press [1] on the OTP token and enter the OTP, which is displayed on the token, in the [One-time Password (OTP)] field.

Click Login

Password Change Screen



The Password Change screen is displayed in case that your password is expired.

Enter the password, which you entered on the Login screen, in the [Current Password] field.

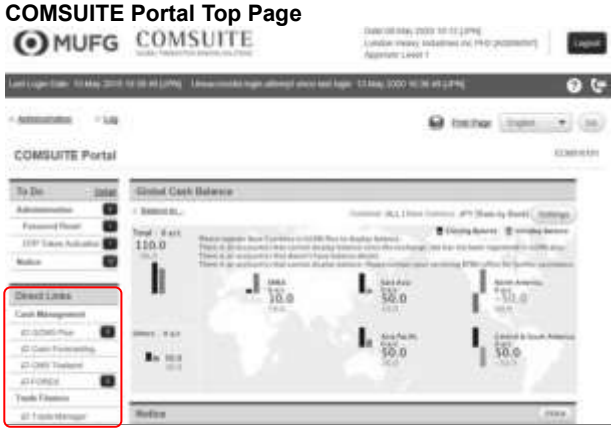
Enter your new password in the [New Password] field and [New Password (confirmation)] field.

See below for the password creation rules.

☞ **1-3 Change Password**

Click Next

COMSUITE Portal Top Page



The COMSUITE Portal Top Page is displayed.

Click a service you want to use from the Direct Links.

■ When logging in for the first time or logging in after resetting password

Enter the COMSUITE URL in your browser's address bar.

URL: https://ebusiness.bk.mufg.jp/login/

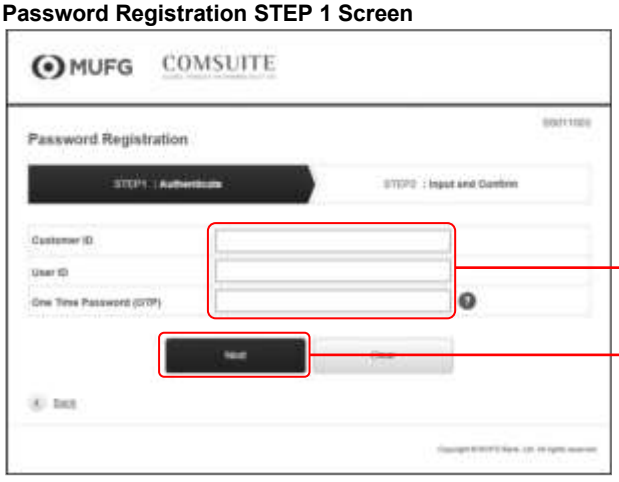
> By adding the login page that is shown after accessing the mentioned URL as a favorite (bookmark), the mark appears as a favorite icon.

Login Screen

The Login screen will be displayed.

Click **Password Registration**

Password Registration STEP 1 Screen

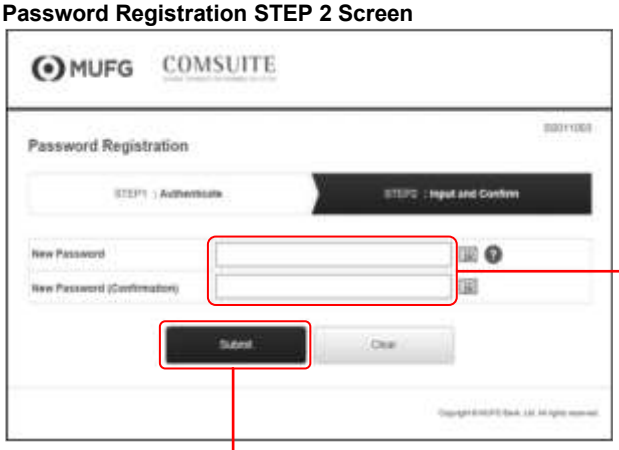


The Password Registration STEP 1 screen is displayed. Please follow the steps below.

Enter your customer ID, user ID, and one-time password (OTP).

Click **Next**

Password Registration STEP 2 Screen



The Password Registration STEP 2 screen is displayed.

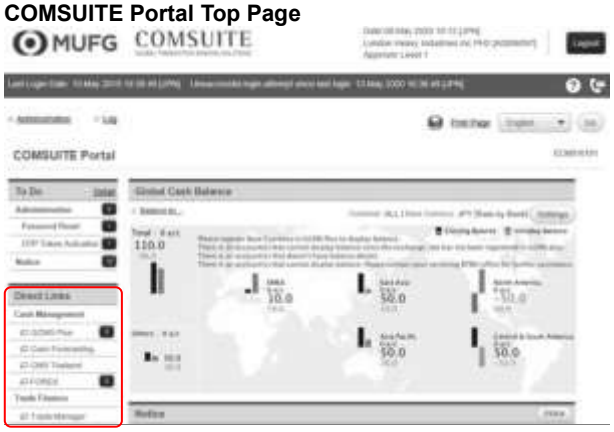
Enter your new password in the [New Password] field and [New Password (confirmation)] fields.

See below for the password creation rules.

☞ **1-3 Change Password**

Click Submit

COMSUITE Portal Top Page



The COMSUITE Portal Top Page is displayed.

Click a service you want to use from the Direct Links.

Attention

When an error message pops up, confirm the following.

- If you have already registered a password, you cannot register a new one. Log in from the Login screen.
- If your OTP token is not activated, you cannot register a password. Confirm with your administrator.
- If you have received a new OTP token to replace an existing one, you need to successfully login using the new one before you can register a password for it. Until then, make sure to keep the existing OTP token so that you can register a password for it.
- If you have entered a wrong customer ID, user ID or one-time password, you cannot register a password. Confirm your entries and try again.

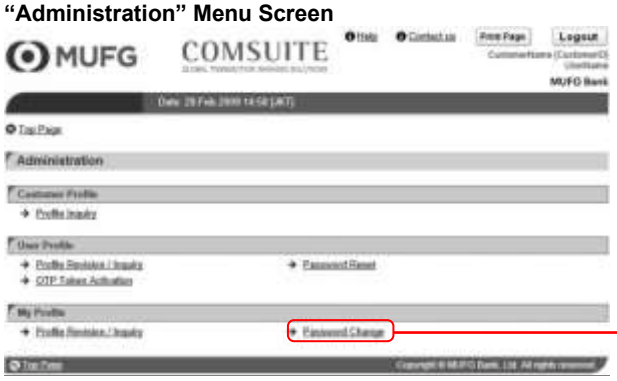
1-3 Change Password

Change your password regularly for security purposes. When setting your password, be sure to take note of its length, contents and expiry date.

Top Page

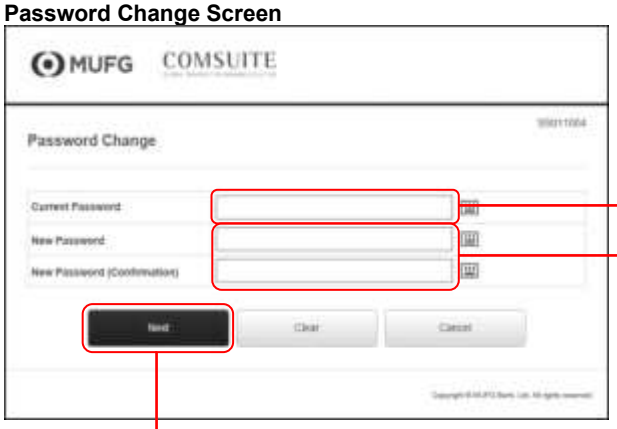
Click "Administration"

"Administration" Menu Screen



Click "Password Change" in "My Profile" sub menu

Password Change Screen



A new window opens to display the Password Change screen.

Enter your old password

Enter your new password

- Your passwords can contain the following three types of characters:
  (i) Numbers 0 through 9
  (ii) Alphabets A through Z and a through z (Note Please ensure that the password contains both uppercase and lowercase characters)
  (iii) Symbols such as ! # $ % & ( ) + - = ? @ _
- Passwords must consist of 8 to 16 characters including all the three types of characters mentioned above.
- The changed password is valid through next 90 days and will be required to change regularly.

Click **Next**

Password Change Screen

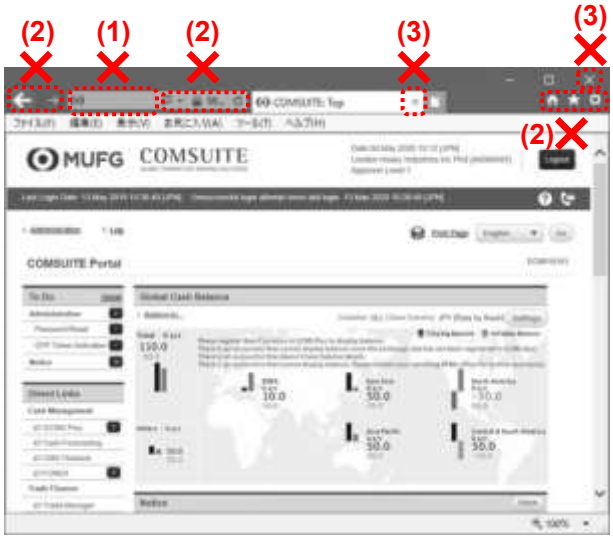
- Passwords are important for personal identification purposes. Be careful not to let others know your password.
- Do not write down your password.
- Change your password regularly.
- Do not reuse your password.
- Avoid using passwords that you use in other places, but use a password that is easy to remember.
- Avoid passwords those are easy for others to guess, or that contain your personal information (i.e. name, telephone number and date of birth).
- Avoid passwords with the same characters in a row, all numbers, or all alphabets.
- Do not share your password with others.
- After your password expired, you cannot use COMSUITE until you change to a new password.
- You can change your password before it expires.

Chapter 2 Security

2-1 Cautions for Smooth Operations

This section describes those operations that may cause problems in the Service.

When using a browser

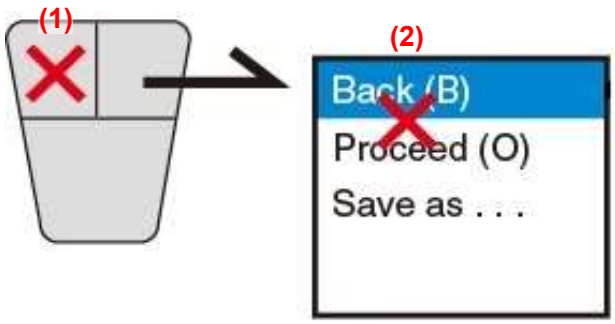


(1) Do not enter a URL address directly in the Address bar.
You cannot jump to any other menu or a site other than COMSUITE Portal by typing addresses directly after logging in.

(2) Do not use the buttons on the browser address bar and toolbar such as [←], [→], [↻], and [X].
They are not supported and may not function normally. Be sure to use only the buttons provided on the COMSUITE Portal pages.

(3) Do not use [X] button in the upper-right corner of tabs and browsers.
By clicking on [X] button, COMSUITE Portal may not close normally. This can result in login failure at the next login attempt.
To close COMSUITE Portal, click on [Logout] button in the upper-right corner of the screen.

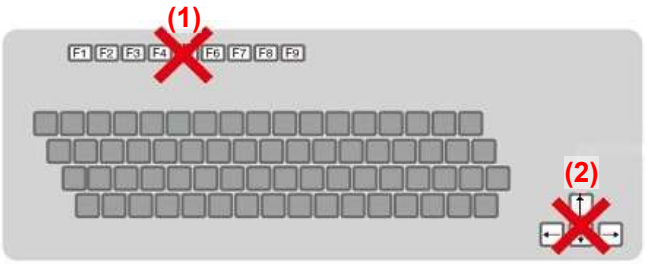
When operating a mouse



(1) Use single-left-click only. (double-click is not supported)
Do not double-click any text link or button.

(2) Do not use "Back" or "Forward" of browsers.
Right-clicking on the browser and selecting the back or forward arrow may bring up an error message or cause irregular operations.
Please be sure to use the text links or buttons on the COMSUITE Portal pages to navigate.

When using a keyboard



(1) Do not use the function key for updating the COMSUITE Portal pages.

(2) Do not use the function keys corresponding to [Forward] button and [Back] button of browsers.

2-2 Security Features

MUFG Bank is committed to providing customers with the safest possible services by minimizing the security risks posed by Internet usage.

■ Internet Security Risks

(1) Security risks associated with use of the Internet include forgery, identity theft and fraud, impersonation, illegal access to your computer system and any other malicious outside attacks.

(2) Your access to our service may be suspended or interrupted due to hardware or software failure and/or any other communication disruptions.

■ MUFG Bank provides the following security features

(1) For your account information, payment instruction data and other communications between your company and MUFG Bank, highly secure SSL (Secure Socket Layer) encryption technology is used to protect your sensitive financial information.

(2) Every user is authenticated by an advanced authentication method which uses one-time password generated by the OTP token (a password used once and expired) in addition to customer ID, user ID and password. For added security, the user is required to enter the transaction authorization code generated by the OTP token, even during approval operations for remittance instructions and applications to revise registered user information.

(3) Your last login time is displayed each time you login, to enable you to check unauthorized access by another person.

(4) For security purposes, your User ID will be locked when consecutive login failures occur a certain times by entering the password, one-time password, or transaction authorization code. You will be locked out until your Administrator completes the password reset procedure. (Please contact your servicing MUFG Bank office for assistance in resetting password if an Administrator is locked and if there is no other Administrator completing the password reset procedure.)

(5) In order to prevent unauthorized operations by someone else while the user leaves his/her seat during login, the time-out facility automatically shuts down the connection after a certain period of inactivity.

(6) Backup organization of the Service is fully ready to provide backup computer and other important facilities in contingency situations.

(7) The information security related technologies we adopt are periodically reviewed and updated to ensure maximum protection.

(8) Servers at Bank are protected by multiple firewalls to prevent unauthorized access via the Internet. We are well prepared to immediately respond to contingency situations.

2-3 Security Management by Customer

The following outlines the recommended security practices for effective security management. You are advised to adopt the following security practices in order to run the operations in a fully secure environment.

Recommended Security Practices

(1) Do not leave your PC unattended once you login. After ending your operation, make sure you logout. When logging out, close all the browser screens. Store the OTP token in a secure place except when you operate your PC.

(2) In Internet Explorer, we recommend not lowering the "Security" settings in "Internet Options" unnecessarily. That is, we recommend setting the "Internet" security level to "medium" or higher, and enabling "Automatic prompting for ActiveX controls" and "Initialize and script ActiveX controls not marked as safe for scripting".

(3) If you share the same PC used for this Service application with any non-user of the Service, please handle the downloaded data with extra caution.

(4) The user activities of the Service for each user can be inquired from the Log menu. It is recommended that you regularly check the activity list and monitor unauthorized access and operations. You can specify the inquiry period to view only the logs you need.

Safekeeping Your User ID, Password and OTP Token

(1) The customer ID, user ID, password and OTP token (including the password generated by your OTP token as well as the response code and transaction authorization code generated by entering the challenge code) for the COMSUITE users must be registered/handled/stored with extra caution, as they are important authentication items.

Handling Your Password

When setting or changing a password, be aware of the following, and do not let other people know your password.

1) Keep passwords confidential.

2) Avoid keeping a paper record of passwords, unless it can be stored securely.

3) Change passwords at regular intervals and avoid reusing or recycling passwords.

4) Select quality passwords with a minimum length of 8 characters which are:

- **Easy to remember;**
- **Not used at any other website;**
- **Not based on anything someone else could easily guess or obtain based on names, telephone numbers, date of birth or any other personal information;**
- **Avoid consecutive identical characters and/or all-numeric or all-alphabetical groups;**
- **Avoid words vulnerable to "dictionary attack" (that is, use words not found in dictionaries);**
- **Avoid sharing your passwords with other users**.

(2) Avoid sharing your user ID and OTP token with other users to ensure that each user's responsibility is clearly defined.

(3) Administrator of your company is requested to keep the privilege level of each user up-to-date by regularly reviewing the assigned privilege level. (Modification/deletion due to personnel transfer, retirement, etc.)

(4) Under no circumstances, shall an MUFG Bank representative ask your password, the password generated by your OTP token, the response code and transaction authorization code generated by entering the challenge code.

(5) If you suspect unauthorized use of your user ID or password, operations you do not remember or other suspicions incidents, contact your MUFG Bank Branch/Office.

(6) Please immediately report any loss of your OTP token to "MUFG Bank Helpdesk for OTP Token Loss" shown in Customer Support.

Protecting Your PC and Information

(1) It is recommended that you install virus-scanning software to protect your PC from virus infection. Please make sure that the scanning software is updated regularly with the latest virus pattern files available to detect new viruses.

(2) Any incoming Internet e-mail from an unknown sender and/or with a suspicious attachment file must be handled with caution.

(3) If your PC is connected to the Internet, please protect your PC from hacker programs by refraining from downloading any software, data or program unless obtained from reliable sources.

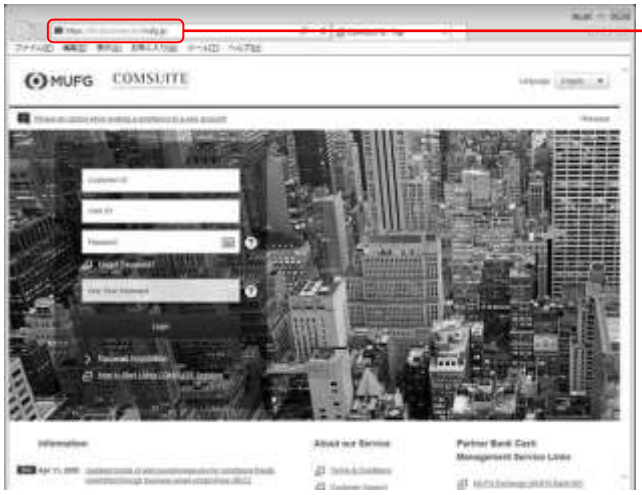
(4) Please make sure to run the password protected screen saver, if available.

(5) Any printed reports must be cleared from the printer immediately.

2-4 Confirmation of Trusted Server

In recent years, there have been crimes that show a fake web page (not from MUFG Bank's legitimate site) and illegally obtain IDs and passwords using a technique referred to as "phishing". To take measures for this, this service provides a method to confirm that the page is sent from MUFG Bank's legitimate server:

2-4-1 Confirm the address shown in the address bar of your browser.



Confirm that the address shown in the address bar begins with "https://e.ebusiness.bk.mufg.jp/**".**

2-4-2 Display and confirm the SSL certificate of the server you access

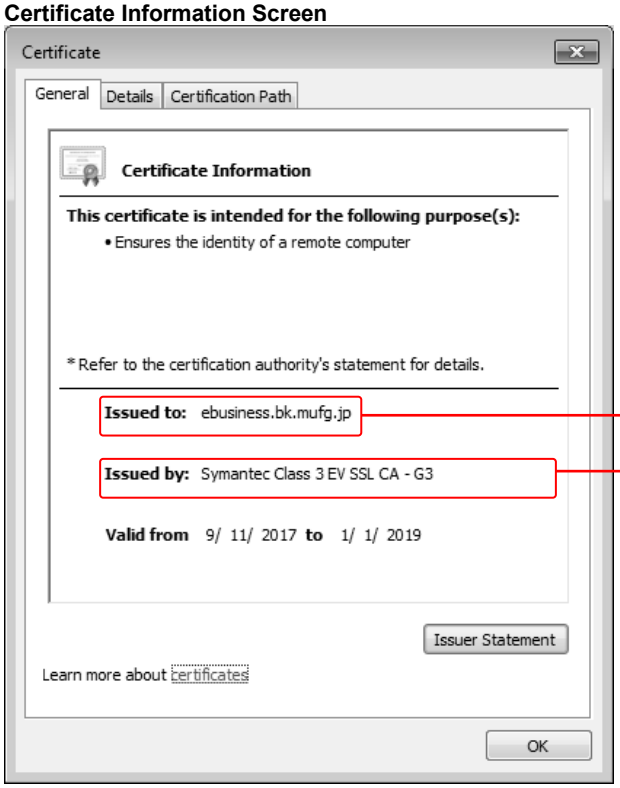
■ In case of Internet Explorer

Login Screen

Confirm that the key icon is shown at the right of the address bar.

Click the key icon.

Certificate Information Screen



Confirm the contents of the certificate.

If the certificate shows the following, it means the COMSUITE legitimate server.

Issued to: ebusiness.bk.mufg.jp

Issued by: Symantec Class 3 EV SSL CA – G3

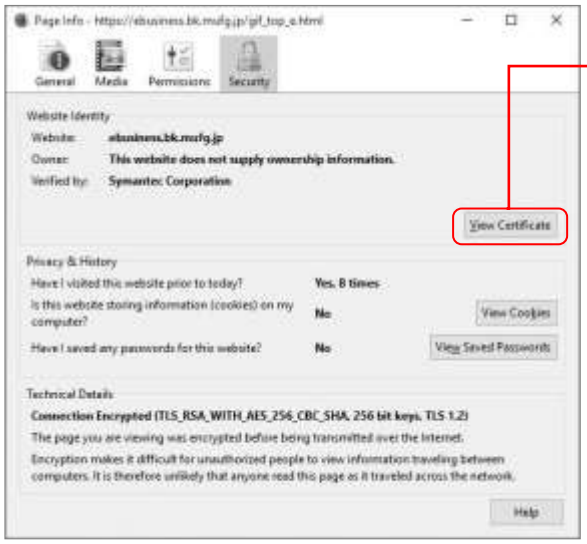
■ In case of Firefox

Login Screen

Confirm that the key icon is shown at the left of the address bar.

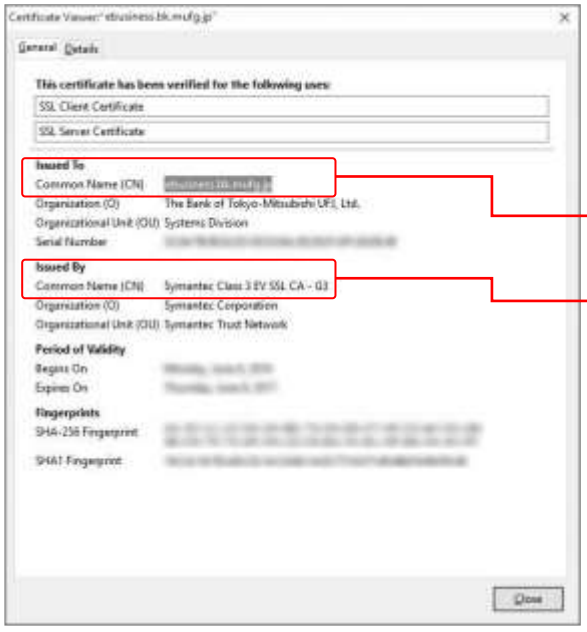
Click the key icon.

Certificate Information Screen



Click “View Certificate”.

Certificate Information Screen



Confirm the contents of the certificate.

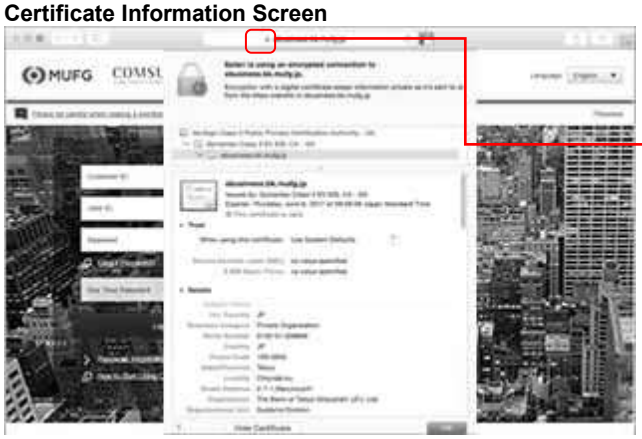
If the certificate shows the following, it means the COMSUITE legitimate server.

Issued To
Common Name (CN):
ebusiness.bk.mufg.jp

Issued By
Common Name (CN):
Symantec Class 3 EV SSL CA - G3

■ In case of Safari

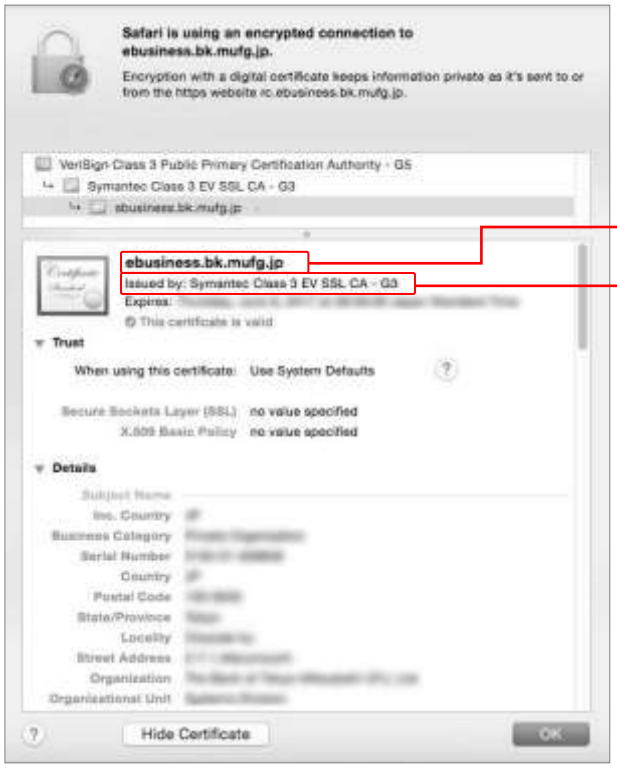
Certificate Information Screen



Confirm that the key icon is shown on the left of the address bar.

Click the key icon.

Certificate Information Screen



Confirm the contents of the certificate.

If the certificate shows the following, it means the COMSUITE legitimate server.

Title: **ebusiness.bk.mufg.jp**

Issued by: **Symantec Class 3 EV SSL CA - G3**

Attention and Trademarks

Attention

- This manual is provided based on the basic agreement of each product (hereinafter referred to as “Basic Agreement”). Provisions in the Basic Agreement are applied to this manual.
- Note that the contents of this manual are subject to change without prior notice. The latest version of this manual is posted at "Customer Support" on the Login screen of "COMSUITE".
- Before using the Service, please be thoroughly familiar with and understand how to use the equipment and software as well as restrictions and other assumptions.
- This manual is property of MUFG Bank, issued to every customer under the Basic Agreement, and shall not be given to any third party.
-

Trademarks

- "COMSUITE" and "GCMS Plus" are registered trademarks or the trademarks of MUFG Bank, Ltd. in Japan and other countries.
- In the text, "Microsoft® Windows® Operating System" is referred to as "Windows".
  Microsoft, Windows and Internet Explorer are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.
- Safari is trademark of Apple Inc, registered in the U.S. and other countries.
- Firefox and the Firefox logo are either registered trademarks or trademarks of Mozilla Foundation U.S.A. in the United States and/or other countries.
- Symantec is a trademark or a registered trademark of Symantec Corporation or its affiliates in the U.S. and other countries.
- Any other company and product names mentioned in this manual are registered trademarks of their respective companies.
- Trademark symbols ™ and ®are not noted in the text of this manual.