

User first-time login to Business Banking:

1. Receive two emails with login credentials.
2. Log in with system-generated username and password.
3. Accept Terms and Conditions.
4. Validate identity (i.e. MFA).
5. Change the username.
6. Change the password.
7. Enjoy the benefits and ease of Business Banking!

Key Points:

- Immediately after the financial institution successfully sets up the business*, the Primary Admin and Secondary Admin(s) **receive two emails: one with the username and one with the password.**
- The login screen for Business Banking is the **same login screen** for Online Banking.
- The username and password are both **system-generated, random values.**
- The business admins **must change the username and password** during initial login.
- The same process applies when a Primary Admin or Secondary Admin sets up a **new business user.**

** exception: if the FI enables user screening, the emails go out after the FI approves the business admin or user via Admin Platform.*

Online Banking First Time Login	Business Banking First Time Login
Enrollment is part of the first-time login	Enrollment happens prior to and outside of the first-time login
User selects username and password	User changes the system-generated username and password
User can edit email/phone numbers for One Time Passcode	Phone call is the only option for One Time Passcode and the number is not editable

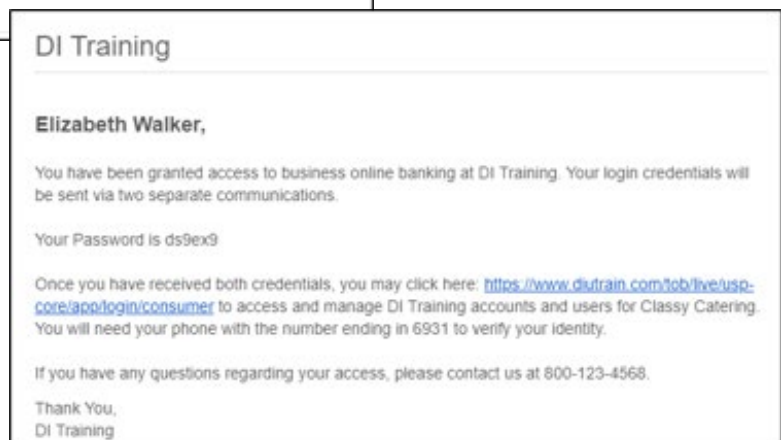
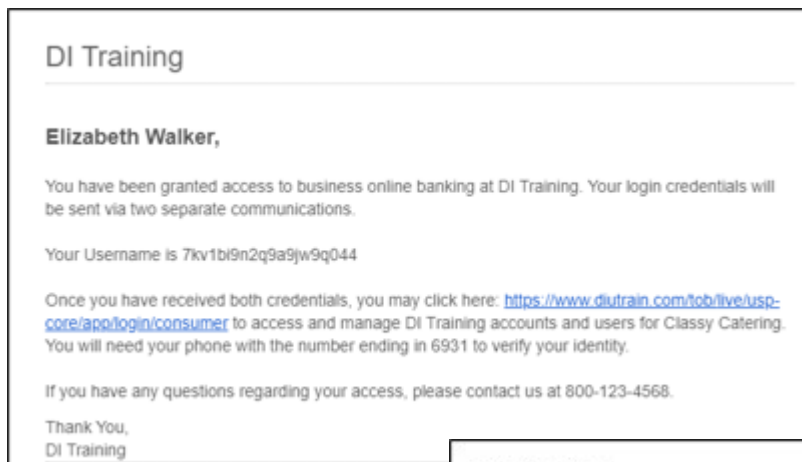
Step 1: Receive emails with login credentials

The system sends two emails to every new user. The From email address is set by your financial institution. The subject line is “You have been granted access to Online Banking”.

Can my financial institution customize these emails?

Only these elements of the email are custom:

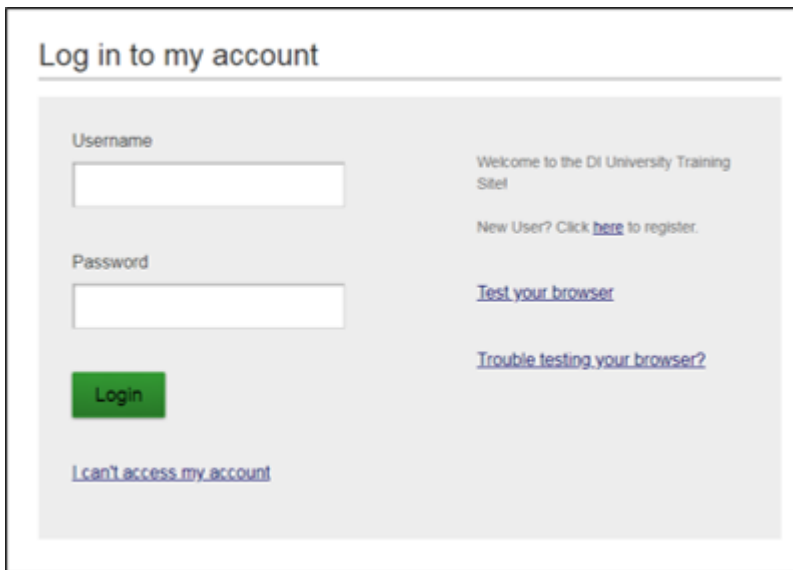
1. “DI Training” = Financial institution name
2. “Elizabeth Walker” = Name of the Business Admin or User
3. “www.diutrain.com...” = URL to your Digital Banking login screen
4. “Classy Catering” = Business name
5. “6931” = Last 4 digits of the person’s phone, used for MFA
6. “800-123-4568” = FI Support number



Step 2: Go to login screen

The login screen for Business Banking is the **same login screen** for Online Banking.

1. Click the link in the email or just go there in a browser.
2. Copy the username from the email and paste into the Username field.
3. Copy the password from the other email and paste into the Password field.



The screenshot shows a login interface with the title "Log in to my account". It features two input fields: "Username" and "Password". Below the "Password" field is a green "Login" button. To the right of the input fields, there is a welcome message: "Welcome to the DI University Training Site!". Below this, it says "New User? Click [here](#) to register." and provides two links: "[Test your browser](#)" and "[Trouble testing your browser?](#)". At the bottom left, there is a link: "[I can't access my account](#)".

Step 3: Accept Terms and Conditions

If enabled by the FI, users must agree to (but is not forced to open) the Terms and Conditions, which displays a PDF doc that the business can download and print.

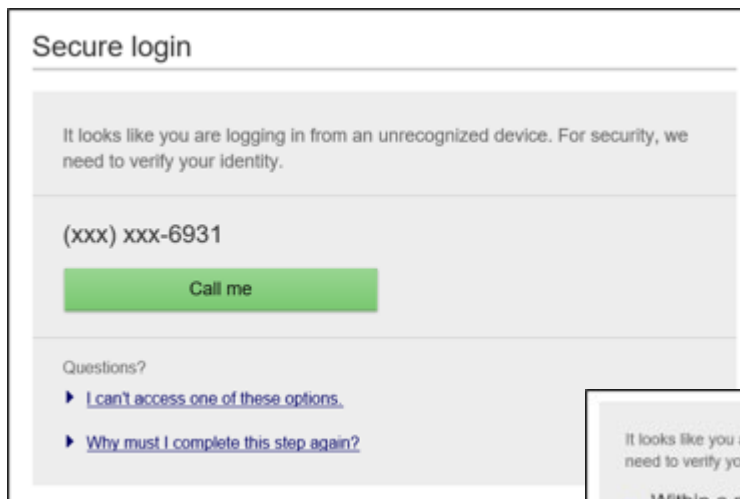


The screenshot shows a screen titled "Terms and conditions". It features a button with a right-pointing arrow and the text "Show the terms and conditions". Below this, it states "You must accept the terms and conditions to continue." At the bottom, there are two buttons: "Accept" (highlighted in blue) and "Decline".

Step 4: Validate identity

The business user must authenticate identity during the initial login, as well as future logins when the computer isn't recognized.

1. Click Call Me.
 - The call goes to the number is associated with the business user, not the phone on the main business profile.
2. Enter the 6-digit code;
 - expires after 10 minutes.
3. Register the device:
 - “Yes, register my **private** device” - bypasses this screen for future logins.
 - “No, this is a **public** device” - presents this screen at the next login.



Secure login

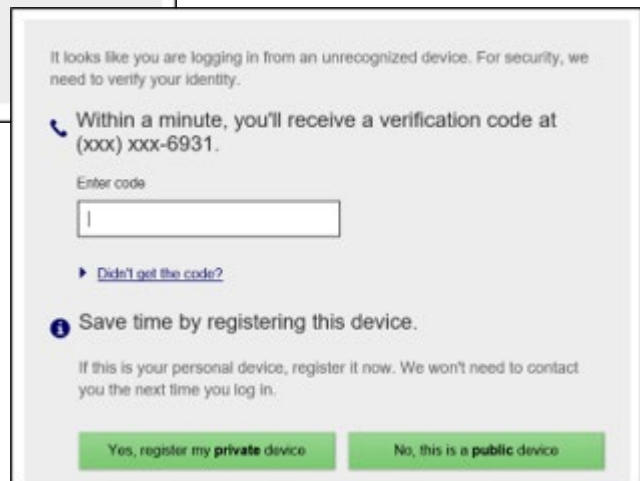
It looks like you are logging in from an unrecognized device. For security, we need to verify your identity.

(xxx) xxx-6931

Call me

Questions?

- ▶ [I can't access one of these options.](#)
- ▶ [Why must I complete this step again?](#)



It looks like you are logging in from an unrecognized device. For security, we need to verify your identity.

Within a minute, you'll receive a verification code at (xxx) xxx-6931.

Enter code

Did't get the code?

i Save time by registering this device.

If this is your personal device, register it now. We won't need to contact you the next time you log in.

Yes, register my **private** device

No, this is a **public** device

Step 5: Change the Temporary Username

The business user must change their username as well during the initial login. Requirements are stated on screen.

Success! You need to change your username.

Create a new Username that will be used for all future logins.

⚠ Create your Username

New Username

▶ Minimum of six characters
▶ Cannot be all numbers

Save

Step 6: Change the Temporary Password

The business user must change their password upon initial login. Requirements are the same as Online Banking and are stated on screen.

Success! You need to change your password.

Temporary password

 [SHOW](#)

New password

 [SHOW](#)

▶ Minimum of six characters
▶ Use a mix of letters, numbers or symbols

Retype password

 [SHOW](#)

▶ Passwords must match

Update password

Tips: The temporary password expires (duration set by the FI).

For future logins, if the computer is not recognized, the user must verify their identity. Options not available at first time login that may show if the user set it up in My Settings:

- **Text Me** button –shows if the user text enables their phone
- Additional **phone number** – shows if the user adds additional numbers
- **Email Me** - shows only if your financial institution allows email MFA
- **Token** – shows only if your financial institution contracts for tokens and the user enters their Credential ID in My Settings
- **Authenticator** – shows if the FI enables Timed OTP and the user has the Google Authenticator app or Microsoft Authenticator app and enables it in My Settings

The image shows a 'Secure login' screen with a message: 'It looks like you are logging in from an unrecognized device. For security, we need to verify your identity.' Below this, there are five verification methods, each with a green button:

- Phone Number 1:** (xxx) xxx-6931. Buttons: Text me, Call me.
- Phone Number 2:** (xxx) xxx-9815. Button: Call me.
- Email:** a*****@gmail.com. Button: Email me.
- Token:** Button: Enter code.
- Authenticator:** Button: Enter code.

