Multi-Factor Authentication FAQ

Updated: February 6, 2025

Contents

Multi-Factor Authentication Introduction

Multi-factor Authentication (MFA) is an authentication method that requires users to provide two or more verification factors to access a resource, such as an application or online account. When you sign into your Blue Yonder training account for the first time on a new device or app (like a web browser), you need more than just your username and password. You will also need a second verification method—referred to as a second 'factor'—to verify your identity.

Smart devices are equipped with a built-in virtual authenticator app that supports the **Time-based One-Time password (TOTP) algorithm**.

- Does your company have a business authenticator app such as DUO or Okta?
    - Review the Step-by-Step Instructions
- Would you prefer to use your smart phones built in MFA application? Users who wish to use their smart phones default MFA app, scanning the QR MFA registration code will open Password Keeper
    - Review the FAQ Section "How do I complete my Multi-Factor Authentication Registration with my iPhone or Android"

Popular authenticator apps include Google Authenticator, Microsoft Authenticator, Okta Verify, Cisco DUO, iOS & Android password keeper, among many others available in app stores.

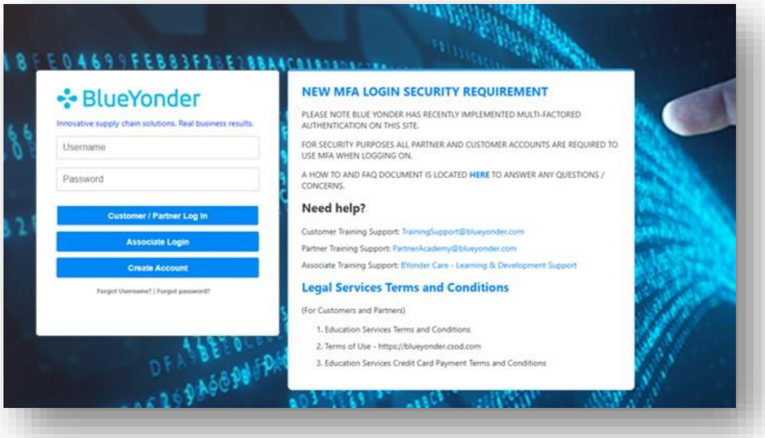
Step by Step Instructions

Log-in with your Blue Yonder training credentials; the multi-factor authentication (MFA) QR code pop-up window will display, and you will be prompted to register a smart device.

1. **Recommendation** is to add to your **existing** Time-based One Time Password (TOTP) app (e.g., DUO, Okta, AuthO, PingID, etc.)
2. Begin by opening your company's existing Time-based One Time Password (TOTP) app and **then scan the QR code** to register your device
3. Create a new account in your Time-based One Time Password (TOTP) app to generate a unique code specifically for accessing the SKY Portal.
4. Add details, e.g., 'Blue Yonder Training' (if applicable)
5. Next enter your Blue Yonder Training user ID and password (if applicable)
6. Locate the MFA Security Key Code that displays during the MFA registration process

7. Make a note of where you've saved the Blue Yonder Training MFA security key code, as you'll need to enter a refreshed MFA security code every 24 hours

Log-on screen view



BlueYonder
Innovative supply chain solutions. Real business results.
Username
Password
Customer / Partner Log In
Associate Login
Create Account
Forgot Username? | Forgot password?

NEW MFA LOGIN SECURITY REQUIREMENT

PLEASE NOTE BLUE YONDER HAS RECENTLY IMPLEMENTED MULTI-FACTORED AUTHENTICATION ON THIS SITE.

FOR SECURITY PURPOSES ALL PARTNER AND CUSTOMER ACCOUNTS ARE REQUIRED TO USE MFA WHEN LOGGING ON.

A HOW TO AND FAQ DOCUMENT IS LOCATED HERE TO ANSWER ANY QUESTIONS / CONCERNS.

Need help?

Customer Training Support: TrainingSupport@blueyonder.com

Partner Training Support: PartnerAcademy@blueyonder.com

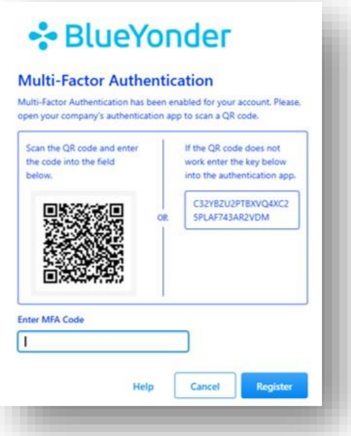
Associate Training Support: BYonder Care - Learning & Development Support

Legal Services Terms and Conditions

(For Customers and Partners)

1. Education Services Terms and Conditions
2. Terms of Use - https://blueyonder.csod.com
3. Education Services Credit Card Payment Terms and Conditions

MFA Prompt view



Multi-Factor Authentication

Multi-Factor Authentication has been enabled for your account. Please open your company's authentication app to scan a QR code.

Scan the QR code and enter the code into the field below.

If the QR code does not work enter the key below into the authentication app.

C32YBZU2PTBXVQ4XC2
5PLAF743AR2VDM

Enter MFA Code

Once you have registered your smart device, any future log-in sessions will require you to input the MFA security key code. The MFA security key code will be active for a 24-hour period.

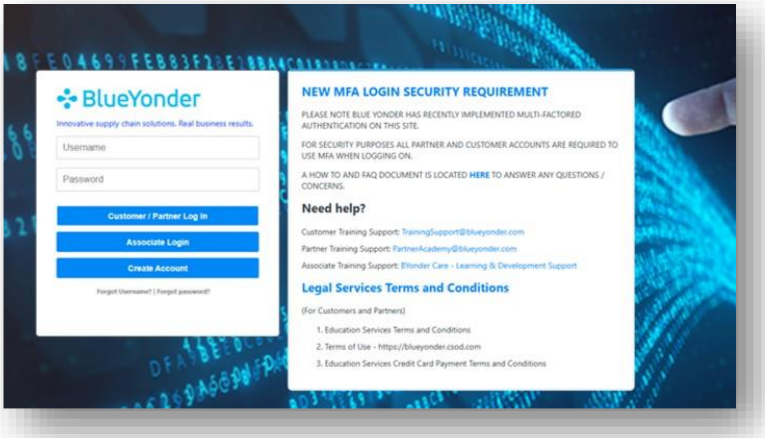
FAQ

How do I complete the Multi-Factor Authentication Registration with my iPhone or Android's default MFA app (e.g. password keeper)

Log-in with your Blue Yonder training credentials, the multi-factor authentication (MFA) pop-up window will display, and you will be prompted to register a smart device.

1. **Begin by scanning the QR Code**, the QR code link will take you to your smart device's default built in multi-factor authenticator (e.g. Password management in iOS & Android)
2. Click on the add icon '**+**' located in the upper right corner
3. Add the details, e.g., 'Blue Yonder Training'
4. Enter your Credentials, (e.g., your Blue Yonder Training user ID and password)
5. Enter the MFA Security Key Code to complete the MFA registration process
6. **Caution:** Make a note of where you've saved the Blue Yonder Training MFA security key code, as you'll need to enter the MFA security key code for future log-in sessions.
    - To locate easily, use your smart phone's "search feature" and search for 'password'

Log-on screen view



BlueYonder

Innovative supply chain solutions. Real business results.

Username

Password

Customer / Partner Log In

Associate Login

Create Account

Forgot Username? | Forgot password?

NEW MFA LOGIN SECURITY REQUIREMENT

PLEASE NOTE BLUE YONDER HAS RECENTLY IMPLEMENTED MULTI-FACTORED AUTHENTICATION ON THIS SITE.

FOR SECURITY PURPOSES ALL PARTNER AND CUSTOMER ACCOUNTS ARE REQUIRED TO USE MFA WHEN LOGGING ON.

A HOW TO AND FAQ DOCUMENT IS LOCATED HERE TO ANSWER ANY QUESTIONS / CONCERNS.

Need help?

Customer Training Support: TrainingSupport@blueyonder.com

Partner Training Support: PartnerAcademy@blueyonder.com

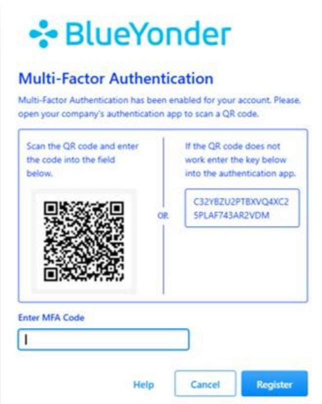
Associate Training Support: BYonder Care - Learning & Development Support

Legal Services Terms and Conditions

(For Customers and Partners)

1. Education Services Terms and Conditions
2. Terms of Use - https://blueyonder.csod.com
3. Education Services Credit Card Payment Terms and Conditions

MFA Prompt view



BlueYonder

Multi-Factor Authentication

Multi-Factor Authentication has been enabled for your account. Please. open your company's authentication app to scan a QR code.

Scan the QR code and enter the code into the field below.

OR

If the QR code does not work enter the key below into the authentication app.

C32YBZU2PTBXVQ4XC2
5PLAF743AR2VDM

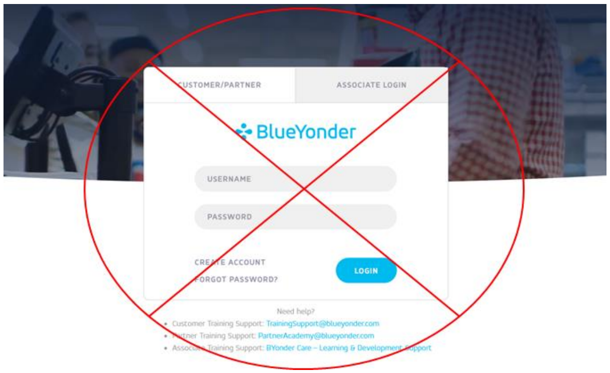
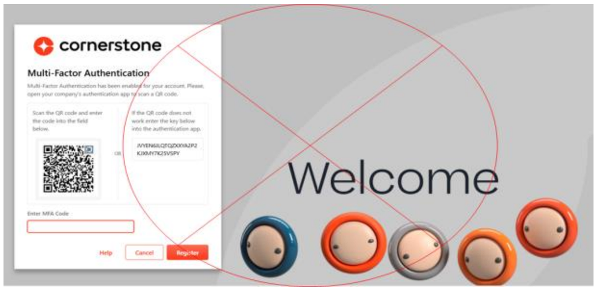
Enter MFA Code

Help | Cancel | Register

Once you have registered your smart device, any future log-in sessions will require you to add the MFA security key code. The MFA security key code will be active for a 24-hour period. e.g., required to enter MFA code once per day.

Why does my Log-in Screen and MFA prompt look different than what is displayed in the Step-by-Step Instructions.

The Blue Yonder training link that you have is outdated, be sure to update your bookmark or create a bookmark https://blueyonder.csod.com/

 CUSTOMER/PARTNER ASSOCIATE LOGIN BlueYonder USERNAME PASSWORD CREATE ACCOUNT FORGOT PASSWORD? LOGIN Need help? • Customer Training Support: TrainingSupport@blueyonder.com • Partner Training Support: PartnerAcademy@blueyonder.com • Associate Training Support: BYonder Care – Learning & Development Support	 cornerstone Multi-Factor Authentication Multi-Factor Authentication has been enabled for your account. Please, open your company's authentication app to scan a QR code. Scan the QR code and enter the code into the field below. OR If the QR code does not work enter the key below into the authentication app. JVYEN6JLQTQZXXYA2P2 KJXMY7K25VSPY Enter MFA Code Help | Cancel | Register Welcome

Why does the Multi-Factor Authentication (MFA) Registration Process require 3 security key steps?

When a user has a ***temporary*** password, the MFA registration process initially requires three MFA steps. The MFA Registration with a temporary password is a 3-process activity. Registration of your smart device is a one-time inconvenience.

- **Initial Log-in**: Enter your credentials, you will be prompted to register your smart device.
    - **Recommendation** is to add to your *existing* Time-based One Time Password (TOTP) app (e.g., DUO, Okta, AuthO, PingID, etc)
    - Begin by opening your company's existing Time-based One Time Password (TOTP) app and then scan the QR code to **register** your device
    - Click on the add icon '**+**' located in the upper right corner
    - Add the details, such as "Blue Yonder's SKY portal"
    - Enter your Credentials, e.g., your Blue Yonder SKY portal user ID and password
    - **Locate the MFA Security Key Code** that displays during the MFA registration process
    - Make a note of where you've saved this MFA security code, as you'll need to update it every 24 hours
- **Temporary Credentials**: Enter your temporary credentials. You will be prompted for the MFA key a second time
- **Update Password**: You'll be prompted to update your password
- **Updated Credentials**: Enter your updated credentials (new password) and the MFA security key code for the 3rd time. The MFA token will then be valid for a 24-hour period

This step-by-step approach ensures the user's device is securely registered and their password is updated, while maintaining the validity of the MFA token for 24 hours within the same session.

Why does the Multi-Factor Authentication (MFA) Registration process require 2 security key steps?

When a user has an **existing** password, the MFA registration process requires two MFA steps. Registration of the smart device is a one-time inconvenience.

- Enter your Blue Yonder training credentials; you will be prompted to register your smart device.
    1. Register Device: ***Recommendation*** is to add to your *existing* TOTP device (e.g., DUO, Okta, AuthO, PingID, etc.)
    2. Begin by opening your company's existing TOTP authenticator and scan the QR code to **register** your device
    3. Click on the add icon '**+**' in the upper right corner

4. Add the details, e.g., "Blue Yonder's SKY portal"
5. Enter your Blue Yonder training credentials: Enter your user ID and password.
6. **Locate the MFA Security Key Code** that displays during the MFA registration process
7. Enter your updated credentials, enter the MFA security key code for the 2nd time.
8. The MFA security key code will then be valid for a 24-hour period

This step-by-step approach ensures the user's device is securely registered and their password is updated, while maintaining the validity of the MFA token for 24 hours within the same session.

Why do I have to reset my password?

Resetting your password as part of the new Multi-Factor Authentication (MFA) process is essential for boosting the security of your account. Here are a few key reasons:

- **Enhanced Security**: By resetting your password, you ensure that your account is protected by a strong, unique password that complies with the latest security standards. This reduces the risk of unauthorized access.
- **Compliance with New Policies**: The new MFA process and password requirements aim to safeguard sensitive information. Compliance with these policies helps maintain the security and integrity of the system for everyone.
- **Prevention of Password Fatigue**: Regularly updating passwords prevents the reuse of old passwords across multiple accounts, which can be a security risk if one of those accounts gets compromised.
- **Protection Against Cyber Threats**: Cyber threats are constantly evolving. By updating your password, you stay one step ahead of potential attackers who might try to exploit older, weaker passwords.

How do I unregister my MFA Device or who do I contact for additional support?

Please contact our training support team for assistance.

- **Customer** Training Support: TrainingSupport@blueyonder.com
- **Partner** Training Support: PartnerAcademy@blueyonder.com