

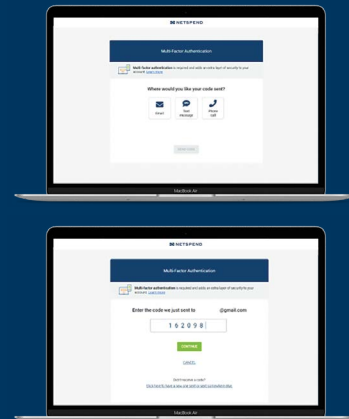
MULTI-FACTOR AUTHENTICATION AS A SECURITY ENHANCEMENT FOR NETSPEND-HOSTED APPLICATIONS

Multi Factor Authentication (MFA) is a form of strong authentication that leverages more than one factor (i.e. password alone) to authenticate a user to a system. Users will need to validate the device they are using to access any Netspend-hosted application by entering a code that has been sent (at each user's option) via SMS text to their mobile device, to their email, or via voice-call to their mobile device or landline.

Things You Need to Know

This step-by-step flow will give you some basic information on how your user experience will work:

- 1 You log in to application**
When you enter your credentials in the application, the system will determine if MFA is required for that login.
- 2 You select method for validation code**
You will select where Netspend should send the validation code (via SMS text to mobile device, email, or voice-call to mobile device or landline).
- 3 You enter the validation code**
After you receive the validation code via your selected method, you will enter that code where indicated on the login flow.
- 4 You are logged in to application**
Once successful in providing the validation code, you will be directed to the application home page as normal.



You will have **5** attempts to log in using MFA before you are locked out of the application. We recommend that your mobile device or web browser operating system is up-to-date for the most optimized login experience.

For assistance or to resolve any login issues, please contact your company administrator or Client Services at **1-888-414-8885 / clientcommunications@netspend.com**.

You will be required to verify with MFA every time it has been 24 hours since your last MFA verification. MFA is also required when you sign in from a new device or web browser.

For questions, contact your company administrator or Client Services at **1-888-414-8885 / clientcommunications@netspend.com**.

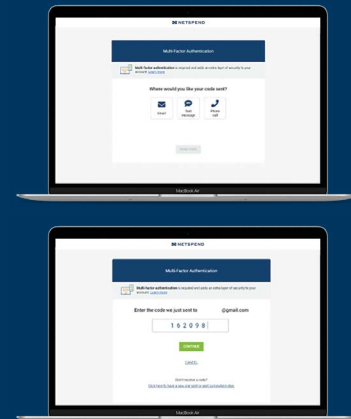
MULTI-FACTOR AUTHENTICATION AS A SECURITY ENHANCEMENT FOR NETSPEND-HOSTED APPLICATIONS

Multi Factor Authentication (MFA) is a form of strong authentication that leverages more than one factor (i.e. password alone) to authenticate a user to a system. Users will need to validate the device they are using to access any Netspend-hosted application by entering a code that has been sent (at each user's option) via SMS text to their mobile device, to their email, or via voice-call to their mobile device or landline.

Things You Need to Know

This step-by-step flow will give you some basic information on how your user experience will work:

- 1 You log in to application**
When you enter your credentials in the application, the system will determine if MFA is required for that login.
- 2 You select method for validation code**
You will select where Netspend should send the validation code (via SMS text to mobile device, email, or voice-call to mobile device or landline).
- 3 You enter the validation code**
After you receive the validation code via your selected method, you will enter that code where indicated on the login flow.
- 4 You are logged in to application**
Once successful in providing the validation code, you will be directed to the application home page as normal.



You will have **5** attempts to log in using MFA before you are locked out of the application. We recommend that your mobile device or web browser operating system is up-to-date for the most optimized login experience.

For assistance or to resolve any login issues, please contact your company administrator or Client Services at **1-888-414-8885 / clientcommunications@netspend.com**.

You will be required to verify with MFA every time it has been 24 hours since your last MFA verification. MFA is also required when you sign in from a new device or web browser.

For questions, contact your company administrator or Client Services at **1-888-414-8885 / clientcommunications@netspend.com**.

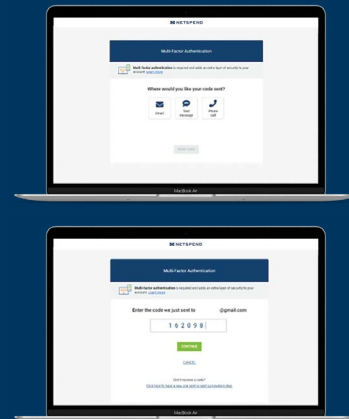
MULTI-FACTOR AUTHENTICATION AS A SECURITY ENHANCEMENT FOR NETSPEND-HOSTED APPLICATIONS

Multi Factor Authentication (MFA) is a form of strong authentication that leverages more than one factor (i.e. password alone) to authenticate a user to a system. Users will need to validate the device they are using to access any Netspend-hosted application by entering a code that has been sent (at each user's option) via SMS text to their mobile device, to their email, or via voice-call to their mobile device or landline.

Things You Need to Know

This step-by-step flow will give you some basic information on how your user experience will work:

- 1 You log in to application**
When you enter your credentials in the application, the system will determine if MFA is required for that login.
- 2 You select method for validation code**
You will select where Netspend should send the validation code (via SMS text to mobile device, email, or voice-call to mobile device or landline).
- 3 You enter the validation code**
After you receive the validation code via your selected method, you will enter that code where indicated on the login flow.
- 4 You are logged in to application**
Once successful in providing the validation code, you will be directed to the application home page as normal.



You will have **5** attempts to log in using MFA before you are locked out of the application. We recommend that your mobile device or web browser operating system is up-to-date for the most optimized login experience.

For assistance or to resolve any login issues, please contact your company administrator or Client Services at **1-888-414-8885 / clientcommunications@netspend.com**.

You will be required to verify with MFA every time it has been 24 hours since your last MFA verification. MFA is also required when you sign in from a new device or web browser.

For questions, contact your company administrator or Client Services at **1-888-414-8885 / clientcommunications@netspend.com**.

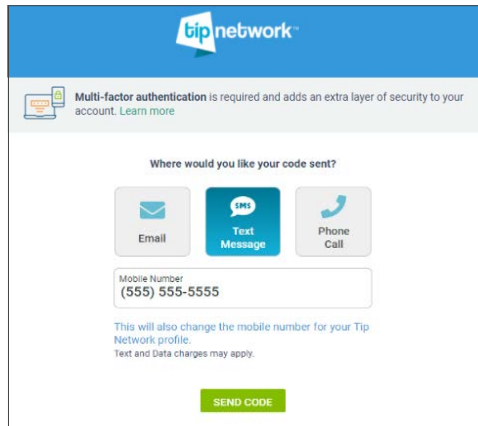
Multi-Factor Authentication as a Security Enhancement for Netspend-Hosted Applications

Multi-Factor Authentication (MFA) is an enhanced layer of security that leverages more than one factor (i.e. a one time code in addition to password alone) to verify program or system access. Users will need to validate the device they are using to access any Netspend-hosted application by entering a code that has been sent (at each user's option) via SMS text to their mobile device, to their email, or via voice-call to their mobile device or landline.

Things You Need to Know

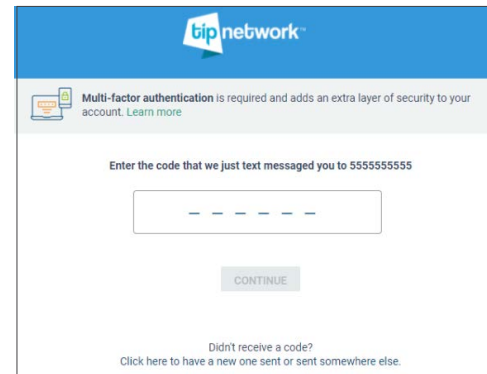
This step-by-step flow will give you some basic information on how your user experience will work:

- 1 You log in to application**
When you enter your credentials in the application, the system will determine if MFA is required for that login.
- 2 You select method for validation code**
You will select where Netspend should send the validation code (via SMS text to mobile device, email, or voice-call to mobile device or landline).



The screenshot shows the Tip Network login interface. At the top, it says "Multi-factor authentication is required and adds an extra layer of security to your account. Learn more". Below this, it asks "Where would you like your code sent?" and provides three options: Email, Text Message (selected), and Phone Call. A mobile number field contains "(555) 555-5555". A note below the field states: "This will also change the mobile number for your Tip Network profile. Text and Data charges may apply." At the bottom, there is a green "SEND CODE" button.

- 3 You enter the validation code**
After you receive the validation code via your selected method, you will enter that code where indicated on the login flow.



The screenshot shows the Tip Network login interface. At the top, it says "Multi-factor authentication is required and adds an extra layer of security to your account. Learn more". Below this, it asks "Enter the code that we just text messaged you to 5555555555". There is a text input field with a dashed line indicating where to enter the code. Below the field is a "CONTINUE" button. At the bottom, it says "Didn't receive a code? Click here to have a new one sent or sent somewhere else."

- 4 You are logged in to application**
Once successful in providing the validation code, you will be directed to the application home page as normal.

You will have **5** attempts to log in using MFA before you are locked out of the application. We recommend that your mobile device or web browser operating system is up-to-date for the most optimized login experience. Contact support@tipnetwork.com for assistance to resolve any login issues.

If you are an employee, you will be prompted every 45 days to maintain secure access to the Tip Network application. If you are a manager, you will be prompted every 24 hours to maintain secure access. Please know that MFA will be required again if you sign in from a new device or web browser.

For questions, contact support@tipnetwork.com.