

# Mastercard **Connect**

## Frequently Asked Questions

### How do I sign up for Mastercard Connect?

On the Mastercard Connect landing page, navigate to the Sign Up link in the left panel. There you'll find an easy three-step process to sign up for Mastercard Connect.

### Which browser can I use for Mastercard Connect?

Mastercard recommends the following browsers for optimum performance:

- Internet Explorer (version 9, 10 & 11 and does not support version 8) - Chrome (version 45+) - Firefox (version 39+) - Safari (Mac only, version 9+)

**Note:** Some applications within Mastercard Connect may require specific browsers. In addition, Mastercard recommends the following optional browser plug-ins:

- Adobe Flash® 9 or higher
- Adobe Reader® 8 or higher

These Plug-ins may be needed when viewing videos or downloading manuals.

### What is the cost of Mastercard Connect?

Mastercard Connect is free of charge. Customers may incur costs for certain applications within Mastercard Connect.

### Is Mastercard Connect secure?

Mastercard Connect is designed with several advanced security features. The website's robust environment includes operational integrity and security.

### Is the data being transmitted through Mastercard Connect secure?

Traffic flowing between the client browser and the Mastercard Connect environment is protected using Secure Sockets Layer (SSL) encryption technology.

### Can I obtain access across my company for Mastercard Connect instead of each individual employee?

No. Mastercard Connect access is user driven only. Each individual user must have his or her own ID to use the site.

## How does a user authenticate to Mastercard Connect?

Mastercard uses two levels of authentication: password only and password plus SecurID token number, which is known as “two-factor authentication.”

During the Mastercard Connect sign-up process, users choose a password that they use to sign in. If a user requests a Mastercard Connect application that allows him or her to access sensitive, payment card data (for example, primary account numbers), the two-factor authentication will be required. Security and Business Administrators are assigned a two-factor authentication type when they register for Mastercard Connect.

## What types of two-factor authentication does Mastercard support?

The primary, two-factor authentication type that Mastercard offers is RSA's SecurID Software Token. To learn more about installing and using software token authentication, please visit the Software Token Installation and User Guide on the Mastercard Connect sign-in page. Organizations technically unable to use software authentication may still use RSA's SecurID hardware tokens.

## Is there a fee associated with using two-factor authentication?

Software tokens used for two-factor authentication does not have a fee associated. Organizations that elect to use hardware tokens will pay a quarterly fee per token.

## What do I do if I forget my password or PIN?

If you forget your password or PIN, click the Forgot Password/PIN link, enter your user ID, and answer your verification questions. A temporary password will be emailed to you if you are a password user. You can reset your PIN if you are a PIN user.

## My SecurID has been lost or damaged. How do I replace it?

If you need to replace your SecurID, navigate to the Replace SecurID® link in the left panel. Once there, enter your user ID, answer your verification questions, review or change your mailing address, and submit your request for a new token.

## Can multiple users share a single account?

No. Each user must have his or her own account to use Mastercard Connect. Whether you are a password user or a SecurID user, you must use your individual account to access Mastercard Connect. Sharing authentication credentials or otherwise using SecurIDs outside the Mastercard security policy may result in the revocation of the SecurID and termination of access to Mastercard Connect.

## What happens if I don't log in to Mastercard Connect regularly?

You risk being considered an Inactive User and your user account could be deleted from the system.