



LastPass 

Using LastPass

Why Use LastPass?

- Great password management is impossible w/o a great tool
- Auto-fill (hands-free login) will save you approximately 1 hour per month
- You will never feel the frustration of a forgotten password again
- Fewer calls to the helpdesk
- Better security for company tools and data

Why Use LastPass?

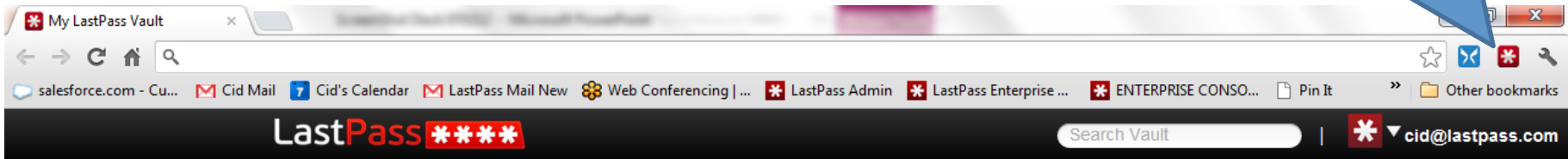
- Welcome email walks you thru downloading LastPass and creating your account
- For your Master Password, consider using a passphrase (I like 2 go 2 the beach!) instead of password
- Your Master Password is the last password you will have to remember
- Login to LastPass
- Stores sites as you go (no personal data please)
- Handsfree login after that!

Getting Started with LastPass Video Tutorial:

https://www.youtube.com/watch?v=tx8tnVX8z7w&feature=player_embedded

Your LastPassVault (accessed via the Plug-in or from www.lastpass.com)

The LastPass Plug-in
Red Icon = Logged-on
Gray = Logged-off



Collapse and Expand
All Folders

Actions

- Enterprise Console
- Manage Shared Folders
- Settings
- Add Site
- Add Secure Note
- Create Group
- User Manual
- Security Check

Help spread the word

Do you like LastPass?

Tell a friend!

GET FREE PREMIUM

'Group'

Vault | Form Fill Profiles | Identities | Shares | Video

Name	Actions
Customer Folder	
Secure Notes	
Shared-Sales	
Work Accounts	
Amazon Cid LastPass Acct	[Edit] [Launch] [Delete]
chat.lastpass.com Cid	[Edit] [Launch] [Delete]
Deutsche Telekom encrypted ma	[Edit] [Launch] [Delete]
dropbox.com	[Edit] [Launch] [Delete]
eva.virginia.gov	[Edit] [Launch] [Delete]
Google Adwords	[Edit] [Launch] [Delete]
Google Docs	[Edit] [Launch] [Delete]
HEP-connect trial login	[Edit] [Launch] [Delete]
Lastpass Calendar	[Edit] [Launch] [Delete]
LastPass Mail Google Gmail	[Edit] [Launch] [Delete]

URL: https://www.amazon.com/ap/signin?_encoding=UTF8&openid.assor

Name: Amazon Cid LastPass Acct | Group: Work Accounts

Username: cid@lastpass.com | Password: [Show] [History]

Notes:

Favorite | Never AutoFill | Require Password Reprompt | AutoLogin

Delete | Share | Save | Cancel

• Edit
• Launch
• Delete

Logging in and Saving Existing Credentials

Step 1: Browse to the desired site and log in.

Step 2: Note the prompt in the notification bar. Hit 'save site'.

Step 3: Fill out the 'edit' form with your preferences for the site.

- If the site has only 1 related login, then you might want to select 'auto-login'**
- If the site is particularly sensitive (financial services), then you might want to select 'Require Password Reprompt'.**
- Assign to a group to keep your vault well-organized.**

****Please do not store personal data to your Enterprise vault.
Instead, create a separate personal account and link the two.**

User Manual: <http://helpdesk.lastpass.com/password-manager-basics/adding-a-site/>

Link a personal acct: <http://enterprise.lastpass.com/getting-started/link-personal-accounts/>

Saving Existing Credentials

www.linkedin.com/home

Should LastPass remember this password? Save Site Never... Not Now

Account Type: Business Plus

Home Profile Contacts Groups Jobs Inbox Companies News More

Thinking of college in the Metro D.C. Area? University of Phoenix® has 5 local locations.

Share an update

Attach a link

Share

LinkedIn Today: See all Top Headlines for You

With Google Now, Android Puts Apple's Siri To Shame

Augmented Reality Shopping Coming Soon

No, the iPhone Isn't the Most Disruptive Product in History

People You May Know *updated*

- Suzanne Cosgrove McGovern, Manager, Sustainable Development and [Connect](#)
- linda scott, accounts payable at Acme Packet [Connect](#)
- Jeff Herr, VP, Digital at California Newspapers Partnership [Connect](#)

See more »

Cid, Follow Hewlett-Packard

Cid Ferrara Hewlett-Packard

Keep up with interesting, relevant updates about Hewlett-Packard.

All Updates • LastPass Coworkers • Connections • More ▾

Recent • Top • 🔍

Seth Marlowe is now connected to **Edward Tillman**, Principal Agent, The Tillman Agency at Nationwide Insurance

Send a message • 1 minute ago

Save All Entered Data

'Save all entered data (SAED)' can be used for storing non-standard and troublesome logins such as multi-page login screens or floating screens. Rather than saving just the login data, 'SAED' allows you to capture and store every field on the page.

Step 1: Browse to the desired site and enter username and password.

Step 2: Prior to hitting the submit button, go to the plug-in and select 'SAED'.

Step 3: Fill out the 'edit' form with your preferences for the site and hit 'save'.

User Manual: <http://helpdesk.lastpass.com/login-problems/>

Visiting a Saved Site – “Hands-free Login”

Step 1: Browse to the desired site as you normally would: by typing in the URL, or by clicking on the bookmark.

Step 2: When you arrive at the login screen LastPass will automatically fill in the username and password fields. If you have ‘auto-fill’ set, then simply hit the submit button to login to the site. If you have multiple accounts, then select the right account from the auto-fill dropdown options.

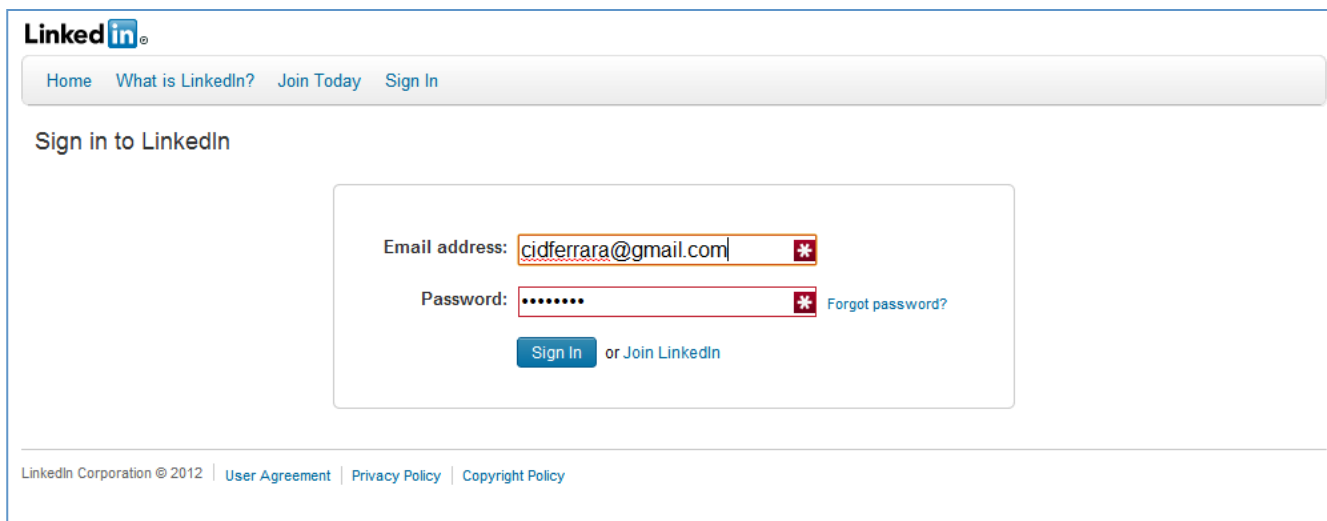
If you have ‘auto-login’ set, then LastPass will automatically hit the submit button for you.

Troubleshooting:


- (1) If LastPass does not take action, first check to make sure that the LastPass icon in the browser bar is red. Red = logged-on. Gray = logged-off.**
- (2) If the icon is red, then look for the ‘auto-fill’ button in the notification bar. Click it to fill in the username and password.**
- (3) If you are still experiencing problems, then this may be a non-standard login page. In this case, try saving the site again using ‘Save all Entered Data’.**

LastPass: The LAST password you’ll have to remember!

Logging in with Stored Credentials (Auto-Fill)



The screenshot shows the LinkedIn login page. At the top left is the LinkedIn logo. Below it is a navigation bar with links for Home, What is LinkedIn?, Join Today, and Sign In. The main heading is "Sign in to LinkedIn". The login form contains two input fields: "Email address" with the value "cidferrara@gmail.com" and "Password" with masked characters "*****". Both fields have a red asterisk icon on the right. Below the password field is a "Forgot password?" link. At the bottom of the form are two buttons: "Sign In" and "or Join LinkedIn". The footer contains the text "LinkedIn Corporation © 2012 | User Agreement | Privacy Policy | Copyright Policy".

LinkedIn 

[Home](#) [What is LinkedIn?](#) [Join Today](#) [Sign In](#)

Sign in to LinkedIn

Email address: *

Password: * [Forgot password?](#)

[Sign In](#) or [Join LinkedIn](#)

LinkedIn Corporation © 2012 | [User Agreement](#) | [Privacy Policy](#) | [Copyright Policy](#)

Updating Existing Login Credentials

Step 1: Browse to the site in question. Sign in to your account on the Website. Find and select the 'update password' option.

Step 2: As you are filling out the form and you place your cursor in the password field, note the notification bar at the top of the window. Select 'Generate password'. The password will automatically be copied into the password fields.

Step 3: Save/submit the change. Note the notification bar. Select 'confirm'.

The password has been updated and safely stored in your vault.

User Manual:

[http://helpdesk.lastpass.com/password-manager-basics/generating-a-password/
changing-the-password-for-a-stored-site-to-a-generated-password/](http://helpdesk.lastpass.com/password-manager-basics/generating-a-password/changing-the-password-for-a-stored-site-to-a-generated-password/)

Updating Passwords Using 'Generate Password' Tool

The image shows a composite screenshot of the LastPass web interface. On the left, a 'Change your password' dialog box is open, containing instructions and input fields for 'Old password', 'New password', and 'Confirm new password'. A 'Change password' button is visible. In the center, a 'Tools' menu is open, with 'Generate Secure Password' highlighted by a red oval. On the right, a 'Generate Password' tool window is shown, featuring the LastPass logo, a 'Show Advanced Options' checkbox, and various settings: 'Password Length' (12), 'Pronounceable' (unchecked), 'A-Z' (checked), 'a-z' (checked), '0-9' (checked), 'Special' (unchecked), 'Minimum Digit Count' (1), 'Avoid Ambiguous Characters' (unchecked), and 'Require Every Character Type' (checked). The generated password 'e6FZKdUgDJ4h' is displayed in a text box with a dropdown arrow, accompanied by a strength indicator bar. 'Generate', 'Copy', and 'Close' buttons are at the bottom.

Change your password

- Passwords are case-sensitive and must be at least 6 characters.
- A good password should contain a mix of capital and lower-case letters, numbers and symbols.

Old password:

New password:

Confirm new password:

Change password or **Cancel**

Privacy Controls Settings

Tools

- ◀ BACK
- Generate Secure Password**
- Identities (All)
- Site Search
- Recheck Page
- Refresh Sites
- Import From
- Export To
- Print
- Check For Updates
- Clear Local Cache
- Security Check
- Other Sessions
- About...
- + Add Site
- + Add Secure Note

◀ BACK

LastPass ****

Show Advanced Options

Password Length

Pronounceable

A-Z a-z 0-9 Special

Minimum Digit Count

Avoid Ambiguous Characters

Require Every Character Type

▼

Generate **Copy** **Close**

Creating and Saving New Credentials

Step 1: Browse to the new site and find the 'register' page.

Step 2: Click on the password field and note the notification bar. Select 'Generate'.

Step 3: Complete and submit the registration form. (Do not hit the 'Save Site' button at this time or it will save the incorrect URL.)

Step 4: Find and select 'log-off'.

Step 5: Find and select 'log-in'.

Step 6: Click on the LastPass icon in your browser. Scroll to the bottom of the menu and select 'Copy generated password'. Paste into password field.

Step 7: Submit the page. Note the notification bar. Select 'Save Site'.

- If the site has only 1 related login, then you might want to select 'auto-login'**
- If the site is particularly sensitive (financial services), then you might want to select 'Require Password Reprompt'.**
- Assign to a group to keep your vault well-organized.**

Tips and Tricks

Always edit/update and store credentials at the Site, never in the LastPass vault.

If a site is not logging you in properly:

- 1. Go to your vault -> edit.**
- 2. Verify username and password fields.**
- 3. Copy and paste the username and password into the login screen manually. If this does not work, then it is likely that incorrect info was stored in LastPass.**

If LastPass is taking you to the wrong page of the site, then you have probably not saved the login URL of the site. To correct: surf to the login screen of the site, copy the full URL, click on the plug-in -> my LastPass vault -> 'edit' next to the site in question -> paste the copied URL into the URL space.

If all else fails, write down the password, delete the entry from your vault, and start over.

AUTOMATED FORM FILL: <http://helpdesk.lastpass.com/fill-form-basics/>

Using LastPass to store the data you typically have to type into web forms is both easy and secure. Your data is encrypted locally on your computer with the key that only you know before it is sent to LastPass, so you can securely store your credit card, ssn, phone number, and other sensitive data you wish to easily access.

SECURE NOTES: <http://helpdesk.lastpass.com/password-manager-basics/secure-notes/>

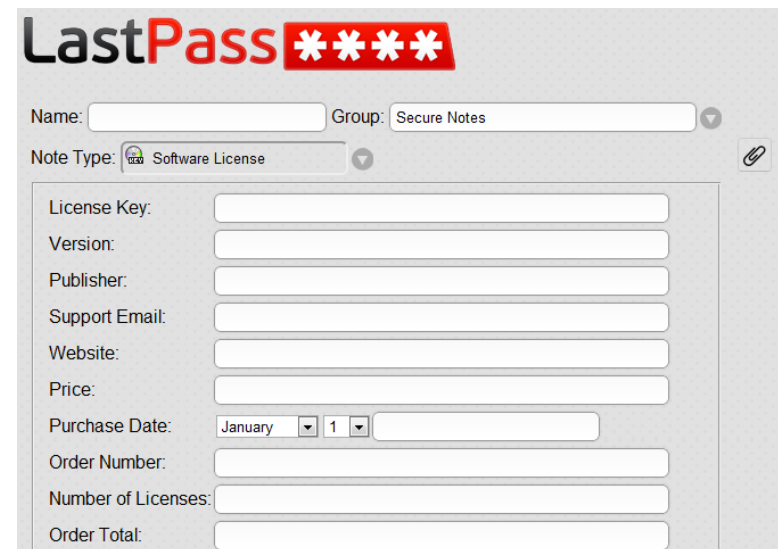
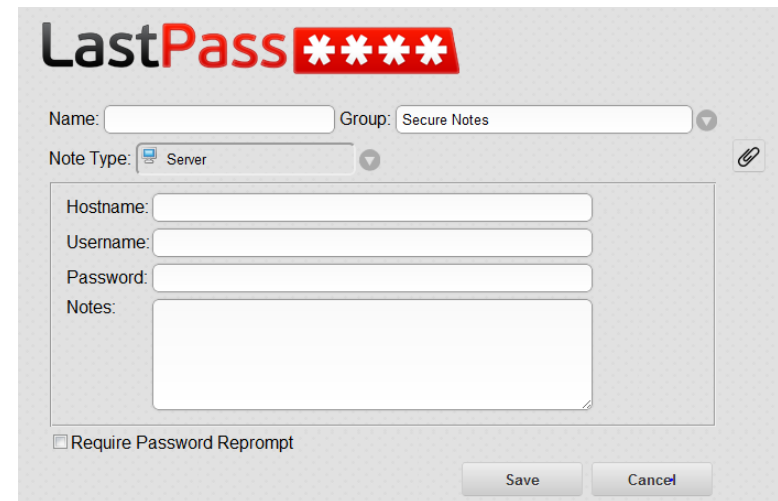
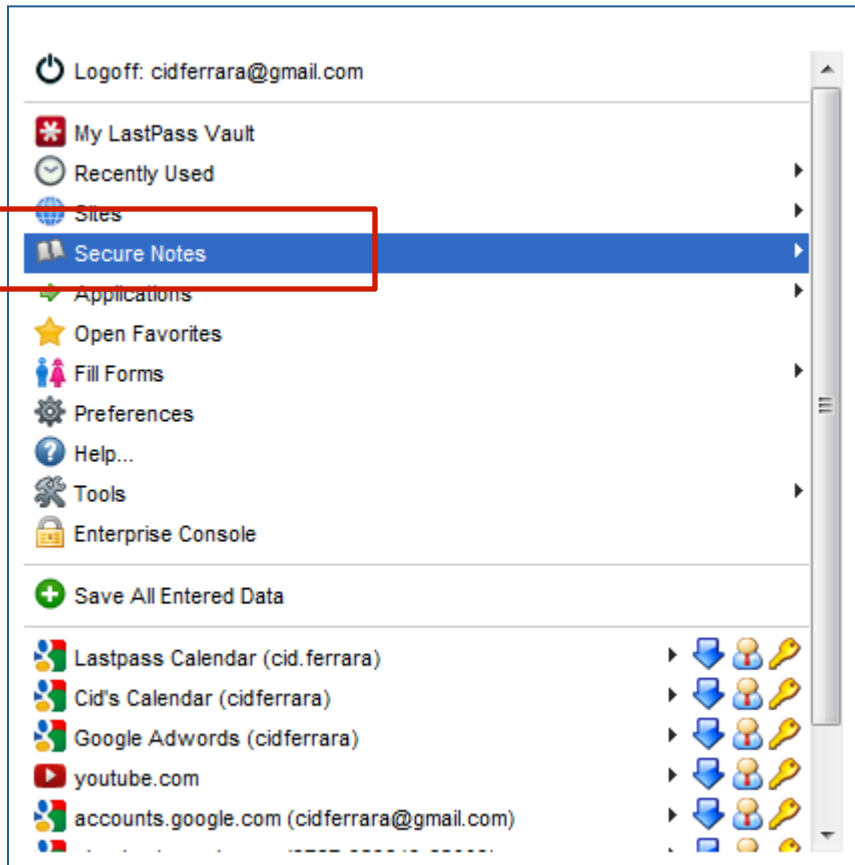
LastPass Secure Notes allow you to store private information safely and securely. Think of it as a password-protected, digital notepad that you can access from anywhere, at anytime. Some examples of data that you might save in a secure note include bank account numbers, social security numbers of your family members, passport numbers, combinations to safes, etc.

SECURITY CHALLENGE:

<https://lastpass.com/index.php?securitychallenge=&fromwebsite=1&lpnorefresh=1>

Storing your logins with LastPass is just the first step. Now you need to generate random, secure passwords for all of your sites. Having identical or similar passwords for multiple websites is extremely dangerous, because access to one account becomes equivalent to access to all of your accounts. The Security Challenge will help you determine where you're at, and give you steps for improving your security with LastPass. As always with LastPass, all encryption and decryption is done 100% locally on your machine. All unencrypted passwords are tested with local checks only.

Updating Passwords Using 'Generate Password' Tool





LastPass for Applications (Windows Only)

Saving Non-Web Based (Application) Credentials

Step 1: Open the application that you wish to save.

Step 2: Click the LastApp icon in the system tray and select 'add application'.

Step 3: Click 'find', then click on the application window. Return to the LP window and click 'next'.

Step 4: Type the credentials into the LastApp form and select 'auto-fill', or hit 'train' (depends on the app.)

Step 5: Hit 'save'. At this point the new app will have been added to the list of stored apps. You can close all open windows.

User Manual: <http://helpdesk.lastpass.com/password-manager-basics/adding-a-site/>

Launching a Saved App – “Hands-free” Login

Step 1: Click on the LastApp icon in the system tray and scroll up to ‘Applications’ and rest on the desired application. Then select ‘launch’ from the menu.

Step 2: The stored credentials will auto-fill on the login form. Click the submit button to log-in.

LastPass: The LAST password you’ll have to remember!

User Manual: <http://helpdesk.lastpass.com/password-manager-basics/adding-a-site/>